Certificate Policy

for the

State of Washington

Public Key Infrastructure

TABLE OF CONTENTS

1 INTRODUCTION

2 GENERAL PROVISIONS

3 IDENTIFICATION AND AUTHENTICATION

4 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

5 CA FACILITY AND MANAGEMENT CONTROLS

6 TECHNICAL SECURITY CONTROLS

7 CERTIFICATE AND CRL PROFILES

8 POLICY ADMINISTRATION

Appendices

1 INTRODUCTION

1.1 OVERVIEW

This Certificate Policy ("this Policy") contains the rules governing the issuance and use of Certificates among those parties authorized to participate in the Public Key Infrastructure ("PKI") described by this Policy.

This PKI is intended to support digital signatures, encryption and access control applications in the following electronic environments:

- Communications and transactions between and/or within agencies, departments, units and/or Organizations which are a part of any governmental body ("Government Agencies");
- Communications and transactions among or between Government Agencies, Public Organizations, Private Organizations and/or Individuals, in connection with governmental activities;
- Communications and transactions among or between Government Agencies, Public Organizations, Private Organizations, and/or Individuals as health care providers, health plans and other participants in the health care sector;
- Communications and transactions among or between Government Agencies, Public Organizations, Private Organizations, and/or Individuals as universities, colleges, teaching and research personnel, students and other participants in the academic sector;
- Communications and transactions among or between Government Agencies, Public Organizations, Private Organizations and/or Individuals in connection with consumer activities; and
- Communications and transactions among or between Government Agencies, Public Organizations, Private Organizations and/or Individuals for any other purpose not specified above.

In particular, this Policy describes the relationships within the PKI, among and between:

- Government Agencies in their capacity as Subscribers to Certificates;
- Government Agencies in their capacity as parties relying upon Certificates issued under this Policy ("Relying Parties");
- Public Organizations in their capacity as Subscribers to Certificates;
- Public Organizations in their capacity as Relying Parties;
- Private Organizations in their capacity as Subscribers to Certificates;
- Private Organizations in their capacity as Relying Parties;
- Individuals in their capacity as Subscribers to Certificates;
- Individuals in their capacity as Relying Parties;

- An Issuing Certificate Authority ("Issuing CA") under this Policy;
- Private Organizations acting as Repositories or Certificate Manufacturing Authorities ("CMA") under this Policy;
- Private Organizations and Individuals acting in the capacity of Registration Authority ("RA") under this Policy; and
- The State of Washington, through its Department of Information Services, and the PKI Policy Management Authority ("PMA").

Certificates issued under this Policy may be used:

- To verify Digital Signatures;
- To encrypt and authenticate electronic communications;
- To provide evidence of identity in order to support access controls established by Relying Parties to prevent unauthorized access to computer systems and electronic information and documents, under conditions established by such Relying Parties.

1.1.1 Policy Overview

The PKI governed by this Policy makes use of Issuing CA's licensed under the laws of the State of Washington. Subscribers and Relying Parties not located in the State of Washington may obtain and/or rely upon Certificates issued under this Policy, and such Certificates may be used for transactions, applications and communications outside the State of Washington, provided that the laws of the State of Washington are applied as a matter of law, unless prohibited by Federal law or by a private agreement between the Issuing CA and a Relying Party.

1.1.1.1 State Licensure of Issuing CA

Issuing CA's under this Policy are required to be licensed under the State of Washington's Electronic Authentication Act (EAA), codified as Chapter 19.34 of the Revised Code of Washington. CAs licensed in Washington are required to maintain "trustworthy systems" for the issuance and management of certificates. Licensed CAs are also required to use only personnel who have passed background security checks and tests of their understanding of certificate management for duties involving the issuance of certificates, operation of certificate systems, and the establishment or adoption of CA operational and security policies.

Washington state licensure of an Issuing CA is a factor a Subscriber or Relying Party may consider in determining whether and how to use or rely upon a Certificate. The EAA provides that Digital Signatures created with certificates issued by licensed CAs may constitute legal signatures, which have the same force and effect under Washington State law as handwritten signatures.
Relying Parties that rely on a certificate issued under this Policy that do not consent to Washington State jurisdiction and the EAA, and who have not executed a private Relying Party Agreement with an Issuing CA, are subject to forfeiture of claims as provided in section 2.1.4.5. This Policy recognizes that, in the case of transactions involving the federal government, Federal law may prevail.

1.1.1.2 Identity Assurance and Certificate Types

This Policy provides for three (3) types of Certificate. Among the factors that differentiate each type are the degree of assurance of the identity of the Subscriber provided by (1) the procedures used to Identify and Authenticate ("I&A") the Subscriber prior to issuance of the Certificate ("I&A Procedures"), and (2) the degree of security a

Subscriber is required to use to protect his/her Private Key under this Policy ("Subscriber Security Obligations"). The three Certificate types are designated High, Intermediate and Standard.

It is a general rule that security and convenience considerations must be balanced in selecting procedures for access to and use of electronic systems, and that any increase in security may cause a decrease in convenience. This PKI uses three Certificate types in order to permit Subscribers and Relying Parties to select the preferred balance between security and convenience for their intended uses.

The Certificate type to be used for any given application, transaction or communication must be determined by the parties using or engaging in that application, transaction or communication, based upon their judgment as to the appropriate balance between security and convenience for their purposes. While this Policy identifies Recommended Reliance Limits and suggests some uses applicable to each Certificate type, these are for general guidance and should be considered as only some of the factors applicable to a decision about the use of any type of Certificate for any specific use or transaction.

High Assurance Level Certificates are based upon the most secure I&A Procedures and strictest Subscriber Security Obligations applicable to this PKI. Standard Assurance Level Certificates are based upon the most convenient I&A Procedures and least stringent Subscriber Security Obligations. Intermediate Assurance Level Certificates fall between High and Standard in terms of both convenience and security.

The I&A Procedures and Subscriber Security Obligations applicable to each Certificate type are described below. Certificates may be issued to Individuals, Organizations, and Electronic Devices, subject to the limitations of this Policy.

Certificates may be issued under this Policy following I&A of a Subscriber's identity in the manner set forth in this Policy. An Issuing CA will revoke Certificates in the circumstances enumerated in Section 4.9. An Issuing CA is required to maintain records and information logs in the manner described in Section 5.5.

Private Keys must be created, used and stored in a trustworthy and secure manner. Keys may have a validity period as indicated in this Policy. Confidentiality Keys issued by an Issuing CA will be backed-up to protect against data loss or data corruption. No personal information collected by an Issuing CA may be disclosed without the Subscriber's consent unless required by law. CA activities are subject to inspection and/or audit for compliance with this Policy in accordance with Section 2.7.

1.1.2 General Definitions — Capitalized terms used herein and in related agreements and other documents incorporating this Policy have the following meanings:

Affiliated Individual — An Individual who is authorized by an Organization to hold a Certificate containing the Organization's name as an employee, partner, member, officer, agent, licensee, permitee or other associate of the Organization.

Authenticating RA — A Registration Authority which has been authenticated by an Issuing CA, issued a Registration Authority Certificate by the Issuing CA, and entered into an agreement with the Issuing CA authorizing the Authenticating RA to process Subscriber applications for Certificates, and conduct I&A of Subscribers in accordance with all applicable laws and this Policy.

Activation Data — Private data used or required to access or activate cryptographic modules (i.e., a PIN,

	pass phrase or a manually-held key share used to unlock Private Keys for signing or decryption events).
Authority Revocation List (ARL)	A list of revoked CA certificates. An ARL is a CRL for CA cross-certificates.
CA Certificate	The Certificate at the beginning of a certification chain within the State of Washington PKI hierarchy, self-issued in a secure and trustworthy manner. A CA Certificate is established as part of the set-up and activation of an Issuing CA. The CA Certificate contains the Public Key that corresponds to the CA Private Signing Key that the CA uses to create Certificates. The CA Certificate, and its corresponding Public Key, may be embedded in software or obtained or downloaded by the affirmative act of an Relying Party in order to establish a certification chain.
CA Private Signing Key	The Private Key that corresponds to an Issuing CA's Public Key listed in the CA Certificate and that is used to sign Certificates.
CA Private Root Key	The Private Key used to sign the CA Certificate and certify the CA's Public/Private Key Pair.
Certificate	A computer-based record or electronic message that at a minimum: (a) identifies the Certification Authority issuing it; (b) names or identifies a Subscriber; (c) contains the Public Key of the Subscriber; (d) identifies the Certificate's operational period; (e) is digitally signed by a Certification Authority.
Certificate Policy (CP)	This Policy, which contains a named set of rules that indicates the applicability of a Certificate to particular communities and classes of applications with common security requirements.
Certificate Profile	The protocol used in Section 7 of this Policy to establish the allowed format and contents of data fields within a Certificate. Data fields within a Certificate usually identify the Issuing CA, the Subscriber, the Issuing CA's Certification Practice Statement, the Certificate's validity period and other information that identifies the Subscriber. Certificate Profile is attached hereto as Appendix A and incorporated by reference.
Certificate Revocation List (CRL)	A list of Certificates indicating whether a Certificate has been revoked earlier than the end of the Certificate's validity period.
Certification Authority (CA)	See Issuing CA.
Certification Practice Statement (CPS)	A statement of the practices that an Issuing CA employs in issuing and/or administering Certificates in accordance with this Policy.
Confidentiality Key	The Private Key of a Key Pair used by the Subscriber to decrypt messages encrypted with the Public Key of the Key Pair.
Cross-Certificate	A Certificate used to establish a trust relationship between two Certification Authorities.
Cryptomodule	Hardware and/or software that: (I) generates Key Pairs, (ii) stores cryptographic material, and/or (iii) performs cryptographic functions.
Digital Signature	The transformation of a message involving a Certificate and Public Key Cryptography such that a Relying Party having the initial message and the Subscriber's Certificate

	can accurately determine (a) whether the transformation was created using the Private Key that corresponds to the Subscriber's Public Key, and (b) whether the message has been altered since the transformation was made.
Distinguished Name (DN)	The unique identifier for a Subscriber so that he, she or it can be located in a directory (e.g., the DN for a Subscriber might contain the following attributes: common name (cn), e-mail address (mail), organization name (o), organizational unit (ou), locality (l), state (st) and country (c)).
Electronic Device	Computer software or hardware or other electronic or automated means configured and enabled by the Subscriber to act as its agent and to initiate or respond to electronic records or performances, in whole or in part, without review or intervention by the Subscriber.
Globally Unique Identifier (GUID)	A Globally Unique Identifier, also called a Universally Unique Identifier (UUID), is the result of a process that yields a 24 character long string, containing combinations of numbers, letters and/or special characters that is appended to the Common Name (CN) in individual or organizational certificates. The GUID may contain only those characters found in the following character set: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz01 23456789[ ]- No other characters may be used. The GUID must be unique within the domain of Certificates issued by an Issuing CA, and must be unique across all other CA domains issuing certificates subject to this Policy. Further information on how a GUID is created and maintained can be found in Appendix B to this Certificate Policy which is attached hereto and incorporated by reference.
Hardware Token	A secure hardware device (e.g. smartcard or a USB token) used to store a Subscriber's Private Keys and Certificates.
High Assurance Level Certificate	A High Assurance Level Certificate may only be issued based upon I&A Procedures which include face-to-face Registration by a Licensed Notary or Operative Personnel acting on behalf of an Issuing CA directly or through an RA, Third Party Identity Proofing, and Out-of-Band notification and delivery of Activation Data. Subscribers must use reasonable efforts to protect the security of a Private Key for a High Assurance Level Certificate, including storage in a Hardware Token or Software Cryptomodule, protected by a Strong PIN or password. A High Assurance Level Certificate may be used to provide evidence of the identity of the Subscriber, for confidential communications using encryption, and as evidence that a message to which the Digital Signature of the Subscriber is affixed has not been altered. The Recommended Reliance Limit for a High Assurance Level Certificate is fifty thousand dollars ($50,000.00).
High-Security Zone	An area to which access is controlled through an entry point and limited to authorized, appropriately screened personnel and properly escorted visitors, accessible only from Security Zones, separated from Security Zones and Operations Zones by a perimeter. High-Security Zones are monitored 24 hours a day and 7 days a week by security staff, other personnel and electronic means.
Identification and Authentication (I&A)	To ascertain and confirm through appropriate inquiry and investigation the identity of a Subscriber or other person.

Individual	A natural person and not a juridical person or legal entity.
Intermediate Assurance Level Certificate	An Intermediate Assurance Level Certificate may be issued by an Issuing CA based upon I&A using online Registration, Third Party Identity Proofing, and Out-of-Band notification and delivery of Activation Data. Subscribers must use reasonable efforts to protect the security of a Private Key for an Intermediate Assurance Level Certificate, including storage in a Hardware Token or Software Cryptomodule protected by a Strong PIN or password. An Intermediate Assurance Level Certificate may be used to provide evidence of the identity of the Subscriber, for confidential communications using encryption, and as evidence that a message to which the Digital Signature of the Subscriber is affixed has not been altered. The Recommended Reliance Limit for an Intermediate Assurance Level Certificate is ten thousand dollars ($10,000.00).
Issue Certificates	The acts performed by an Issuing CA in creating a Certificate, listing itself as "Issuer", and notifying the Certificate applicant of its contents and that the Certificate is ready and available for acceptance.
Issuing CA	An Issuing CA is an entity that has entered into a written agreement with DIS and/or the PMA, granting it a license in accordance with Section 2.9 of this Policy, to issue and manage certificates and to otherwise use this Certificate Policy. DIS, in its sole discretion and in accordance with such agreement, may revoke this license effective immediately upon an Issuing CA's deviation from the agreement, this Policy and/or its Certification Practice Statement.
Key Generation	The trustworthy process of creating a Public/Private Key Pair.
Licensed Notary	A Licensed Notary is a Notary Public licensed and in good standing in the State of Washington, or in any other jurisdiction whose notarial acts are accepted in the State of Washington.
Lightweight Directory Access Protocol	A client-server protocol used for accessing an X.500 directory service over the Internet.
Master Contract	Master Contract refers to that certain Master Contract Number T00-MST-001 for Certification Authority and Public Key Infrastructure Services between Digital Signature Trust Company (DST) and the State of Washington Department of Information Services, dated as of March 30, 2000. The Master Contract is not incorporated into this Policy and applies only between DST and the State in its capacity as a party to the Master Contract; provided that nothing in this Policy shall be deemed to supersede or amend the Master Contract.
Online Certificate Status Checking Protocol (OCSP)	A certificate checking protocol identified by RFC 2560 that enables an application to determine the revocation state of an identified certificate by issuing a status request to an OCSP responder and suspending acceptance of the certificate in question until the responder has provided the application with a response.
Operations Zone	An area where access is limited to personnel who work there and to properly escorted visitors. Operations Zones should be monitored at least periodically, based on a Threat Risk Assessment and should preferably be accessible from a Reception Zone.
Operative Personnel	Operative Personnel are individuals who are agents or employees of an Issuing CA, who are qualified for such service as provided in the Washington Administrative Code.

Organization	An entity legally-recognized in its jurisdiction of origin (e.g.as a company, corporation, partnership, sole proprietorship, government department, non-government organization, university, special interest group or non-profit corporation.)
Out of Band	Communication between parties utilizing a means or method that differs from the current method of communication; for example, where one party uses the U.S. mail to communicate with another party to confirm a current communication through an online application.
Policy	This Certificate Policy, used interchangeably with “CP.”
Policy Management Authority	A committee established by the Director of the Department of Information Services of the State of Washington responsible for making recommendations to DIS for setting, implementing, interpreting and administering policy decisions regarding this Policy and for resolving disputes between parties subject to this Policy.
Private Key	The key of a Public/Private Key Pair kept secret by its holder, used to create Digital Signatures and to decrypt messages or files that were encrypted with the Subscriber’s corresponding Public Key.
Private Organization	A Private Organization is any legally recognized entity other than an Individual, which is not an agency, unit, department, division or other subdivision of any governmental authority of any jurisdiction.
Public Organization	A Public Organization is any agency, unit, department, division or other subdivision of any governmental authority.
Public/Private Key Pair	A Public Key and its corresponding Private Key in Public Key Cryptography (also known as asymmetric cryptography); keys that have the property that the Public Key can verify a Digital Signature that the corresponding Private Key creates; keys that can encrypt and decrypt information for confidentiality purposes, in which the Public Key is used to encrypt data that can be decrypted only by using the intended recipient's corresponding Private Key.
Public Key	The key of a Public/Private Key Pair that is used to verify a Digital Signature created with its corresponding Private Key, that can be made publicly available in a Certificate, and that can also be used to encrypt messages or files which can then be decrypted only with the intended recipient's corresponding Private Key. The Public Key is delivered to the Issuing CA during the Certificate application process.
Public Key Cryptography	A type of cryptography also known as asymmetric cryptography that uses a unique Public/Private Key Pair of mathematically related numbers. The Public Key can be made available to anyone who wishes to use it, while the Private Key is kept secret by its holder. Either key can be used to encrypt information or generate a Digital Signature, but only the corresponding key can decrypt that information or verify that Digital Signature.
Public Key Infrastructure (PKI)	The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based Public Key Cryptography system.
Public Repository	See Repository.
Reasonable Reliance	Reliance on a Digital Certificate is considered reasonable under the following conditions. The Relying Party has:

- Verified that a Digital Signature in question was created by the Private Key corresponding to the Public Key in the Certificate while the Certificate was valid (i.e., confirmed that the document signed with the Digital Signature had not been altered and an online status check of the Certificate confirmed that the Certificate was valid); or, for the purposes of access control, verified that the Certificate was valid and an online status check of the Certificate was confirmed,

- Complied with the requirements of the Certificate User Notice set forth in Section 7.1.8; and

- Used the Certificate for purposes appropriate under this Policy, without knowledge of any facts that would cause a person of ordinary business prudence to refrain from relying on the Certificate, and under circumstances where reliance would be reasonable and otherwise in good faith in light of all the circumstances that were known or should have been known to the Relying Party prior to reliance.

Reception Zone	The entry to a facility where the initial contact between the public and an Issuing CA or Authenticating RA occurs, where services are provided, information is exchanged and access to restricted (Operations, Security and High-security) zones is controlled. To varying degrees, activity in a Reception Zone is monitored by the personnel who work there, by other personnel or by security staff. Access by the public may be limited to specific times of the day or for specific reasons. Entry beyond the Reception Zone is indicated by a recognizable perimeter such as a doorway or an arrangement of furniture and dividers in an open office environment.
Registration	Registration is the process of receiving or obtaining a request for a Certificate from a Subscriber, and collecting and entering the information needed from that Subscriber to include in and support I&A and issuance of a Certificate.
Registration Authorities	Organizations or Individuals that are authorized by an Issuing CA to locally collect Subscribers' identity information for purposes of entry into a Certificate. No Organization or Individual shall be authorized to act as an RA by an Issuing CA unless the Issuing CA has bound the Individual or Organization to comply with the terms of this Policy.
Relying Party	A Relying Party is an Individual or Organization who relies on a certificate issued under the terms of this Policy. A Relying Party's actions in reliance upon a certificate are reasonable when their actions constitute Reasonable Reliance as specified in this Policy.
Relying Party Agreement	A Relying Party Agreement is an agreement between an Issuing CA and any Individual or Organization under which the Individual or Organization has agreed to be bound by this Policy and an Issuing CA's Certification Practice Statement.
Repository	An online system maintained by or on behalf of a Certification Authority for storing and retrieving Certificates and other information relevant to Certificates and Digital Signatures.
Recommended Reliance Limit	A Recommended Reliance Limit is an Issuing CA's recommended maximum total amount which a Relying Party should risk in a transaction or communication depending

	upon a given Certificate. Recommended Reliance Limits vary by Certificate Type. A Relying Party is advised to consider the Recommended Reliance Limit in electing to rely upon a Certificate, but is not prohibited from using any Certificate Type for any purpose or transaction based upon the applicable Recommended Reliance Limit.
Revocation or Revoke a Certificate	The act of making a Certificate ineffective permanently from a specified time forward. Revocation is effected by notation or inclusion in a set of revoked Certificates or other directory or database of revoked Certificates.
Security Zone	An area to which access is limited to authorized personnel and to authorized and properly escorted visitors. Security Zones should preferably be accessible from an Operations Zone, and through a specific entry point. A Security Zone need not be separated from an Operations Zone by a secure perimeter. A Security Zone should be monitored 24 hours a day and 7 days a week by security staff, other personnel or electronic means.
Shared Secret	Activation Data used to assist parties in authenticating identity and establishing a reliable channel of communication. For purposes of establishing identity between an RA and a Subscriber, a Shared Secret may consist of a PIN or password shared solely between the RA and the Subscriber, but not the Issuing CA. For purposes of establishing identity between the Subscriber and the Issuing CA necessary for certificate issuance, a Shared Secret consists of different Activation Data, which is shared among the RA, Subscriber and Issuing CA.
Signature Key	The Private Key of a Key Pair used by the Subscriber for signing and to establish non-repudiation.
Software Cryptomodule	A software program that performs the functions of a Cryptomodule.
Sponsoring Organization	An Organization that has authorized the issuance of a Certificate identifying the Subscriber as having an affiliation with the Organization (e.g., as an employee, partner, member, officer, agent, licensee, permitee or other associate).
Standard Assurance Level Certificate	A Standard Assurance Level Certificate may be issued by an Issuing CA based upon I&A procedures using online Registration, Third Party Identity Proofing, and Out-of-Band notification and delivery of Activation Data. A Subscriber may store a Private Key for a Standard Assurance Level Certificate in the browser of any computer at the Subscriber's election and risk. Use of a password or PIN to protect the Private Key is required. The Recommend Reliance Limit for a Standard Assurance Level Certificate is one thousand dollars ($1,000.00).
State	The State of Washington.
Strong PIN or Password	An alphanumeric code of at least eight characters used to gain access to a locked system.
Subscriber	An Individual, Organization or Electronic Device that (a) is named or identified in a Certificate as its subject, and (b) holds a Private Key that corresponds to a Public Key listed in that Certificate. A Subscriber is the entity whose name appears as the subject in a Certificate, and who asserts that it uses the Certificate and corresponding Keys in accordance with this Policy.

Third Party Identity Proofing	"Third Party Identity Proofing" is a process by which an Issuing CA confirms Subscriber information provided in Registration, by verification through other organizations and agencies which serve as information or reference services.
Trustworthy System	Computer hardware and software that: (a) are reasonably secure from intrusion and misuse; and (b) conform with requirements established in the Washington Administrative Code.

1.1. Acronyms

ARL	Authority Revocation List
CA	Certification Authority
CMA	Certificate Manufacturing Authority
CP	Certificate Policy, used interchangeably with "Policy."
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DST	Digital Signature Trust Co.
I&A	Identification and Authentication
LDAP	Lightweight Directory Access Protocol
OID	Object Identifier
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RA	Registration Authority
RCW	Revised Code of Washington
PMA	Policy Management Authority
WAC	Washington Administrative Code
X.500	The ITU-T (International Telecommunication Union-T) standard that establishes a distributed, hierarchical directory protocol organized by country, region, Organization, etc.
X.509	The ITU-T (International Telecommunication Union-T) standard for Certificates. X.509, version 3, refers to Certificates containing or capable of containing extensions.

1.2 IDENTI-FICATION

The American National Standards Institute ("ANSI") has assigned a unique numeric object identifier ("OID") of 2.16.840.1.113839to DST. DST has specifically assigned an OID to the State of Washington for this Policy, 2.16.840.1.113839.0.4, which may not be used except as specifically authorized by this Policy.

The Policy OID to be asserted in Certificates issued in accordance with the policy stipulations herein shall have a base arc of: {joint-iso-ccitt (2) country (16) USA (840) organization (1) DST(113839)) CP (0) StateofWashington (4)}, and all Certificates issued under this Policy shall reference this arc in the Certificate Policies field of the Certificate.

There are three levels of assurance in this Policy, and each level of assurance has an Object Identifier (OID) to be asserted in certificates issued by an Issuing CA. The OIDs are identified as follows:

High Assurance Level Certificate
id-HighAssuranceLevel ID::= {id-Stateofwashington 1 } → 2.16.840.1.113839.0.4.1

Intermediate Assurance Level Certificate
id-IntermediateAssuranceLevel ID::= { id-Stateofwashington 2}
→2.16.840.1.113839.0.4.2

Standard Assurance Level Certificate
id-StandardAssuranceLevel ID::= { id-Stateofwashington 3 } →2.16.840.1.113839.0.4.3

Each level of Certificate, High, Intermediate or Standard, may be issued to certify a key as being used either for signing (Digital Signature Private Key) or for encryption (Confidentiality Key). The use of a specific key will be determined by the key usage extension, discussed in Sections 6.1.9 and 7.1.7.

1.3 COMMUNITY AND APPLICABILITY

This Policy describes an open-but-bounded ("OBB") Public Key Infrastructure, as described in the Internet Engineering Task Force ("IETF") Public Key Infrastructure X.509 ("PKIX") Part 4 Framework. A Certificate issued in an OBB PKI may be relied upon by multiple parties. An Issuing CA in an OBB PKI is a legal entity independent of its Subscribers and Relying Parties. A CP adopted for an OBB PKI reflects the agreements and understandings of the parties using the PKI.

The OBB PKI described in this Policy is based in the State of Washington, and this Policy is intended to be interpreted and enforced under the terms of the Washington Electronic Authentication Act ("EAA"), codified at Revised Code of Washington Chapter 19.34, as well as all regulations promulgated under the EAA. Certificates issued pursuant to this Policy may be used for communications and transactions and by parties within or outside the State of Washington, and between parties within and parties outside the State of Washington.

This Policy describes the rights and obligations of persons and entities authorized under this Policy to fulfill any of the following roles: Certificate Service Provider roles and End Entity roles, and Policy Management Authority Roles. Certificate Service Provider roles are Certification Authority, Registration Authority, Certificate Manufacturing Authority, and Repository. End Entity roles are Subscriber and Relying Parties. Requirements for persons and entities authorized to fulfill any of these roles are in this Section.

The community served by this OBB PKI includes any authorized party (Certificate Service Provider, Policy Management Authority, Relying Party and Subscriber) as defined by this Policy.

1.3.1 The Policy Management Authority

The Policy Management Authority (PMA) for this Policy advises the State of Washington Department of Information Services on policy matters and resolves disputes between parties served by this Policy.
The Policy Management Authority shall include representatives of the Washington Department of Information Services, customers using the PKI and others deemed appropriate by DIS, who shall be selected by the Director of the Washington Department of Information Services. Prior to the formal constitution of the PMA, PMA functions will be performed by a committee or task group established for such purposes by the Washington Department of Information Services, which will be deemed to be the PMA for all purposes under this Policy until the PMA is formally constituted.

1.3.1.1 Registration Authorities (RAs)

An Issuing CA shall remain responsible to the entities served by this Policy for the Certificates it issues. However, under this Policy, an Issuing CA may subcontract Registration Authority functions to RAs, subject to their agreement to be bound by this CP. An RA operating under this Policy is only responsible for those duties assigned to it by an Issuing CA pursuant to an agreement with the Issuing CA. Only Operative Personnel of an Issuing CA are authorized to accept applications and conduct I&A.

1.3.1.2 Certificate Manufacturing Authorities (CMAs)

An Issuing CA shall be responsible for the manufacture of Certificates. However, an Issuing CA may subcontract functions to third party Certificate Manufacturing Authorities (CMAs) who agree to be bound by this Policy, but an Issuing CA shall remain responsible for the performance and audit of those services in accordance with this Policy.

1.3.2	Repositories	An Issuing CA shall perform the role and functions of the Repository. An Issuing CA may subcontract performance of the Repository functions to a third party Repository who agrees to be bound by this Policy, but an Issuing CA remains responsible for the performance and audit of those services in accordance with this Policy.
1.3.3	End entities	
1.3.3.1	Subscribers	A Subscriber is the entity whose name appears as the subject in a Certificate, and uses the Certificate and corresponding Keys in accordance with this Policy. An Issuing CA may issue Certificates that reference this Policy to Individuals, Organizations and Electronic Devices provided that responsibility and accountability is attributable to an Individual as custodian of the Public/Private Key Pair.
1.3.3.2	Relying Parties	A Relying Party is any Individual or Organization that relies upon a Certificate issued under the terms of this Policy.
1.3.4	Applicability and Applications	
1.3.4.1	Determination of Acceptability of Certificate Type by Relying Party	This Policy is suitable for use in connection with electronic transactions as set forth below. The determination of the acceptability of any given Certificate Type for any particular purpose or transaction must be made by the Relying Party which intends to rely upon Certificates issued under this Policy. The factors to be considered by a Relying Party in making such a determination include: • Any legal requirements for the identification of a party, the protection of the confidentiality or privacy of information, or the legal acceptability of Digital Signatures which may apply; • All facts listed in the Certificate or of which the Relying Party has notice, including this Policy; • The economic value of the transaction or communication, if applicable; • The potential losses or damage which might be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction or communication; • The applicability of the laws of the State of Washington; • The Recommended Reliance Limit applicable to the Certificate Type; • The Relying Party's previous course of dealing with the Subscriber, if any; • Usage of trade, especially trade conducted by secure systems or other computer-based methods; and • Any other indicia of reliability or unreliability, or other facts of which the Relying Party knows or has notice, pertaining to the Subscriber and/or the application, communication or transaction.
1.3.4.1.1	Standard Assurance Level Certificates	Standard Assurance Level Certificates may be relied upon as evidence of the identity of the Subscriber and as reasonable evidence that an electronic message or document has not been altered, subject to the general prohibitions on Certificate use stated below. The Recommended Reliance Limit should be considered when a false or

		incorrect identification of the Subscriber or a failure of the security or integrity of an electronic message or document may have significant legal or financial consequences. The Recommended Reliance Limit for a Standard Assurance Level Certificate is one thousand dollars ($1,000.00).
1.3.4.1.2	Intermediate Assurance Level Certificates	Intermediate Assurance Level Certificates may be used in connection with any purpose or transaction for which a Standard Assurance Level Certificate may be used. Subject to the general prohibitions on Certificate use stated below, an Intermediate Assurance Level Certificate may be relied upon as reasonable evidence of the identity of the Subscriber, for confidential communications using encryption, and as reasonable evidence that an electronic message or document has not been altered. The Recommended Reliance Limit for an Intermediate Assurance Level Certificate is ten thousand dollars ($10,000.00).
1.3.4.1.3	High Assurance Level Certificates	High Assurance Level Certificates may be used in connection with any purpose or transaction for which a Standard or Intermediate Assurance Level Certificate may be used. Subject to the general prohibitions on Certificate use stated below, a High Assurance Level Certificate may be used for any purpose or transaction in which a false or incorrect identification, or a failure of the security or integrity of an electronic message could lead to a serious compromise of private information, imprisonment, financial loss, or legal action for correction. The Recommended Reliance Limit for a High Assurance Level Certificate is fifty thousand dollars ($50,000).
1.3.4.2	Purposes	Certificates that reference this Policy are intended to support verification of Digital Signatures in applications where the identity of communicating parties needs to be authenticated, where a message or file needs to be bound to the identity of its originator by a signature, where the integrity of the file or message has to be assured, to enable encryption for confidential communications, and for authentication for access control. The suitability of a given Certificate for any given purpose depends upon the level of assurance of the identity of the Subscriber required by a Relying Party for that purpose, and the acceptability of Digital Signatures under applicable law.
1.3.4.3	Prohibited Applications	No Certificate that references this Policy may be used for the execution of any application requiring fail safe performance, such as the operation of nuclear power facilities, air traffic control systems, aircraft navigation systems, weapons control systems, or any other system whose failure could lead to injury, death or material environmental damage, or where otherwise prohibited by law.
1.3.4.4	Cross-certification	DIS or its designee may approve the issuance of a cross-certificate between CAs. Any cross-certification to external organizations will only be done after approval by DIS or its designee.

1.4 CONTACT DETAILS

This Certificate Policy is owned by the State of Washington.

1.4.1	Specification / Policy Administration Organization	Communication to the PMA should be addressed to: Scott Bream State of Washington Department of Information Service 1110 Jefferson St. SE Olympia, WA 98504-2445
1.4.2	Contact person	Questions regarding the implementation and administration of this Policy should be directed to: Scott Bream

State of Washington
Department of Information Service
1110 Jefferson St. SE
Olympia, WA 98504-2445

1.4.3 Person determining CPS suitability for Policy

The Department of Information Services will, with guidance of the PMA, and in the exercise of reasonable discretion, determine the suitability of any CPS to this Policy.

2 GENERAL PROVISIONS

Nothing in this Policy shall be construed to conflict with, alter, or eliminate any other obligation, responsibility, or liability that may be imposed on any person by virtue of any contract or obligation that is otherwise determined to be controlling by applicable law, including but not limited to the terms of the Master Contract.

2.1 APPORTIONING LEGAL RESPONSIBILITIES AMONG PARTIES

2.1.1 CA Obligations, Representations and Liability

An Issuing CA is authorized and required to conduct the following aspects of the issuance and management of Certificates:

- Application, enrollment and I&A for all categories of Certificate, provided that the Issuing CA may delegate such duties to the extent and as provided in this Policy;
- Acceptance of completed applications and enrollment materials for Certificates from RAs, and enrollment of Subscribers upon such acceptance;
- The certificate manufacturing process;
- Publication, suspension, revocation and renewal of Certificates; and
- Management of Issuing CA operations and infrastructure related to Certificates in accordance with the requirements, representations, and warranties of this Policy.

2.1.1.1 Notification of certificate issuance and revocation

An Issuing CA shall make CRLs available to Subscribers and Relying Parties in accordance with Section 4.9. An Issuing CA shall notify a Subscriber when a Certificate bearing the Subscriber's DN is issued or revoked.

2.1.1.2 Accuracy of representations

By issuing a Certificate that references this Policy, an Issuing CA certifies and warrants to the Subscriber, and to all Relying Parties who reasonably rely on the information contained in the Certificate during its operational period and in accordance with this Policy, that:

- The Issuing CA has issued, and will manage, the Certificate in accordance with this Policy;
- The Issuing CA has complied with the requirements of this Policy and any applicable CPS when authenticating the Subscriber and issuing the Certificate;
- There are no misrepresentations of fact in the Certificate reasonably known to the Issuing CA, and the Issuing CA has taken reasonable steps to verify any additional information in the Certificate;
- Information provided to the Issuing CA by the RA and/or Subscriber in the

Certificate application for inclusion in the Certificate has been accurately transcribed to the Certificate; and

- The Certificate meets all material requirements of this Policy and the Issuing CA's CPS.

2.1.1.3 Time between certificate request and issuance

Certificates shall be issued within the following time period following completion of I&A:

- High Assurance Level Certificates - Three (3) Business Days;
- Intermediate Assurance Level Certificates - Three (3) Business Days; and
- Standard Assurance Level Certificates - Three (3) Business Days.

2.1.1.4 Certificate revocation and renewal

An Issuing CA must ensure that any procedures for the expiration, revocation and renewal of a Certificate will conform to the relevant provisions of this Policy and will be expressly stated in the Subscriber Agreement and any other applicable document outlining the terms and conditions of the Certificate use. An Issuing CA must ensure that key changeover procedures are in accordance with Section 5.6. An Issuing CA will also ensure that notice of revocation of a Certificate will be posted to the CRL within the time limits stated in Section 4.9. The address of the CRL must be defined in the Certificate.

2.1.1.5 Protection of Private Keys

An Issuing CA must ensure that its Private Keys and Activation Data are protected in accordance with Parts 4 and 6 of this Policy.

2.1.1.6 Restrictions on Issuing CA's Private Key use

An Issuing CA must ensure that its CA Private Signing Key is used only to sign Certificates and CRLs. An Issuing CA may issue Certificates to Subscribers, CA and Authenticating RA personnel, devices and applications. An Issuing CA must ensure that Private Keys issued to its personnel, employees, officers, agents, and subcontractors to access and operate CA applications are used only for such purposes. If required, CA personnel should be issued sets of Subscriber keys and Certificates to be used for purposes other than CA use.

2.1.1.7 Assure Compliance

An Issuing CA must ensure that only it accepts and uses registration information transmitted as follows: (a) directly to the Issuing CA from Subscribers, or (b) directly from an RA which has contractually warranted to the Issuing CA that it understands and is obligated to comply with this Policy. An Issuing CA will ensure that its certification and repository services, issuance and revocation of Certificates, and issuance of CRLs are in accordance with this Policy. It shall ensure that all RAs follow the requirements of this Policy when dealing with any Certificates containing this Policy's OID or the associated keys. The Issuing CA and RAs will be obliged to ensure that their authentication and validation procedures are implemented as set forth in Part 3.

2.1.1.8 Consequences of Breach

Neither an Issuing CA nor any RA shall be deemed to be a party to any transaction between a Subscriber and any Relying Party due to its performance of duties under this Policy. Claims against an Issuing CA or RA are limited to showing that the Issuing CA or RA operated in a manner inconsistent with the law, this Policy, the CPS or a related agreement.

An Issuing CA is responsible and shall be liable only to Relying Parties, and only for direct damages suffered by such Relying Parties to the extent that they are proven to have been (a) caused by the failure of the Issuing CA or RA to comply with the terms of this Policy, and (b) sustained by such Relying Parties as a result of reliance on a

		Certificate in accordance with this Policy, but (c) only to the extent that the damages result from Reasonable Reliance on and use of the Certificate for purposes appropriate for the type of Certificate relied upon, as provided in this Policy. Except as expressly prohibited in this Policy, or superceding authority, an Issuing CA and any RA may disclaim all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.
2.1.2	RA Obligations, Representations and Liability	An Issuing CA shall have primary responsibility for all I&A and for all certificate manufacturing and issuing functions, but may delegate performance of these obligations to RAs. An Issuing CA is responsible to Subscribers and Relying Parties to ensure that the services performed by RAs are performed in a manner consistent with this Policy. If RAs are used to conduct I&A of Subscribers, then all such RAs must comply with all provisions of this Policy and the Issuing CA's CPS. All RAs shall be required to disclose and give notice to Subscribers of all relevant information pertaining to the rights and obligations of the Issuing CA, RA and Subscriber contained in this Policy, the Subscriber agreement, if applicable, and any other relevant document outlining the terms and conditions of use. An Issuing CA may enter into an indemnification agreement with an RA in accordance with section 2.3, so long as the Issuing CA remains responsible to Subscribers, Relying Parties and the State of Washington for the actions of the RA.
2.1.2.1	Notification of certificate issuance and revocation	Unless otherwise provided by contract, there are no requirements that an RA notify a Subscriber or Relying Party of the issuance or revocation of a Certificate.
2.1.2.2	Accuracy of representations	When an RA submits Subscriber information to a CA, it must certify to the Issuing CA that it has authenticated the identity of that Subscriber in accordance with Parts 3 and 4 of this Policy.
2.1.2.3	Protection of Private Keys	Each Individual performing RA duties on-line through a remote administration application with the Issuing CA must ensure that his or her Private Keys are protected in accordance with 5 and 6.
2.1.2.4	Restrictions on Private Key use	Private keys used by an RA administrator to access and operate RA Applications on-line with the Issuing CA must not be used for any other purpose.
2.1.2.5	RA Security and Operations Manual	Each RA shall comply with the provisions of the RA Security and Operations Manual provided to RAs by the Issuing CA.
2.1.2.6	Consequences of Breach	An RA shall indemnify, hold harmless and defend the Issuing CA against damages and claims arising from or pertaining to the alleged or proven failure of the RA to comply with the terms of this Policy and any applicable agreement with the Issuing CA; PROVIDED, HOWEVER that the Issuing CA will retain primary responsibility for any such damages and claims.
2.1.3	Subscriber Obligations, Representations and Liability	The responsibilities of each Subscriber for a Certificate are to:

2.1.3.1	Representations	Upon application for a Certificate and in all subsequent communications, provide complete and accurate responses to all appropriate requests for information made by the Issuing CA (or RA) during the applicant registration, certificate application, and authentication of identity processes; and upon notice to Subscriber of issuance of a Certificate naming the applicant as the Subscriber, review the Certificate to ensure that all Subscriber information included in it is accurate, and to accept or reject the Certificate in accordance with Section 4.4;
2.1.3.2	Subscriber Security Obligations/ Protection of Subscriber Private Key and key token	Generate a Key Pair using a secure system, and take appropriate precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the Private Key. “Appropriate precautions” and “secure system,” for purposes of the different types of Certificate provided for in this Policy, shall mean the following:
2.1.3.2.1	Standard Assurance Level Certificates	The Subscriber must use reasonable efforts to protect the Private Key for a Standard Assurance Level Certificate, which may be stored in the browser of any computer at the Subscriber’s election and risk. Use of a password or PIN to protect the Private Key is required.
2.1.3.2.2	Intermediate Assurance Level Certificates	The Subscriber must use reasonable efforts to protect the Private Key for an Intermediate Assurance Level Certificate, which will include storage in a Hardware Token or Software Cryptomodule protected by a strong PIN or password.
2.1.3.2.3	High Assurance Level Certificates	The Subscriber must use reasonable efforts to protect the Private Key for a High Assurance Level Certificate, which will include storage in a Hardware Token or Software Cryptomodule, protected by a strong PIN or password.
2.1.3.3	Restrictions on End-Entity Private Key use	Use the Certificate and the corresponding Private Key exclusively for purposes authorized by this Policy and only in a manner consistent with this Policy; and
2.1.3.4	Notification upon Private Key compromise	Instruct the Issuing CA (or RA, if applicable) to revoke the Certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the Private Key, or, in the case of a Certificate issued to an Affiliated Individual under Section 3.1.8, whenever the Affiliated Individual is no longer affiliated with the Organization.
2.1.3.5	Consequences of Breach	A Subscriber who is found to have acted in a manner counter to these obligations will have its Certificate revoked, and will forfeit all claims he or she may have against any other party to the PKI in the event of a dispute arising from the failure to fulfill the obligations above.
2.1.4	Relying Party Obligations, Representations and Liability	Prior to relying on or using a Certificate issued under this Policy, a Relying Party is obligated to:
2.1.4.1	Use of Certificates for appropriate purpose	Ensure that the Certificate and intended use are appropriate under the provisions of this Policy.
2.1.4.2	Verification responsibilities	See 2.1.4.3 below.

2.1.4.3	Revocation check responsibility	Check the status of the Certificate through OCSP or against the appropriate and current CRL in accordance with the requirements stated in Section 4.9 (as part of this verification process the Digital Signature of the CRL must also be validated).
2.1.4.4	Reasonable Reliance	For Digital Signatures created during the validity period of a Certificate, a Relying Party has a right to rely on a Certificate only under circumstances constituting Reasonable Reliance as defined in 1.1.2.
2.1.4.5	Consequences of Breach	A Relying Party who is found to have acted in a manner counter to these obligations will forfeit all claims he, she or it may have against the Issuing CA and the RA in the event of a dispute arising out of or in connection with the failure to fulfill the obligations of this subsection 2.1.4; HOWEVER, if the sole action of the Relying Party is the failure to consent to the application of the laws of the State of Washington for the reliance upon a certificate issued under this Policy, then the Relying Party will forfeit any claim in excess of that which would be permitted under Washington law.

2.2 LIMITATION ON LIABILITY

UNLESS OTHERWISE PROHIBITED BY FEDERAL LAW, OR OTHERWISE STIPULATED IN A RELYING PARTY AGREEMENT BETWEEN AN ISSUING CA AND THE RELYING PARTY, PARTIES THAT CHOOSE TO RELY ON ANY CERTIFICATE ISSUED UNDER THIS POLICY CONSENT TO THE LIMITATIONS OF LIABILITY ESTABLISHED BY WASHINGTON LAW AND THIS POLICY, REGARDLESS OF JURISDICTION, CHOICE OF LAW POLICIES, PLACE OF PERFORMANCE, DOMICILE OF PARTIES OR MINIMUM CONTACTS, INCLUDING THE FOLLOWING PROVISIONS WHICH PROVIDE THAT NEITHER AN ISSUING CA NOR ANY RA SHALL BE LIABLE:

2.2.1	Policy Compliance as a Defense	For any loss caused by reliance on a false or forged Certificate, if an Issuing CA or RA complied with all material requirements of this Policy;
2.2.2	Application of Recommended Reliance Limits	For any loss in excess of the Recommended Reliance Limits stated below that is caused by reliance upon a misrepresentation in a Certificate of a fact that an Issuing CA or any RA is required to confirm, or for any breach of the representations made by an Issuing CA and/or RA in this Policy, and/or for failure to comply with the requirements for issuance of a certificate under the laws of the State of Washington: • High Assurance Level Certificate – Recommended Reliance Limit: $50,000.00; • Intermediate Assurance Level Certificate – Recommended Reliance Limit: $10,000.00; and • Standard Assurance Level Certificate – Recommended Reliance Limit: $1,000.00.
2.2.3	No Personal Injury	For any damages for personal injury, pain and suffering, or emotional distress;
2.2.4	No Consequential Damages	For any consequential or incidental damages, to the greatest extent permitted by law; except as expressly permitted by section 2.2.2 above;
2.2.5	No Punitive Damages	For any punitive or exemplary damages, to the greatest extent permitted by law.
2.2.6	Apportionment of Damages	In any action based upon losses arising from or pertaining to the use or reliance upon Certificates issued under this Policy, any damages awarded shall be reduced as permitted by law by the extent of the fault attributable to the claimant(s), and damages

shall be awarded against a party only to the extent to which that party, or that party's employees, agents, or subcontractors, are found to be at fault in causing such damages. No defendant shall be deemed liable to pay damages for losses found to have been caused by another party.

2.3 FINANCIAL RESPONS-IBILITY

An Issuing CA and Authenticating RAs shall provide the following financial assurances:

2.3.1.1 Financial Assurance

2.3.1.1.1 An Issuing CA — An Issuing CA shall obtain and maintain a bond from a surety, and in the form and amount required for a licensed Certification Authority under Washington law.

2.3.1.1.2 Registration Authorities — An RA shall maintain adequate financial assurance in the form of a bond, guaranty, irrevocable letter of credit, and in the form and amount deemed appropriate by the Issuing CA.

2.3.1.2 Insurance

2.3.1.2.1 An Issuing CA — An Issuing CA shall at a minimum maintain the following insurance coverage, naming the State of Washington as an additional insured, which will cover the Issuing CA, the State, and their employees, officers, agents, subcontractors, designees, etc:

- Professional liability errors and omissions, with a deductible not exceeding twenty-five thousand dollars ($25,000.00), including coverage of not less than one million dollars ($1,000,000.00) per occurrence/two million dollars ($2,000,000.00) aggregate.

- Crime coverage with a deductible not to exceed one million dollars ($1,000,000.00), including coverage of not less than five million dollars single limit per occurrence/ten million dollars ($10,000,000.00) aggregate, covering occurrences in at least the following categories: computer fraud, forgery, money and securities, and employee dishonesty.

2.3.1.2.2 Registration Authorities — An Issuing CA may require that an RA maintains professional liability error and omissions and crime coverage insurance in adequate amounts and under terms consistent with the policy terms applicable to an Issuing CA, from an insurance company satisfactory to the Issuing CA.

2.3.1.3 Consequences of failure to meet Financial Responsibilities — The failure of an Issuing CA or RA to continuously maintain a required bond or insurance coverage may be the basis for revocation or suspension of its approval to participate in the issuance of Certificates and may also be the basis for revocation or suspension of Certificates previously issued.

2.3.1.4 Indemnification — Where applicable, an Issuing CA and any RA may seek compensation from another party to the PKI, if it can be shown that deliberate, wanton, or willful acts of the other party has caused the Issuing CA or RA loss, either financially or in reputation. However, the indemnification shall not relieve the CA or RA from its primary responsibilities to others who are not parties to the indemnification agreement.

2.3.1.4.1 Issuing CA — An Issuing CA may require RAs, and/or Subscribers, and may permit Relying Parties to enter into contracts, or may include provisions in its contracts with such parties,

		under which the RA, Subscriber and/or Relying Party agrees to indemnify, hold harmless and defend the Issuing CA against any claims arising from or pertaining to wrongful or negligent acts or omissions of the RA, Subscriber and/or Relying Party, as applicable.
2.3.1.4.2	Registration Authorities	An RA may enter into contracts, or include provisions in its contracts with Subscribers, under which Subscribers agree to indemnify, hold harmless and defend the RA against any claims arising from or pertaining to wrongful or negligent acts or omissions of the Subscriber.
2.3.2.2	Fiduciary relationships	Issuance of Certificates in accordance with this Policy does not make an Issuing CA or any RA, an agent, fiduciary, trustee, or other representative of Subscribers or Relying Parties.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1	Governing law	The laws of the United States of America and the State of Washington shall govern the enforceability, construction, interpretation, and validity of this Policy unless otherwise provided in an agreement between an Issuing CA and a Relying Party.
2.4.2	Specific Provisions: severability, survival, merger, and notice	An Issuing CA must ensure that any agreements by that CA will contain appropriate provisions governing severability, survival, merger or notice.
2.4.3	Dispute resolution procedures	In the event of any dispute or disagreement between two or more parties ("Disputing Parties") arising out of or pertaining to this Policy or related agreements, the Disputing Parties shall use their best efforts to settle the dispute or disagreement through negotiations in good faith following notice from one Disputing Party to the other(s). If the dispute is between the Issuing CA and an RA and pertains to the interpretation of this Policy, the party giving such notice shall at the same time submit the dispute to the PMA for resolution. In the event a party disputes an interpretation by the PMA, whether issued in connection with a dispute between two other parties or otherwise, the Disputing Party shall give notice of such dispute to the PMA, and the Disputing Party and the PMA shall use their best efforts to settle the dispute or disagreement through negotiations in good faith following notice from the Disputing Party to the PMA. If the Disputing Parties cannot reach a mutually agreeable resolution of the dispute or disagreement within sixty (60) days following the date of such notice or the date on which the PMA issues its interpretation or declines to make an interpretation (whichever is later, if applicable), then the Disputing Parties shall submit the dispute to binding arbitration to be conducted in accordance with the American Arbitration Association's rules for Commercial Arbitration. If the Arbitrator finds that the claim or defense of a party to a dispute is frivolous, fraudulent, or made with intent to harass, oppress, or delay, then the Arbitrator(s) has the discretion to award the other parties attorney fees and costs in connection with the claim or defense; otherwise, each party shall bear its own legal costs, and all parties shall pay a pro rata share of any fee payable to the arbitrator.

2.5 FEES

Notice of any fee charged to a Subscriber or Relying Party must be brought to the attention of that entity. Fees charged to entities governed by the Master Contract, will be in accordance with the fee structure set forth therein.

2.5.1	Certificate Issuance, Renewal, Suspension, and Revocation Fees	An Issuing CA and RAs may establish and charge a reasonable certificate issuance fee for providing identification, authentication, registration and certificate issuance services to potential Subscribers.
2.5.2	Certificate Access Fees	An Issuing CA may establish and charge a reasonable fee for providing certificate status information services.
2.5.3	Revocation Status Information Access Fees (Certificate Validation Services)	An Issuing CA may establish and charge a reasonable fee for providing certificate revocation information services.
2.5.4	Fees for Other Services such as Policy Information	The State, an Issuing CA and RAs may establish and charge other reasonable fees. However, no fee may be charged for access to review the provisions of this Policy.
2.5.5	Refund Policy	Any fees collected for certificate applications that are not approved shall be refunded.

2.6 NOTICE AND PUBLICATION

2.6.1	Publication of CA information	An Issuing CA shall cause the operation of a secure on-line Repository that is available to Relying Parties and that contains (1) issued Certificates that reference this Policy, (2) a Certificate Revocation List ("CRL") or on-line certificate status database, (3) the Issuing CA's Certificate for its CA Private Signing Key, (4) past and current versions of the Issuing CA's CPS, (5) a copy of this Policy, and (6) other relevant information relating to Certificates that reference this Policy.
2.6.2	Frequency of publication	Certificates are published following Subscriber acceptance procedure specified in Section 4.4. The CRL is published as specified in Section 4.9.
2.6.3	Access controls	An Issuing CA shall not impose any access controls on this Policy, the Issuing CA's Certificate for its CA Private Signing Key, and past and current versions of the Issuing CA's CPS. An Issuing CA may impose access controls on Certificates and Certificate status information, in accordance with provisions of this Policy.
2.6.4	Location	The location of publication will be one appropriate to the certificate-using community, in accordance with the total security requirements, and shall identify an X.500 directory and an LDAP interface.
2.6.5	Revocation Information	The sole source of information regarding the validity or revocation of a Certificate shall be that which is provided by the Issuing CA. Relying Parties may elect to rely on revoked Certificates, based on the reason for revocation, and information from other sources. Reliance on a revoked Certificate based upon information from another source or sources shall not be deemed “Reasonable Reliance” for purposes of this Policy. In order to support such an election, revocation reason codes may be provided through revocation mechanisms (e.g., the reason Code in an X.509 Version 2 CRL). In order to preserve trust in the PKI, the dissemination of information concerning the events

leading up to an investigation of a revocation may be limited to those involved.

2.7 COMPLIANCE AUDITS

2.7.1	Frequency	An Issuing CA shall submit to compliance audits applicable to licensed certification authorities under Washington law. This Policy makes no stipulation as to the exact frequency of such compliance inspections.
2.7.2	Identity and Qualifications of Auditor	Any auditor must be qualified to conduct a compliance audit under Washington law and must be sufficiently familiar with the Issuing CA's practices.
2.7.3	Auditor's Neutrality	The auditor(s) and CA must have a contractual relationship for the performance of the audit, and the auditor(s) shall be sufficiently separated organizationally from the Issuing CA to provide an unbiased, independent evaluation.
2.7.4	Scope of Audit	Audits shall be in scope and substance in compliance with the AICPA/CICA WebTrust Principles and Criteria for Certification Authorities and shall meet the requirements for licensure as a Certification Authority under Washington law.
2.7.5	Communication of Results	The results of any inspection or audit of the Issuing CA shall be reported to the Issuing CA, and filed with the State as required by Washington law.
2.7.6	Actions Taken as a Result of Audit	If an audit reports any material noncompliance with applicable law, this Policy or any other contractual obligations of an Issuing CA to the State, the Issuing CA with DIS approval shall develop a plan to cure such noncompliance. The State may recommend or identify remedies it desires in the course of development of such a plan. In the event the Issuing CA fails to take appropriate action in response to the inspection report, the State may proceed as provided in the Washington Administrative Code and/or remedies outlined in the Master Contract.

2.8 PRIVACY AND DATA PROTECTION POLICY

As described below, Certificates, and personal or corporate information appearing on them or in public directories, are not considered confidential. All other personal or corporate information held by an Issuing CA or an RA is considered confidential and shall be used only for the purpose of providing such CA Services and carrying out the provisions of this Policy. A Certificate should only contain information that is relevant and necessary to effect transactions with the Certificate.

2.8.1	Sensitivity of Types of Private Information.	
2.8.1.1	Private/Confidential Information	Information that is considered private and/or confidential or personally identifiable by this Policy must not be disclosed in any manner to any person without the prior consent of the Subscriber. Information collected will not be sold, rented, leased or disclosed in any manner to any person without prior express written consent of the Subscriber unless required by law or court order, except as provided herein or as may be necessary for the performance of CA Services.
2.8.1.1.1	Private Key Information	Digital Signature Private Keys shall be kept confidential. Any key information disclosure by a Subscriber is at the Subscriber's own risk. Any Private Key management keys held by an Issuing CA shall be held in strictest confidence. Under no

		circumstances shall any Private Key appear unencrypted outside the cryptographic module.
2.8.1.1.2	CA and RA Information	All information stored locally on an Issuing CA and RA equipment (not in the Repository) shall be handled as sensitive, and access shall be restricted to those with an official need-to-know in order to perform their official duties. Private Keys used to sign Certificates that will assert security privileges are classified at the same level as the privileges that are to be asserted. In any cases where an Issuing CA does not independently verify security privilege information, this requirement extends to RAs.
2.8.1.1.3	Audit Information	Audit information is to be considered sensitive and must not be disclosed to anyone for any purpose other than auditing or mandatory reporting purposes or where otherwise required by law.
2.8.1.2	Non-Private Information	Certificates and CRLs, and personal or corporate information appearing on them and in public directories, are not considered confidential. Information contained on a single Certificate or related status information shall not be considered confidential, when the information is used in accordance with the purposes of providing CA Services and carrying out the provisions of this Policy. Notwithstanding the above, the information contained in a Certificate may not be used by any Individual or Organization other than a Relying Party, and may only be used for purposes within the scope of this Policy. Information pertaining to CA management of Certificates, such as compilations of certificate information, shall be treated as confidential by any party subject to this Policy, and may only be disclosed by consent or as required by law or court order.
2.8.2	Permitted Acquisition of Private Information; Disclosure	An Issuing CA shall collect only such personal information about a Subscriber as is necessary for the issuance of a Certificate to the Subscriber. For the purpose of proper administration of Certificates, an Issuing CA or RA may request non-certificate information to be used in issuing and managing Certificates (e.g., identifying numbers, business or home addresses and telephone numbers). Collection of personal information may be subject to collection, maintenance, retention and protection requirements of state and federal law.
2.8.3	Permitted Use of Private Information by Acquirer.	Personal information collected for the purposes of Certificate issuance, maintenance and revocation shall only be used for such purposes. When the personal information includes a Social Security Number (SSN) in order to establish the identity of a Subscriber, the SSN will never be displayed in the Certificate and will be held in confidence by the CA.
2.8.4	Permitted Distribution of Private Information by Acquirer.	An Issuing CA or RA may distribute personal information with the Subscriber's express consent, or as required by law or court order.
2.8.5	Opportunity of Owner to Correct Private Information.	Information must be made available by an Issuing CA or RA to the Subscriber involved following an appropriate request by such Subscriber and must be subject to correction and/or revision by such Subscriber;
2.8.6	Release of Information to Law Enforcement Officials.	An Issuing CA will not disclose Certificate or Certificate-related information to any law enforcement agency, except when: (a) authorized by this Policy; (b) required to be disclosed by law, governmental rule or regulation, or court order; or (c) authorized by the Subscriber when necessary to effect an appropriate use of the Certificate. All

requests for disclosure of private and/or confidential information from a law enforcement agency must be made in accordance with applicable law.

2.8.7 Release of Information in Other Legal Proceedings. All requests for disclosure of private and/or confidential information for purposes of litigation must be made in writing, except where prohibited by law. An Issuing CA shall give all interested persons or parties reasonable prior written notice before making any disclosure of Certificate or Certificate-related information whose disclosure is required by law, governmental rule or regulation, court order or judicially-issued subpoena. Non-disclosure of confidential information shall remain an obligation notwithstanding the status of a Certificate (current or revoked) or the status of the Issuing CA.

2.8.8 Other information releases An Issuing CA may not disclose private and/or confidential information, unless it obtains the Subscriber's express consent.

2.9 INTELLECTUAL PROPERTY RIGHTS

The Private Key shall be treated as the sole property of the legitimate holder of the corresponding Public Key identified in a Certificate. This Certificate Policy and its OID are the property of the State and may be used by an Issuing CA as provided in the Master Contract, and/or in accordance with the provisions of this Policy. Any other use of the above without the express written permission of the State is expressly prohibited.

2.10 VALIDITY OF CERTIFICATES

2.10.1 Acceptance. The act of acceptance of a Certificate by a Subscriber shall be logged by the Issuing CA and may consist of a record made when the Certificate subject downloads the Certificate. Such act shall be recorded and maintained in an auditable trail kept by the Issuing CA in a trustworthy manner that comports with industry standards and any applicable laws.

2.10.2 Operational Period. Unless accepted or waived by a Relying Party, after its expiration date an expired Certificate may no longer be used for purposes of authentication, signing and non-repudiation.

2.10.3 Validity of Actions During Operational Period and Legal All Relying Parties' Digital Signature verification applications must be able to verify that the Digital Signature was created during the Certificate's operational period.

2.10.4 Revocation After a Certificate has been revoked or expired, a party may elect to rely on a revoked or invalid Certificate, based on surrounding circumstances; and information from other sources. However, an Issuing CA is not liable for such reliance, and Relying Parties rely on the Certificate at their own risk.

3 IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

An Issuing CA shall establish trustworthy procedures whereby RAs may be authenticated by the Issuing CA and issued a Certificate (collectively, such RAs shall be called "Authenticating RAs"). An Authenticating RA may designate one or more Individuals as its agent(s) to conduct registration activities, and authorize them to represent the RA in connection with the issuance and revocation of Certificates for Subscribers. The Issuing CA may rely on such designated individual(s) appointed by the Authenticating RA to properly authenticate individual applicants. The Authenticating RA and its agents shall require proof of identity, as required in this Part 3 of the Policy.

Subject to the requirements noted below, Certificate applications may be communicated from the applicant to an Issuing CA or an Authenticating RA (and authorizations to issue Certificates may be communicated from an Authenticating RA to an Issuing CA) electronically via e-mail or a web site, provided that all communication is secure, such as by using SSL or a similar security protocol, by first class U.S. mail, or in person.

When an applicant registers his or her information with an Issuing CA and a Subscriber account is created, a GUID is associated with the Subscriber's account. A Subscriber's account GUID shall remain the same as long as the Subscriber renews the Certificate with the Issuing CA as provided in Section 3.2, or if the Issuing CA elects to revoke and re-issue a certificate in lieu of suspension.

3.1.1 Types of names

The subject name used for Certificates shall be the Subscriber's authenticated common name. Each Subscriber must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the Certificate Subject Name field and in accordance with PKIX Part 1. Each Subscriber may use an alternative name via the Subject Alternate Name field, which must also be in accordance with PKIX Part 1. The DN must be in the form of a X.501 printable string and must not be blank.

3.1.2 Need for names to be meaningful

The contents of each Certificate Subject and Issuer Name field must have an association with the authenticated name of the Subscriber. In the case of Individuals the authenticated common name should be a combination of first name, surname, and optionally initials. The DN may also include an organizational position or role. In the case of other entities the DN will reflect the authenticated legal name of the Subscriber. Where a Certificate refers to a role or position, the Certificate must also contain the identity of the person who holds that role or position. A Certificate issued for a device or application must include the authenticated name of the application and/or name of the person or organization responsible for that device or application.

3.1.3 Rules for interpreting various name forms

An Issuing CA may defer to a naming authority for guidance on name interpretation and subordination.

3.1.4 Uniqueness of names

The Subject Name listed in a Certificate shall be unambiguous and unique for all Certificates issued by an Issuing CA and conform to X.500 standards for name uniqueness. Additional numbers or letters must be appended to the real name to ensure the name's uniqueness within the domain of Certificates issued by an Issuing CA, and conform to the definition of the GUID attached hereto and incorporated herein by reference. No wildcard name forms are allowed. Each name shall be unique and for a single unique entity.

3.1.5	Name claim dispute resolution procedure	An Issuing CA shall be the final authority with respect to all decisions regarding Subscriber names in Certificates it issues. If necessary, a party requesting a Certificate may be required to demonstrate its right to use a particular name. The Issuing CA shall investigate and correct if necessary any name collisions brought to its attention. If appropriate, the Issuing CA shall coordinate with and defer to the appropriate naming authority.
3.1.6	Recognition, authentication, and role of trademarks	No Subscriber is guaranteed that its name will contain a trademark, trade name, corporate name or other specific referential material, though the Issuing CA may attempt to accommodate such requests. The Issuing CA shall not knowingly allow an entity to hold a name that a civil court has determined it has no right to use; provided that the Issuing CA has no obligation to make any inquiry or investigation into the existence or validity or such an order, or the status of any trademark and is not required to revoke and re-issue such a name to the rightful owner if it has already issued one sufficient for identification within the PKI.
3.1.7	Method to prove possession of Private Key	Subscribers are required to prove possession of the Private Key corresponding to the Public Key in a certificate request. For Signature Keys, this may be done by signing the request. An Issuing CA shall establish that the applicant is in possession of the Private Key corresponding to the Public Key submitted with the application in accordance with an appropriate secure protocol selected by the Issuing CA with the State's approval. Prior to the issuance of a Certificate, the Subscriber will confirm its identity through the use of appropriate secure protocol selected at the Issuing CA's discretion in consultation with the State. For Encryption Keys, an Issuing CA or Authenticating RA may encrypt the Subscriber's Certificate in a confirmation request message. The Subscriber can then decrypt and return the Certificate to the Issuing CA or RA in a confirmation message. Other mechanisms may also be acceptable. In the case where the Private Key is generated directly on a hardware token or smart card, or in a key generator that benignly transfers the Key to the token or smart card, then the Subscriber is deemed to be in possession of the Private Key at the time of generation or transfer. If the Subscriber is not in possession of the token or smart card when the Key is generated, then the token or smart card shall be delivered immediately to the Subscriber via a trustworthy and accountable method (see Section 6.1.2).
3.1.8	I&A Procedures	Acceptable I&A for High Certificates issued under this Policy shall consist of confirmation of identification information by an identify proofing process that incorporates at least two (2) of the following currently-valid individual identity items cross-checked by Third Party Identity Proofing for consistency, provided that at least one item of identification must be a photo ID issued as a result of an antecedent, personal appearance before a Government Agency. Acceptable forms of photo ID include: • Driver's license with photo; • Official photo ID issued by any state; • U.S. passport with photo; and

- Military ID with photo.

Other forms of acceptable identification include:

- Voter registration card;
- Birth certificate notarized or certified by an authorized public entity;
- Alien registration card;
- Major credit card;
- Employee identification card, including employer name and street address;
- Social security number; and
- Utility bill with matching name and address.

Additional procedures required for I&A for each Certificate Type are as follows:

3.1.8.1 High Assurance Level Certificates

High Assurance Level Certificates may only be issued after I&A conducted either:

- By (a) in-person appearance of an individual applying to become a Subscriber before a Licensed Notary or Operative Personnel of the Issuing CA, including (b) presentment of identification documentation as prescribed above, (c) written attestation by the Licensed Notary or Operative Personnel of the review and acceptance of such identification documentation, including attached photocopies of the documentation reviewed, and (d) acceptable confirmation by Third Party Identity Proofing by the Issuing CA; or
- By alternative procedures which produce an equivalent assurance as determined by DIS with guidance from the PMA.

3.1.8.1.1 Individual — See above.

3.1.8.1.2 Organizations — • No stipulation.

3.1.8.1.3 Electronic Device — No High Assurance Certificate may be issued for an Electronic Device.

3.1.8.2 Intermediate Assurance Level Certificates — An Intermediate Assurance Level Certificate may be issued by an Issuing CA based on I&A Procedure applicable to High Assurance Level Certificates or upon I&A using online Registration and Third Party Identity Proofing.

3.1.8.2.1 Individual — See above.

3.1.8.2.2 Organization — No stipulation.

3.1.8.2.3 Electronic Device — An Intermediate Assurance Level Certificate may be issued for an Electronic Device as provided in section 3.1.9.

3.1.8.3 Standard Assurance Level Certificates — A Standard Assurance Level Certificate may be issued by any I&A Procedure applicable to High or Intermediate Assurance Level Certificates, and may also be issued using online Registration and Third Party Identity Proofing.

3.1.8.3.1	Individual	See above.
3.1.8.3.2	Organization	No stipulation.
3.1.8.3	Electronic Device	A Standard Assurance Level Certificate may be issued to an Electronic Device as provided in Section 3.1.9.
3.1.9	Electronic Devices	A certificate request identifying an Electronic Device as the subject of a Certificate may be made by an approved Subscriber for whom the Electronic Device's signature is attributable for the purposes of accountability and responsibility. Identification and Authentication of the applicant must follow this Policy's requirements as if the Subscriber was applying for the Certificate on its own behalf.

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY

3.2.1	Certificate re-key	Within three months prior to the scheduled expiration of the operational period of a Certificate issued following authentication under this Policy, a Subscriber may request issuance of a new Certificate for a new Key Pair from the Issuing CA that issued the original Certificate, provided the original Certificate has not been suspended or revoked. The Subscriber's account GUID must remain unchanged and the same GUID appear in the subsequent Certificate. Such a request may be made electronically via a digitally signed message based on the old Key Pair in the original Certificate. Renewal of an affiliated individual shall require verification that the affiliation still exists. Such verification of affiliation shall be the same as that required for a new application.
3.2.2	Certificate renewal	Renewing a Certificate means creating a new Certificate with the same name, and authorizations as the old one, but referencing a new key pair, extended validity period and a new serial number. As with Certificate Re-keying, the Subscriber's account GUID must remain unchanged and appear in the new Certificate. A Certificate may be renewed if the Public Key has not reached the end of its validity, the Private Key has not been compromised, and the user name and attributes are correct.
3.2.3	Certificate update	Updating a Certificate means creating a new Certificate that has a different key, a different serial number, and differs in one or more other fields, from the old Certificate. The updated Certificate must be manufactured using the same GUID as the current existing Certificate when presented to the Issuing CA by the Subscriber with the update request.

3.3 RE-KEY AFTER REVOCATION

Revoked or expired Certificates shall not be renewed. Applicants without a valid Certificate from an Issuing CA that references this Policy shall be re-authenticated by an Issuing CA or on certificate application, just as with a first-time application, except if an Issuing CA chooses to revoke in lieu of suspension in which case the newly issued Certificate will contain the same GUID.

3.4 REVOCATION REQUEST

A certificate revocation request that is submitted electronically may be authenticated on the basis of a Digital Signature using the Certificate's associated Key Pair. The identity of the person submitting a revocation request in any other manner shall be authenticated in accordance with Section 3.1. Revocation requests authenticated on the basis of the Certificate's associated Key Pair shall always be accepted as valid. Other revocation request authentication mechanisms may be used as well, including a request in writing signed by the Subscriber and sent via U.S. Postal Service first-class mail, or equivalent. These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to quickly revoke Certificates.

4 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE REQUEST

It is not the intent of this Policy to impose implementations on an Issuing CA or Subscribers, but to identify the required information and procedures that constitute assurance and support trust in the PKI. The following procedures satisfy the security requirements of this document. The following steps are required when applying for a Certificate: establish identity of subject as provided above; obtain a Public/Private Key Pair for each Certificate required; prove to the Issuing CA that the Public Key forms a functioning Key Pair with the Private Key held by the user as provided above; provide a point of contact for verification of any roles or authorizations requested.

4.1.1	Who Can Request a Certificate	An applicant for a Certificate shall complete a certificate application in a form prescribed by the Issuing CA and enter into a Subscriber agreement with the Issuing CA. All applications are subject to review, approval and acceptance by the Issuing CA. The certificate application process may be initiated by the persons identified in Section 3.1.
4.1.2	Certificate Request Process	An applicant for a Certificate shall complete a certificate application and provide requested information in a form prescribed by the Issuing CA and this Policy.
4.1.3	Time to Process a Certificate Request	See Section 2.1.1.3, above.
4.1.4	Application for Cross-certificate	DIS, in consultation with an Issuing CA will specify procedures to apply for a cross-certificate. Procedures and policies for application and administration of cross-certificates shall be established through the amendment of this Policy.

4.2 CERTIFICATE APPLICATION VALIDATION

No stipulation

4.3 CERTIFICATE ISSUANCE

4.3.1	Applicant Notification	Upon successful completion of the Subscriber I&A process in accordance with this Policy, and complete and final approval of the certificate application, the Issuing CA shall issue the requested Certificate, notify the applicant thereof, and make the Certificate available to the applicant pursuant to a procedure whereby the Certificate is initially delivered to, or available for pickup by, the Subscriber only. The Issuing CA will not issue a Certificate without the consent of the applicant and, if applicable, the applicant's sponsor.
4.3.2	Issuance by CA	An Issuing CA or Authenticating RA shall use an Out-of-Band notification process linked to the Certificate applicant's physical U.S. postal mail address, or equivalent, and deliver the Certificate only to the Subscriber.
4.3.3	Notification of Certificate Issuance to Subscribers	After successful validation of the Certificate application and issuance of the Certificate, the Issuing CA must notify the Subscriber in a trustworthy and confidential manner that the Certificate has been issued.

4.4 CERTIFICATE ACCEPTANCE

Acceptance is the action by a Subscriber that triggers the Subscriber's duties and potential liability, and constitutes acceptance of this Policy and the terms of any applicable CPS and agreement incorporating this Policy. The Issuing CA may define, in its CPS, a technical or procedural mechanism to explain the Subscriber responsibilities defined in section 2.1.3; inform the Subscriber of the creation of a Certificate and the contents of the Certificate; and require the Subscriber to indicate acceptance of the responsibilities and the Certificate. The ordering of this process, and the mechanisms used, will depend on factors such as where key is generated and how Certificates are posted. For instance, a Subscriber may agree to its responsibilities at the same time that it accepts the Certificate, or agreeing to its responsibilities may be a precondition for requesting a Certificate.

4.4.1	Certificate Acceptance by the Subscriber	As described in this Policy, a condition to issuing the Certificate, the Subscriber shall indicate acceptance or rejection of the Certificate to the Issuing CA and acknowledge the Subscriber obligations under Section 2.1.3. By accepting the Certificate, the Subscriber is warranting that all information and representations made by the Subscriber that are included in the Certificate are true.
4.4.2	Notification of Certificate Issuance to Others	Notification of certificate issuance to others may be effectuated by publication of the Certificate in a recognized repository.

4.5 Certificate Usage

The issuing CA assumes no responsibility for the use of or reliance upon Certificates except as provided under this Policy.

4.6 Routine Certificate Renewal

Routine certificate renewal may be performed by automatic renewal or re-certifying, and must create a new Key Pair.

4.7 Processing a Request for a New Key

4.7.1	Circumstances for Request of a New Key Certification	In the event that Out-of-Band processes (e.g. a Shared Secret) remain in place to authenticate the Subscriber requesting new key certification, the Issuing CA is not required to re-perform completeI&A of the Subscriber.
4.7.2	Who can request Certification of a New Key	Only the Subscriber may request certification of a new key.
4.7.3	Treatment of a Request for Certification of a New Key	Complete re-authentication of a Subscriber by performing the I&A identified in Section 3.1 is not required if out-of-band processes remain in place to authenticate the requester, including for example, the use of a shared secret or bio-metric means of identity verification.
4.7.4	Notification of Certification Request for a New Key to Subscriber	The notification procedures used by the Issuing CA or Authenticating RA should be the same as with a new Subscriber request.

4.8 Certificate Modifications

No Stipulation.

4.9 Certificate Revocation

4.9.1	Circumstances for Revocation Permissive Revocation	A Subscriber may request revocation of a Certificate at any time for any reason. A Sponsoring Organization may, where applicable, request revocation of an affiliated individual Certificate at any time for any reason. An Issuing CA may also revoke a Certificate upon failure of the Subscriber (or any sponsoring organization, where applicable) to meet its obligations under this Policy, the applicable CPS, or any other agreement, regulation, or law applicable to the Certificate that may be in force. This includes revoking a Certificate when a suspected or known compromise of the Private Key has occurred.
	Required Revocation	A Subscriber, or a Sponsoring Organization (where applicable) shall promptly request revocation of a Certificate: whenever the name on the Certificate is no longer current, complete or true ; whenever the Private Key, or the media holding the Private Key, associated with the Certificate is known or suspected of being lost, disclosed, compromised or subjected to unauthorized use in any way, or; whenever an affiliated Individual is no longer affiliated with a Sponsoring Organization. An Issuing CA shall revoke a Certificate: upon request of the Subscriber or Sponsoring Organization; upon failure of the Subscriber (or the Sponsoring Organization, where applicable) to meet its material obligations under this Policy, any applicable CPS, or any other agreement,

		regulation, or law applicable to the Certificate that may be in force; if knowledge or reasonable suspicion of compromise is obtained; if the Issuing CA determines that the Certificate was not properly issued in accordance with this Policy and/or any applicable CPS.
4.9.2	Who Can Request Revocation	An Issuing CA may summarily revoke Certificates within its domain, provided that notice and cause are given. An RA can request the revocation of a Subscriber's Certificate on the Subscriber's behalf, the Subscriber's Sponsoring Organization, or other authorized party. The Subscriber is authorized to request the revocation of his or her own certificate, as is the Subscriber's Sponsoring Organization.
4.9.3	Procedure for Revocation Request	As described in this Policy, a certificate revocation request should be promptly communicated to the Issuing CA, either directly or through the Authenticating RA authorized to accept such notices on behalf of the Issuing CA. A certificate revocation request may be communicated electronically if it is digitally signed with the Private Key of the Subscriber or the Sponsoring Organization (where applicable). Alternatively, the Subscriber, or Sponsoring Organization (where applicable), may request revocation by contacting the Issuing CA or its Authenticating RA in person and providing adequate proof of identification in accordance with this Policy, or an equivalent method.
	Revocation Request Grace Period	An Issuing CA shall revoke a Certificate as quickly as practical upon receipt of a proper revocation request, and shall always revoke Certificates within the time constraints described in this Section 4.9. Notwithstanding the foregoing, a grace period of three (3) hours shall exist between the time a Subscriber makes a revocation request and the time a Certificate is revoked.
	Suspension	A Certificate may be placed in suspended status following an unsigned request for certificate revocation, pending authentication of the revocation request.
4.9.4	Time to Process a Revocation Request	Promptly following revocation of a Certificate, the CRL or certificate status database in the Repository, as applicable, shall be updated. All revocation requests and the resulting actions taken by the Issuing CA shall be archived. Certificates may be revoked prior to their expiration. Revocation is effected by notation or inclusion in a set of revoked certificates or other directory or database of revoked certificates.
4.9.5	Certificate Revocation Lists	
4.9.5.1	CRL Issuance Frequency	CRLs shall be issued daily, even if there are no changes or updates to be made, to ensure timeliness of information. CRLs may be issued more frequently than required; if there are circumstances under which the Issuing CA will post early updates, these shall be spelled out in a CPS. The Issuing CA shall ensure that superceded CRLs are removed from the directory system upon posting of the latest CRL. A CRL shall be issued with a validity period of no more than four weeks. If a CRL is being issued as a result of a key compromise or revocation, the CRL must be posted as quickly as feasible, but shall be posted no later than six hours after notification of the compromise or decision to revoke by the Issuing CA. CAs shall make public the details of certificate revocation information posting, 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 Relying Parties.

4.9.5.2	CRL Latency	Interim CRLs will be made available to Relying Parties.
4.9.6	On-line Revocation/Status Checking	Whenever an on-line certificate status database is used as an alternative to a CRL, such database shall be updated and checked according to the same requirements as defined for a CRL.
	Online Revocation/Status Checking Availability	Issuing CAs shall validate online, near-real-time the status of the Certificate indicated in a Certificate validation request message.
	Online Revocation Checking Requirements	Each Relying Party will validate every Certificate it receives in connection with a transaction, in accordance with and by the means identified in the Certificate.
	Other Forms of Revocation Advertisements Available	An Issuing CA may also use other methods to publicize revoked Certificates.

4.10 Certificate Status Services

See 4.9.6

4.11 End of Subscription

If an Individual's or Organization's subscription to the PKI ends prior to the expiration of any Certificates issued under that subscription, the Issuing CA shall revoke any unexpired Certificates issued or held under the subscription.

4.12 Private Key Recovery

Under no circumstances will a Private Signing Key be stored for purposes of recovery by a CA. If a Key Pair is used for both signature and confidentiality purposes, recovery of the Private Key is prohibited.

5 CA FACILITY AND MANAGEMENT CONTROLS

5.1 Physical Controls

An Issuing CA, and all RAs, CMAs and Repositories, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing CA Services. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in the Section on Procedural Controls (5.2.1). Access shall be controlled through the use of electronic access controls, mechanical combination locksets, or deadbolts. Such access controls must be manually or electronically monitored for unauthorized intrusion at all times.

5.1.1 Site location and construction

Any Issuing CA site must:

- Satisfy at least the requirements for a Security Zone;
- Be manually or electronically monitored for unauthorized intrusion at all times;
- Ensure that access to the Issuing CA server is limited to those personnel identified on an access list, and implement dual access control requirements to

the Issuing CA server for such personnel;

- Ensure personnel not on the access list are properly escorted and supervised;
- Ensure a site access log is maintained and inspected periodically; and
- Ensure all removable media and paper containing sensitive plain text information are stored in containers either listed in, or of equivalent strength to those listed in, the Security Equipment Guide.
- Additionally, the location of the Issuing CA server must satisfy at least the requirements for a High-Security Zone.

All Authenticating RA sites must be located in areas that satisfy the controls required for a Reception Zone. If an Authenticating RA workstation is used for on-line entity management with the Issuing CA, the workstation must be located in either:

- A Security Zone; or
- An Operations Zone while attended, with all media security protected when unattended.

The Issuing CA must ensure that the operation of the Authenticating RA's site provides appropriate security protection of the cryptographic module, all system software and Private Keys. The Issuing CA must conduct a threat and risk assessment of any such site. Security must include but may not be limited to:

- Storage of the cryptographic module and the RA Administrator's Private Key should in a secure container or safe.
- Recording of PINs or passwords only in security containers accessible only to designated personnel.
- Employees of Authenticating RAs must not leave their workstations unattended when the cryptography is in an unlocked state (i.e., when the PIN or password has been entered).
- A workstation that contains Private Keys on a hard drive must be physically secured or protected with an appropriate access control product.
- Hardware cryptomodules must be protected physically, which may be done through site protection.

5.1.2 Physical access

CA equipment shall always be protected from unauthorized access. Authenticating RA equipment shall be protected from unauthorized access while the cryptomodule is installed and activated. The Authenticating RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptomodule is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the Authenticating RA equipment environment. For example, Authenticating RA equipment in facilities with controlled access occupied primarily by security personnel will not require an additional layer of controlled access surrounding inactivated Authenticating RA equipment. Authenticating RA equipment in less secure environments will require additional protection, such as being located in a room that is kept locked when the Authenticating RA is not present. Removable CA cryptomodules shall be inactivated and placed in locked containers sufficient for

housing equipment commensurate with the classification, sensitivity, or value level of the information being protected by the certificates issued. Any activation information used to access or enable the cryptomodule or CA equipment shall be stored separately. Such information should be memorized and not written down. If such material is written down it must be securely stored in a locked container.

A security check to the facility housing CA equipment shall occur at least once every 24 hours. The check should ensure that: the equipment is in a state appropriate to the current mode of operation (e.g., that cryptomodules and removable hard disks are in place when "open", and secured when "closed"); any security containers are properly secured; physical security systems (e.g., door locks, vent covers) are functioning properly; and the area is secured against unauthorized access. A role or person shall be made explicitly responsible for making such checks. When a role is responsible, a log identifying the individual performing such a check shall be maintained. A record shall be kept that describes the type of checks performed, the time, and the person who performed them. If the CA equipment is located in a continuously attended facility, there shall be a security check once per shift. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that asserts that the facility entrance door is locked and that, where installed, intrusion detection systems are activated. If the facility housing the CA equipment will be unattended for periods greater than 24 hours, it shall be protected by an intrusion detection system. Additionally, a check shall be made at least once every 24 hours to ensure that all doors to the facility are locked and there have been no attempts at forceful entry.

5.1.3	Power and air conditioning	The facility, which houses Issuing CA equipment, shall be supplied with power and air conditioning sufficient to create a reliable operating environment. In addition, personnel areas within the facility must be supplied with sufficient utilities to satisfy operational, health, and safety needs. The actual quantity and quality of utility service will depend on how the facility operates, e.g., its times of operation (24 hours/7 days or 8 hours/5 days), or whether on-line certificate status checking is provided. The Issuing CA equipment shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Users with needs for long operation hours or short response times may contract with the Issuing CA for additional requirements for backup power generation. The revocation mechanisms shall be supported by uninterruptable power supplies and sufficient backup power generation.
5.1.4	Water exposures	This Policy makes no stipulation on prevention of exposure of CA equipment to water beyond that called for by best business practice. CA equipment shall be installed such that it is not in danger of exposure to water, e.g., on tables or elevated floors. Moisture detectors shall be installed in areas susceptible to flooding. CA operators who have sprinklers for fire control shall have a contingency plan for recovery should the sprinklers malfunction, or cause water damage outside of the fire area.
5.1.5	Fire prevention and protection	This Policy makes no stipulation on prevention of exposure of CA equipment to fire beyond that called for by best business practice. An automatic fire extinguishing system shall be installed in accordance with local code. An Issuing CA shall have a contingency plan, which accounts for damage by fire.
5.1.6	Media storage	Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be stored in a location separate from the Issuing CA equipment.
5.1.7	Waste disposal	Normal office waste shall be removed or destroyed in accordance with best business

practices. Media used to collect or transmit information discussed in section 2.8 shall be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8	Off-site backup	System backups, sufficient to recover from system failure, shall be made on a periodic schedule, described in the CPS. At least one backup copy shall be stored at an offsite location (separate from the Issuing CA equipment). Only the latest backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

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. The people selected to fill these roles must be careful and above reproach as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. First is to design and configure the technology to avoid mistakes and prohibit inappropriate behavior. Second is to distribute the functions among several people, so that any malicious activity requires collusion. The primary trusted roles defined by this Policy are the Issuing CA and the Authenticating RA. Other trusted roles may be defined in other documents, which describe or impose requirements on the Issuing CA's operation.
5.2.1.1	Certification Authority (CA)	All Certificates asserting this Policy must be issued by CA facilities operating under the direct control of an Issuing CA. The responsible individual or body (e.g., board of directors) identified as operating the CA facilities must be named, and made available during compliance audits. Any CA who asserts a policy identifier defined in this document is subject to the stipulations of this Policy. An Issuing CA's role and the corresponding procedures an Issuing CA will follow shall be defined in detail in a Certification Practices Statement (CPS), and may be further described in a Concept of Operations (CONOP) and procedural handbook. Primarily, an Issuing CA's responsibilities are to ensure that the following functions occur according to the stipulations of this Policy: certificate generation and revocation; posting Certificates and CRLs; performing the daily incremental database backups; administrative functions such as compromise reporting and maintaining the database; hardware cryptomodule programming and management.
5.2.1.2	Registration Authority (RA)	Any RA which operates under this Policy is subject to the stipulations of this Policy and of the Registration Authority Agreement it has with an Issuing CA. Primarily, an RA's responsibilities are: verifying identity, either through personal contact, or via agents, when allowed by this Policy; entering user information, and verifying correctness; securely communicating requests to and responses from the Issuing CA; receiving and distributing Subscriber Certificates. The responsibilities and controls for RAs shall be explicitly described in a Registration Authority Agreement with the Issuing CA.
5.2.2	Number of Persons Required per Task	An Issuing CA shall utilize commercially reasonable practices to ensure that one Individual acting alone cannot circumvent safeguards.

To ensure that one Individual acting alone cannot circumvent safeguards, responsibilities at the Issuing CA server should be shared by multiple roles and Individuals. Each account on the Issuing CA server shall have limited capabilities commensurate with the role of the account holder.

An Issuing CA must ensure that no single Individual may gain access to Subscriber Private Keys stored by the Issuing CA. At a minimum, procedural or operational mechanisms must be in place to perform a key recovery, preferably using a split-knowledge technique, such as two Individuals each with a separate password, to prevent the disclosure of the encryption key to an unauthorized individual. Multi-user control is also required for CA key generation as outlined in 6.2.2. All other duties associated with CA roles may be performed by an individual operating alone. An Issuing CA must ensure that any verification process it employs provides for oversight of all activities performed by privileged CA role holders.

To best ensure the integrity of Issuing CA equipment and operation, it is recommended that wherever possible a separate individual be identified for each trusted role. The separation provides a set of checks and balances over the Issuing CA operation. Under no circumstances shall the incumbent of a CA role perform its own auditor function.

5.2.3	Identification and Authentication for Each Role	All CA personnel must have their identity and authorization verified before they are: included in the access list for the Issuing CA site; included in the access list for physical access to the Issuing CA system; given a certificate for the performance of their CA role; given an account on the PKI system. Each of these Certificates and accounts (with the exception of CA signing Certificates) must: be directly attributable to an individual; not be shared; be restricted to actions authorized for that role through the use of CA software, operating system and procedural controls. CA operations must be secured, using mechanisms such as token-based strong authentication and encryption, when accessed across a shared network.

5.3 Personnel Controls

5.3.1	Background Qualifications Experience and Clearance Requirements	CAs, RAs, CMAs, and Repositories shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in manner consistent with this Policy. These policies shall include the certification of all appropriate personnel as “Operative Personnel” as required by Washington law.
5.3.2	Background Check Procedures	CAs shall conduct an appropriate investigation of all personnel who serve in trusted roles (prior to their employment and periodically thereafter as necessary), to verify their trustworthiness and competence in accordance with the requirements of this Policy and CA's personnel practices or equivalent. All personnel who fail an initial or periodic investigation shall not serve or continue to serve in a trusted role.
5.3.3	Training Requirements	An Issuing CA must ensure that all personnel performing duties consistent with the duties of Operative Personnel under Washington law for an Issuing CA and Authenticating RAs must receive: comprehensive training in the Issuing CA/Authenticating RA security principles and mechanisms; security awareness; all PKI software versions in use on the Issuing CA system; all PKI duties they are expected to perform; and disaster recovery and business continuity procedures.

5.3.4	Retraining Frequency and Requirements	The requirements of 5.3.3 must be kept current to accommodate changes in an Issuing CA system. Refresher training must be conducted as required, and an Issuing CA must review these requirements at least once a year.
5.3.5	Job Rotation Frequency and Sequence	This Policy makes no stipulation regarding frequency or sequence of job rotation. Local policies, which do impose requirements, shall provide for continuity and integrity of the PKI service
5.3.6	Sanctions for Unauthorized Actions	In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of an Issuing CA or Authenticating RA, an Issuing CA may suspend his or her access to the Issuing CA system.
5.3.7	Contracting Personnel Requirements	CA must ensure that contractor access to the Issuing CA site is in accordance with 5.1.1.
5.3.8	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 Security Audit Procedures

5.4.1	Types of Event Recorded	Issuing CA equipment shall be able to record events related to the server (installation, modification, accesses), and the application (requests, responses, actions, publications, and error conditions). Events may be attributable to human action (in any role) or automatically invoked by the equipment. At a minimum, the information recorded shall include the type of event, and the time the event occurred. In addition, for some types it will be appropriate to record the success or failure, the source and destination of a message, or the disposition of a created object (e.g., a filename). Where possible, the audit data shall be automatically collected; when this is not possible a logbook, paper form, or other physical mechanism shall be used. The auditing capabilities of the underlying equipment operating system shall be enabled during installation. A record shall be kept of file manipulation and account management. These events shall also be recorded during normal operation of the Issuing CA equipment.
5.4.2	Frequency of Processing Log	An Issuing CA must ensure that its audit logs are reviewed by CA personnel at least weekly and all significant events are explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Supporting manual and electronic logs from the Issuing CA and Authenticating RA should be compared where any action is deemed suspicious. Actions taken following these reviews must be documented.
5.4.3	Retention Period for Audit Log	The information generated on Issuing CA equipment shall be kept on the Issuing CA equipment until the information is moved to an appropriate archive facility. Deletion of the audit log from the Issuing CA equipment shall be performed by a person other than the CA Operator. This person shall be identified in the Issuing CA's CPS. Audit logs shall be retained as archive records in accordance with section 5.5.2.
5.4.4	Protection of Audit Log	The audit log, to the extent possible, will not be open for reading or modification by any human, or by any automated process other than those that perform audit

processing. Any entity that does not have modification access to the audit log may archive it (note that deletion requires modification access). Weekly audit data shall be moved to a safe, secure storage location separate from the Issuing CA equipment.

5.4.5 Audit Log Backup Procedures — Audit logs and audit summaries must be backed up or copied if in manual form.

5.4.6 Audit Collection System (internal vs external) — There is no requirement for the audit log collection system to be external to Issuing CA equipment. The audit process shall run independently and shall not in any way be under the control of the CA Operator. Audit processes will be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, the Issuing CA operation shall cease until the audit capability can be restored. If it is unacceptable to cease CA operation, other means shall be employed to provide audit capability that has been previously arranged with the Issuing CA's auditor.

5.4.7 Notification To Event-Causing Subject — Where an event is logged by the audit collection system no notice need be given to the individual, organization, device or application which caused the event.

5.4.8 Vulnerability Assessments — Events in the audit process are logged, in part, to monitor system vulnerabilities. The Issuing CA must ensure that a vulnerability assessment is performed, reviewed and revised following an examination of these monitored events.

5.5 Records Archival

5.5.1 Types of Event Recorded — CA archive records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following data shall be recorded and archived:

5.5.1.1 Certificate Issuance

(a) Applicant's name as it appears in the certificate's "Common Name" field, which may contain additional numbers or letters appended to the common name to ensure the name's uniqueness within the domain of Certificates issued by the Issuing CA

(b) Method of application (i.e., on-line, in-person, etc.)

(c) For each data element accepted for proofing, including electronic forms:

(1) Name of document presented for identity proofing
(2) Issuing authority
(3) Date of issuance
(4) Date of expiration
(5) All fields verified
(6) Source of verification (i.e., which databases used for cross-checks)
(7) Method of verification (i.e., on-line, in-person)
(8) Date/time of verification

(d) Name of the Authenticating RA

(e) All associated error messages and codes

(f) Date/time of process completion

(g) Date/time of certificate download/acceptance

5.5.1.2 Certificate Validation

(a) Certificate serial number

(b) Certificate status with reason code

(c) All associated error messages and codes

(d) Date/time of all certificate validation requests

(e) Date/time of transmission of certificate status request responses

5.5.1.3 Certificate Revocation

(a) Date/time

(b) Name of the Authenticating RA

(c) Subscriber's common name, which may contain additional numbers or letters appended to the common name to ensure the name's uniqueness within the domain of Certificates issued by the Issuing CA

(d) Reason code for revocation request

(e) Certificate serial number

(f) All associated verification request and revocation data

5.5.1.4 Certificate Renewal

(a) Certificate serial number

(b) Certificate common name, which may contain additional numbers or letters appended to the common name to ensure the name's uniqueness within the domain of Certificates issued by the Issuing CA

(c) New operational period dates

(d) Date/time of completion of renewal process

(e) All associated renewal data

5.5.2 Retention Period for Archive

Archive records shall be kept for a period of at least seven years, and six months following the date of any recorded event or the last effective date of a certificate, whichever is later, without any material loss of data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Applications required to process the archive data shall also be maintained for as long as necessary. After the archive retention period, users are responsible for maintaining the authenticity and integrity of their own documents.

5.5.3 Protection of Archive

No unauthorized user shall be able to write to, modify, or delete the archive. However, archived records may be moved to another medium. The contents of the archive shall not be released as a whole, except as required by law. Records of individual transactions may be released upon request of any entities involved in the transaction or their legally recognized agents. Archive media shall be stored in a separate, safe, secure storage facility.

5.5.4	Archive Backup Procedures	Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a short period of time.
5.5.5	Requirements for Time-Stamping of Records	Certificate validations and witnessed document signing (notarization) shall be time-stamped
5.5.6	Procedures to Obtain and Verify Archive Information	During any audits required by this Policy, the auditor shall verify the integrity of the archives.

5.6 Key Changeover

A Subscriber may only apply to renew his or her Key Pair within three months prior to the expiration of one of the keys, provided the previous certificate has not been revoked. A Subscriber, the Issuing CA, or the Authenticating RA may initiate this key changeover process. Automated key changeover may be permitted. The Issuing CA must ensure that the details of this process are indicated in its CPS. Subscribers without valid keys must be re-authenticated by the Issuing CA or Authenticating RA in the same manner as the initial registration. Where a Subscriber's certificate has been revoked as a result of non-compliance, the Issuing CA must verify that any reasons for non-compliance have been addressed to its satisfaction prior to certificate re-issuance. Keys may not be renewed using an expired Digital Signature key.

5.7 Compromise and Disaster Recovery

5.7.1	Computing Resources Software and/or Data Are Corrupted	An Issuing CA must have in place an appropriate disaster recovery and business resumption plan. The plan must set up and render operational a facility located in a geographic diverse area that is capable of providing CA Services in accordance with this Policy within forty eight (48) hours of an unanticipated emergency. Such plan shall include a complete and periodic test of readiness for such facility. Such plan shall be referenced within the CPS or other appropriate documentation and readily available to Relying Parties for inspection.
5.7.2	Secure Facility After a Natural or Other Type of Disaster	An Issuing CA must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the Issuing CA, the Issuing CA must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.
5.7.3	Entity Public Key Is Revoked	In the event of the need for revocation of a CA's Digital Signature certificate, the Issuing CA must immediately notify: DIS, the PMA; all CAs to whom it has issued cross-Certificates; all of its RAs; all Subscribers; all individuals or organizations who are responsible for a Certificate used by a device or application. The Issuing CA must also: publish the Certificate serial number on an appropriate CRL; revoke all cross-Certificates signed with the revoked Digital Signature certificate. After addressing the factors that led to revocation, the Issuing CA may: generate a new CA signing Key Pair; re-issue Certificates to all Entities and ensure all CRLs and ARLs are signed

using the new key. In the event of the need for revocation of any other entity's Digital Signature certificate see Section 4.9.

5.7.4 Entity Private key Is Compromised

In the event of the compromise, or suspected compromise, of an Issuing CA signing key, the Issuing CA must immediately notify all CAs with whom it has cross-certified. In the event of the compromise, or suspected compromise, of any other entity's signing key, an entity must notify the Issuing CA immediately. The Issuing CA must ensure that its CPS or a publicly available document and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise. In the event of the compromise of a CA's Digital Signature key, the Issuing CA must revoke all Certificates issued using that key and provide appropriate notice (see 5.7.3). After addressing the factors that led to key compromise, the Issuing CA may: generate a new CA Signing Key Pair; re-issue Certificates to all Entities and ensure all CRLs and ARLs are signed using the new key.

5.7.5 Entity Public Key Is Downgraded

In the event of the need for the downgrade of a CA's Digital Signature certificate, an Issuing CA must immediately notify all interested parties including the PMA, other CAs with whom it cross-certified, all RAs, and all Subscribers.

5.8 CA Termination

In the event that an Issuing CA ceases operation, all Subscribers, sponsoring organizations, RAs, CMAs, Repositories, and Relying Parties will be promptly notified of the termination. In addition, all CAs with which cross-certification agreements are current at the time of cessation will be promptly informed of the termination. All Certificates issued by the Issuing CA that reference this Policy will be revoked no later than the time of termination. All current and archived CA identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be transferred to the State (or its designee) within 24 hours of CA cessation and in accordance with this Policy. Transferred data shall not include any data unrelated to this Policy. Key recovery enabled repository data will not be co-mingled with this data, and will be provided separately.

5.9 CUSTOMER SERVICE

An Issuing CA shall implement and maintain Customer Service Center to provide assistance and services to Subscribers and Relying Parties consistent with this Policy, and a system for receiving, recording, responding to, and reporting problems within its own organization and for reporting such problems to the PMA.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key pair generation

Key pairs for CAs, CMAs, Authenticating RAs, Repositories, and Subscribers must be generated in such a way that the Private Key is not known by other than the authorized user of the Key Pair. Acceptable ways of accomplishing this include having all users (CAs, CMAs, Authenticating RAs, Repositories, and Subscribers) generate their own keys on a secure system, and not reveal the Private Keys to anyone else and having keys generated in hardware tokens from which the Private Key cannot be extracted. CA, Authenticating RA, and CMA keys must be generated in hardware

tokens. Key pairs for Repositories, and end-entities can be generated in either hardware or software.

6.1.2	Private key delivery to entity	In most cases, a Private Key will be generated and remain within the crypto boundary of the cryptomodule. If the owner of the module generates the Key, then there is no need to deliver the Private Key. If a Key is not generated by the Subscriber, then the module must be securely delivered. Accountability for the location and state of the module must be maintained until delivery of possession. The Subscriber shall formally acknowledge receipt of the module. If the Subscriber generates the Key, and the Key will be stored by and used by the application, which generated it, or on a hardware token in the possession of the Subscriber, no further action is required. If the Key must be extracted for use by other applications or in other locations, a protected data structure (such as defined in [PKCS#12]) shall be used. The resulting file may be kept on a magnetic medium, or transported electronically.
6.1.3	Public key delivery to certificate issuer	Public Keys must be delivered to an Issuing CA in a secure and trustworthy manner, such as a certificate request message. It may also be accomplished via non-electronic means. These means may include, but are not limited to, floppy disk (or other storage medium) sent via registered mail or courier, or by delivery of a token to the Issuing CA for local key generation at the point of certificate issuance or request. Off-line means shall include identity checking and shall not inhibit proof of possession of corresponding Private Key. Any other methods used for Public Key delivery shall be stipulated in a CPS. In those cases where Public/Private Key Pairs are generated by the Issuing CA on behalf of the Subscriber, the Issuing CA shall implement secure mechanisms to ensure that the token on which the Public/Private Key Pair is held is securely sent to the proper Subscriber, and that the token is not activated prior to receipt by the proper Subscriber.
6.1.4	CA Public Key delivery to users	The Public Key of an Issuing CA's Signing Key Pair may be delivered to Subscribers in an on-line transaction in accordance with IETF PKIX Part 3, or via another appropriate mechanism.
6.1.5	Key sizes	Minimum key length for other than elliptic curve based algorithms is 1024 bits. Minimum key length for elliptic curve group algorithms is 170.
6.1.6	Public key parameters generation	An Issuing CA that utilizes the DSA must generate parameters in accordance with FIPS 186. ECDSA must be utilized in accordance with Draft ANSI Standard X9.62.
6.1.7	Parameter quality checking	Parameters for DSA shall be checked as specified in [FIPS186].
6.1.8	Hardware/software key generation	The generation of Digital Signature keys for all Entities must be randomly generated in a hardware cryptographic module. Any pseudo-random numbers used for key generation material shall be generated by a FIPS approved method.
6.1.9	Key usage purposes (as per X.509 v3 key usage field)	Keys may be used for authentication, non-repudiation and message integrity. They may also be used for session key establishment. CA signing keys are the only keys permitted to be used for signing Certificates and CRLs. The Certificate Key Usage field must be used in accordance with PKIX-1 Certificate and CRL Profile. One of the following Key Usage values must be present in all Certificates: Digital Signature or Non-Repudiation. One of the following additional values must be present in CA certificate-signing Certificates: Key Cert Sign or CRL Sign. Keys shall be certified for use in signing or encrypting, but not both, unless otherwise provided herein. The use

of a specific key is determined by the key usage extension in the X.509 certificate. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using key management Certificates.

6.2 CA PRIVATE KEY PROTECTION

An Issuing CA (and the Authenticating RA, CMA, and Repository) shall each protect its Private Key(s) in accordance with the provisions of this Policy.

6.2.1	Standards for cryptographic module	The relevant standard for cryptomodules is [FIPS140-1], unless DIS, with guidance from the PMA, determines that other comparable validation, certification, or verification standards are sufficient. In such event such standards will be transmitted to Issuing CA's by DIS and published by the CA's. Subscribers shall use cryptographic modules, which meet at least the criteria specified in this Policy. Authenticating RAs require at least Level 2 hardware cryptomodules. A higher level may be used if available or desired. Authenticating RAs and Issuing CAs should provide the option of using any acceptable cryptomodule, to facilitate the management of Certificates. An Issuing CA may use hardware or software cryptomodules for CA key generation and protection, validated at Level 3. Certificates shall be signed using a hardware cryptomodule that meets Level 3.
6.2.2	Private key multi-person control	Multi-person control requires that more than one individual (typically the Issuing CA and one or more separate security officers) independently authorize themselves to the system that will perform CA operations. This mechanism prevents any single party (CA or otherwise) from gaining access to the CA Signing Key. Key management and end-entity signature keys may be backed up in multiple tokens without two-person control so long as the operations to do so are audited, and the Private Keys never exist in unencrypted form outside the token. CA Signing Keys may only be backed up under two-person control. The parties used for two-person control shall be maintained on a list that shall be made available for audit.
6.2.3	Private key escrow	Under no circumstances shall a Signing Key be escrowed. For some purposes (such as data recovery), however, it will be necessary to provide key escrow and/or key recovery for Confidentiality Keys. The method for this shall be described in a CPS.
6.2.4	Private key backup	An entity may optionally back-up its own Digital Signature Private Key. If so, the Key must be copied and stored in encrypted form and protected at a level no lower than stipulated for the primary version of the Key.
6.2.5	Private key archival	If an Issuing CA is acting as a key recovery agent, then it shall archive Private Key management keys as part of its service. Private Signature Keys supporting non-repudiation services shall never be archived. An entity may optionally archive its own Private Key.
6.2.6	Private key entry into cryptographic module	Private Keys are to be generated and kept inside cryptographic modules evaluated to at least FIPS 140-1 Level 3. In the event that a Private Key is to be transported from one cryptomodule to another, the Private Key must be encrypted during transport; Private Keys must never exist in plain text form outside the cryptomodule boundary.
6.2.7	Method of activating Private Key	Private Keys are activated by Activation Data stored securely and separately from Crypto modules.
6.2.8	Method of deactivating Private	Cryptomodules which have been activated must not be left unattended or otherwise open to unauthorized access. After use they must be deactivated, e.g. via a manual

	Key	logout procedure, or by a passive timeout. Hardware cryptomodules should be removed and stored or within the Issuing CA's sole control when not in use.
6.2.9	Method of destroying Private Key	Private keys should be destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked. For software cryptomodules, this can be overwriting the data. For hardware tokens, this will likely be executing a "zeroize" command. Physical destruction of hardware is not required.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

An Issuing CA must retain all verification Public Keys.

6.3.1	Public key archival	Each Issuing CA, Authenticating RA, and CMA shall each protect its Private Key(s) in accordance with the provisions of this Policy.
	Key Replacement	All keys (2048 bits) must have validity periods of no more than twenty years. Suggested validity period: CA public verification key and certificate - twenty years; CA private signing key - eight years; End-Entity public verification key and certificate - twelve years; End-Entity private signing key - two years.
	Restrictions On CA's Private Key Use	The Private Key used by an Issuing CA for issuing Certificates shall be used only for signing such Certificates and, optionally, CRLs or other validation services responses. A Private Key held by an Authenticating RA, if any, is considered the Issuing CA's Private Key, is held by the Authenticating RA as a fiduciary, and shall not be used by the Issuing CA for any other purposes, except as agreed to between the Issuing CA and the Authenticating RA. Any other Private Key used by an Authenticating RA for purposes associated with its RA functions shall not be used for any other purpose without the express permission of the Issuing CA. The Private Key used by each Authenticating RA in connection with the issuance of Certificates shall be used only for communications relating to the approval or revocation of such Certificates.
6.3.2	Usage periods for the public and Private Keys	The key usage periods for keying material are described in Section 6.3.1.

6.4 ACTIVATION DATA

6.4.1	Activation Data generation and installation	A pass-phrase or PIN ("Activation Data") shall be used to protect access to use of the Private Key. The Activation Data may be user selected. If the Activation Data must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated cryptomodule. If this is not done by hand, the user should be advised of the shipping date, method of shipping, and expected delivery date of any Activation Data. As part of the delivery method, users will sign and return a delivery receipt. In addition, users should also receive (and acknowledge) a user advisory statement to help to understand responsibilities in the use and control of the cryptomodule.
6.4.2	Activation Data protection	Activation Data should be memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptomodule is used to protect, and shall not be stored with the cryptomodule. Activation Data shall never be shared. Data used for entity initialization must be protected from unauthorized use by a

combination of cryptographic and physical access control mechanisms. The Private Keys of entities must be protected from unauthorized use by a combination of cryptographic and physical access control mechanisms. The level of protection must be adequate to deter a motivated attacker with substantial resources. If a reusable password scheme is used, the mechanism should include a facility to temporarily lock the account after a predetermined number of login attempts.

6.4.3 Other aspects of Activation Data

This Policy makes no stipulation on the life of Activation Data; however, it should be changed periodically to decrease the likelihood that it has been discovered. CAs may define Activation Data requirements in their CPSs.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific computer security technical requirements

All CA servers must include the following functionality either provided by the operating system, or through a combination of operating system, PKI application, and physical safeguards:

- Access control to CA services and PKI roles;
- Enforced separation of duties for PKI roles;
- Identification and authentication of PKI roles and associated identities;
- Object re-use or separation for CA random access memory;
- Use of cryptography for session communication and database security;
- Archival of CA and End-Entity history and audit data;
- Audit of security related events;
- Self-test of security related CA services;
- Trusted path for identification of PKI roles and associated identities;
- Recovery mechanisms for keys and the Issuing CA system.

6.5.2 Computer security rating

An Issuing CA's equipment shall meet and be operated to at least a C2 [TCSEC] or E2/F-C2 [ITSEC] rating, or equivalent. An Issuing CA's equipment operating at a C2 equivalence shall, as a minimum, implement self-protection, process isolation, discretionary access control, object reuse controls, individual identification and authentication, and a protected audit record.

6.6 LIFE CYCLE TECHNICAL CONTROLS

Equipment (hardware and software) procured to operate a PKI shall be purchased in a fashion to reduce the likelihood that any particular copy was tampered with, such as random selection. Equipment developed for a PKI shall be developed in a controlled environment, and the development process shall be defined and documented. Equipment procured prior to registration as an Issuing CA shall be deemed to satisfy this requirement. CA equipment shall be protectively packaged and delivered via an accountable method. Tamper-evident packaging shall be used, or equipment shall be hand-carried from a controlled procurement environment to the installation site. Equipment procured prior to registration as an Issuing CA shall be deemed to satisfy this requirement. The Issuing CA equipment shall be dedicated to administering a key management infrastructure. It shall not have installed applications or component software, which are not part of the CA configuration. Equipment updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.1 System development controls

An Issuing CA must use CA software that has been designed and developed either under a development methodology such as MIL-STD-498, the System Security Engineering Capability Maturity Model (SSE CMM), or Information Systems Security Engineering Handbook. The design and development process must provide sufficient documentation to support third party security evaluation of the Issuing CA components and be supported by: third party verification of process compliance; on-going Threat Risk Assessments to influence security safeguard design and minimize residual risk.

6.6.2 Security management controls

A formal configuration management methodology must be used for installation and ongoing maintenance of an Issuing CA system. The Issuing CA software, when first loaded, must provide a method for the Issuing CA to verify that the software on the system: originated from the software developer; has not been modified prior to installation; and is the version intended for use. The Issuing CA must provide a mechanism to periodically verify the integrity of the software. The Issuing CA must also have mechanisms and policies in place to control and monitor the configuration of the Issuing CA system. Upon installation time, and at least once every 24 hours, the integrity of the Issuing CA system must be validated.

6.7 NETWORK SECURITY CONTROLS

CA equipment should be connected to no more than two network domains at a time. CA equipment intended to connect to more than one network classification domain shall have procedures defined in a CPS which prevent information from one domain from reaching another (e.g., equipment shutdown, removable hard drives, switching the network connection). CA equipment may operate through a network guard insofar as it does not circumvent the function of the guard. Protection of CA equipment shall be provided against known network attacks. Use of appropriate boundary controls shall be employed. All unused network ports and services shall be turned off. Any network software present on the Issuing CA equipment shall be necessary to the functioning of the Issuing CA application. Root CA equipment shall be stand-alone (off-line) configurations.

6.8 CRYPTO-GRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are as stated above in section 6.2.

7 CERTIFICATE AND CRL PROFILES

7.1 CERTIFICATE PROFILE

Certificates that reference this Policy shall contain Public Keys used for authenticating the sender of an electronic message and verifying the integrity of such messages – i.e., Public Keys used for Digital Signature verification. All Certificates that reference this Policy will be issued in the X.509 version 3 format and will include a reference to the OID for this Policy within the appropriate field. The CPS shall identify the Certificate extensions supported, and the level of support for those extensions.

7.1.1	Version number and base fields	An Issuing CA must issue X.509 Version 3 Certificates, in accordance with the PKIX Certificate and CRL Profile. The PKI End-Entity software must support all the base (non-extension) X.509 fields:
	Version	Version of X.509 certificate, version 3(2)
	Serial Number	Unique serial number for certificate as well as the Certificate extensions defined 7.1.2
	Signature	CA signature to authenticate certificate
	Issuer	Name of CA
	Validity Period	Activation and expiry date for certificate
	Subject	Subscriber's distinguished name, which may contain additional numbers or letters appended to the common name to ensure the name's uniqueness within the domain of Certificates issued by the Issuing CA
	Subject Public Key Information	
7.1.2	Certificate Extensions	No extension shall modify or undermine the use of X.509 base fields. Additionally:
7.1.2.1	Certificate Policies	The certificate Policies field must be populated in all Certificates with one of the policy

		OIDs identified in Section 1.2 and may be set as a non-critical extension. .
7.1.2.2	Policy Constraints	No stipulation.
7.1.2.3	Critical extensions	All entity PKI software must correctly process critical extensions identified in this Policy.
7.1.2.4	Supported Extensions	The CPS must define the use of any extensions supported by an Issuing CA, its Authenticating RAs and End Entities.
7.1.3	Algorithm object identifiers	Certificates under this Policy will use the following OIDs for signatures: id-dsa-with-sha1 {iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3} Certificates under this Policy will use the following OIDs for identifying the algorithm the subject key was generated for: Encryption {iso(1) member-body(2) us(840) (113549) pkcs(1) pkcs-1(1) 1} publicnumber {iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1} Certificates containing keys generated for use with DSA or for use with KEA shall be signed with id-dsa-with-sha1. Keys generated for use with RSA shall be signed using sha-1WithRSAEncryption (1.2.840.113549.1.1.5). For alternate algorithms, only PMA-approved algorithms may be used.
7.1.4	Name forms	Every DN must be in the form of an X.501 printable String
7.1.5	Name constraints	Subject and Issuer DNs must comply with PKIX standards and be present in all Certificates.
7.1.6	Certificate policy object identifier	An Issuing CA must ensure that the Policy OID is contained within the Certificates it issues.
7.1.7	Usage of Key Usage extension	An Issuing CA must populate and mark as critical the Key Usage extension in a Certificate and identify the Subscriber's Private Key as being used either for signing (Digital Signature and non-Repudiation) or for encryption (dataEncipherment and keyEndipherment).
7.1.8	Policy qualifiers syntax and semantics	An Issuing CA must populate the policy Qualifiers extension with the URL of its CP. An Issuing CA shall populate a user notice in one of the Certificate extensions, with the following text: CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$X,000.00
7.2	***CRL PROFILE***	If utilized, CRLs will be issued in the X.509 version 2 format. The CPS shall identify the CRL extensions supported and the level of support for these extensions
7.2.1	Version numbers	An Issuing CA must issue X.509 version two (2) CRLs in accordance with the PKIX Certificate and CRL Profile.
7.2.2	CRL and CRL entry extensions	All entity PKI software must correctly process all CRL extensions identified in the Certificate and CRL profile. The CPS must define the use of any extensions supported by the Issuing CA, and End Entities.

8 POLICY ADMINISTRATION

8.1 POLICY CHANGE PROCEDURES

This Policy will be reviewed by DIS every year. Errors, updates, or suggested changes to this document shall be communicated to the PMA contact on or before the date ninety days from the anniversary date of the day on which this Policy becomes effective. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change. The PMA will review any notices of errors, updates, or suggested changes, and provide recommendations to DIS and Issuing CA's. All proposed material policy changes shall be disseminated to interested parties (see section 8.2) for a period of thirty days beginning sixty days prior to the anniversary date of the date on which this Policy becomes effective (the "Review Period"). DIS shall use its best efforts to accept or reject any proposed changes promptly upon the close of the Review Period.

Not withstanding, if in the judgement of DIS or the PMA, it is determined changes to the policy should be made prior to the annual review, DIS reserves the right to modify the policy upon notification of the proposed changes to Issuing CAs. Issuing CAs will be given reasonable time to comment, and conform to the proposed changes.

8.1.1	List of Items that Can Change Without Notification	Notice of all proposed changes to this Policy under consideration by the State and an Issuing CA that may materially impact users of this Policy (other than editorial or typographical corrections, or changes to the contact details) will be provided to RAs, and will be posted on the World Wide Web site of an Issuing CA. An Issuing CA shall post notice of such proposed changes in its repositories and shall advise Subscribers, in writing in tangible form or by e-mail, of such proposed changes.
8.1.2	List of Items Subject to Notification Requirement	All items in this Policy are subject to the notification requirement. Prior to the effective date of any changes to this Policy, DIS will notify all Issuing CAs.
8.1.3	Comment Period, Process and Procedure	Impacted users may file comments with the PMA within 30 days of the posting of the original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be given.

8.2 PUBLICATION AND NOTIFICATION POLICIES

All issuing CA's shall post a copy of this Policy in electronic form on the Internet.

8.2.1.1	Notification mechanism	DIS will notify, in writing, any party authorized to issue Certificates under this Policy of any proposed changes to this Policy.
8.2.1.2	Mechanism to handle comments	Written and signed comments on proposed changes must be directed to the PMA. Decisions with respect to the proposed changes are at the sole discretion of the State.
8.2.1.3	Final Change Notice	DIS will determine the period for final change notice.
8.2.2	Items whose change requires a new policy	If a policy change is determined by DIS or the PMA to warrant the issuance of a new policy, the State may assign a new Object Identifier (OID) for the modified policy.

8.3 CPS APPROVAL PROCEDURES

Where an Issuing CA's CPS contains information relevant to the security of the Issuing CA, all or part of the CPS need not be made publicly available.

8.4 WAIVERS

Waivers will not be granted under any level of assurance. Variation in an Issuing CA's practice will either be deemed acceptable under this Policy, or a change shall be requested to this Policy, or a new policy shall be established for the non-compliant practice.

Certificate Policy
for the
State of Washington
Public Key Infrastructure

Appendix A
Certificate Profiles

Table of Contents

1 Document Information

1.1 Purpose

The purpose of this document is to define the certificate profiles for the various types of certificates issued by the State of Washington Public Key Infrastructure (PKI). There are six types of certificates that can be issued by the State of Washington PKI:

- Root Certification Authority (CA)
- Subordinate Certification Authorities (CA)
- Browser based Signing certificates (High, Intermediate, and Standard)
- Browser based Confidentiality certificates (High, Intermediate, and Standard)
- Enterprise Signing certificates (High and Intermediate)
- Enterprise Confidentiality certificates (High and Intermediate)

1.2 Acronyms

CA	Certification Authority
CONOP	Concept of Operations
CP	Certificate Policy
CRL	Certificate Revocation List
PKI	Public Key Infrastructure
RFC	Request for Comment

1.3 Scope

The profiles defined in this document are limited to those X.509 V3 certificates that are issued by the State of Washington PKI. The profile for X.509 V2 Certificate Revocation Lists (CRLs) is defined in RFC 2459, and is not included in this document.

2. State of Washington PKI Certificate Profiles

The following profiles define the certificate types and layouts for the State of Washington PKI. It is provided to facilitate the integration of the PKI and various applications, including the Transact Washington Project.

2.1 Digital Signature Trust Co. Root CA X4 Certificate Profile

This is a pre-existing off-line root certification authority that is operated by Digital Signature Trust Co. to sign subordinate roots for other PKIs.

Note: This CA certificate, CRL and ARL will be published to both the DST (ldap.digsigtrust.com and ldapsow.digsigtrust.com directories.)

Subject DN: o=Digital Signature Trust Co.,cn=DST Root CA X4

Root CA Certificate Attribute/Extension	Value/Information
Version	version 3, which is INTEGER 2
SerialNumber	INTEGER
Signature	sha-1WithRSAEncryption OID = 1.2.840.113549.1.1.5
Issuer	cn=DST Root CA X4, o=Digital Signature Trust Co.
Validity	20 years
Subject	cn=DST Root CA X4, o=Digital Signature Trust Co.
subjectPublicKeyInfo	RSAEncryption OID = 1.2.840.113549.1.1.1 parameters field present with NULL value RSA public key is a 2048 bit public key. RSA public key shall be encoded using the ASN.1 type RSAPublicKey: RSAPublicKey ::= SEQUENCE { modulus INTEGER, -- n publicExponent INTEGER -- e -- } where modulus is the modulus n, and publicExponent is the public exponent e. The DER encoded RSAPublicKey is the value of the BIT STRING subjectPublicKey.
issuerUniqueIdentifier	Not Present
subjectUniqueIdentifier	Not Present
Extensions	
authorityKeyIdentifier	Not Present!
subjectKeyIdentifier	Present and not critical keyIdentifier is SHA-1 hash of subjectPublicKey
KeyUsage	Not Present
extKeyUsage	Not Present
privateKeyUsagePeriod	Not Present
certificatePolicies	Not Present
policyMappings	Not Present
subjectAltName	Not Present
issuerAltName	Not Present
subjectDirectoryAttributes	Not Present
basicConstraints	Present and critical cA=TRUE pathLenConstraint not present
NameConstraints	Not Present
policyConstraints	Not Present
AuthorityInfoAccess	Not Present
cRLDistributionPoints	Not Present

Digital Signature Trust DST RootCA X4 V3 Certificate Profile

2.2 Washington State Off-line CA Certificate Profile

This CA is utilized to issue a subordinate sub CA that is utilized as production CA for issuing end entity certificates for the Washington State. This CA will be an offline CA meaning that the Key material will only be utilized to issue the CA certificate for the subordinate CA.

Note: This CA certificate, CRL and ARL will be published to both the DST (ldap.digsigtrust.com and ldapsow.digsigtrust.com directories.)

Subject DN: c=US,o = State of Washington PKI,cn= Washington State CA A1

Root CA Certificate Attribute/Extension	Value/Information
Version	version 3, which is INTEGER 2
SerialNumber	INTEGER
Signature	sha-1WithRSAEncryption OID = 1.2.840.113549.1.1.5
Issuer	cn=DST Root CA X4, o=Digital Signature Trust Co.
Validity	10 years offline
Subject	cn=Washington State CA A1, o=State of Washington PKI,c=US
subjectPublicKeyInfo	RSAEncryption OID = 1.2.840.113549.1.1.1 parameters field present with NULL value RSA public key is a 2048 bit public key. RSA public key shall be encoded using the ASN.1 type RSAPublicKey: RSAPublicKey ::= SEQUENCE { modulus INTEGER, -- n publicExponent INTEGER -- e -- } where modulus is the modulus n, and publicExponent is the public exponent e. The DER encoded RSAPublicKey is the value of the BIT STRING subjectPublicKey.
issuerUniqueIdentifier	Not Present
subjectUniqueIdentifier	Not Present
Extensions	
authorityKeyIdentifier	Present and not critical keyIdentifier is SHA-1 hash of the issuers subjectPublicKey
subjectKeyIdentifier	Present and not critical keyIdentifier is SHA-1 hash of subjectPublicKey
KeyUsage	Not Present
extKeyUsage	Not Present
privateKeyUsagePeriod	Not Present
certificatePolicies	Not Present
policyMappings	Not Present
subjectAltName	Not Present
issuerAltName	Not Present
subjectDirectoryAttributes	Not Present

Root CA Certificate Attribute/Extension	Value/Information
basicConstraints	Present and critical cA=TRUE pathLenConstraint not present
NameConstraints	Not Present
policyConstraints	Not Present
AuthorityInfoAccess	Present and Non critical accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= { ldap://ldap.digsigtrust.com/ cn=DST Root CA X4, o=Digital Signature Trust Co.?cACertificate;binary }
cRLDistributionPoints	Present and Non-critical DistributionPoint field is present and populated with pointer to CRL issued by Superior CA (e.g., URL ldap://ldap.digsigtrust.com/ cn=DST Root CA X4,o=Digital Signature Trust Co.?certificateRevocationList;binary)

Washington State Off-line Root CA Certificate Profile

2.3 State of Washington Subordinate CA Certificate Profile (for Browser Certificates)

This PKI infrastructure utilizes a Certification Authority product for Browser certificates. This profile details the browser certificate subordinate CA.

- Sub CA issuing End Entity certificates for Signature and Confidentiality within "Browsers" subject Subject DN: c=US, o= State of Washington PKI, ou=State of Washington CA, cn= Washington State CA B1

Certificate Attribute/Extension	Value/Information
Version	version 3, which is INTEGER 2
SerialNumber	INTEGER
Signature	sha-1WithRSAEncryption OID = 1.2.840.113549.1.1.5
Issuer	cn=Washington State CA A1,o=State of Washington PKI,c=US
Validity	Valid for 5 years
Subject	cn= Washington State CA B1, ou= State of Washington CA, o=State of Washington PKI, c=US The naming scheme for additional CAs is the common name will contain the following sequence xy where x is an alphabetic character (A-Z) and defines the level within the CA hierarchy and y is an incremental integer from 1 to 9999 of the CA within this level.
SubjectPublicKeyInfo	rSAEncryption OID = 1.2.840.113549.1.1.1 parameters field present with NULL value RSA public key is a 2048 bit public key. RSA public key shall be encoded using the ASN.1 type RSAPublicKey: RSAPublicKey ::= SEQUENCE { modulus INTEGER, -- n publicExponent INTEGER -- e -- } where modulus is the modulus n, and publicExponent is the public exponent e. The DER encoded RSAPublicKey is the value of the BIT STRING subjectPublicKey.
IssuerUniqueIdentifier	Not Present
SubjectUniqueIdentifier	Not Present
Extensions	
AuthorityKeyIdentifier	Present and not critical keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Root CA certificate
SubjectKeyIdentifier	Present and not critical keyIdentifier is SHA-1 hash of subjectPublicKey
keyUsage	Present and critical digitalSignature = 1

	nonRepudiation = 1 dataEncipherment = 0 keyEncipherment = 0 keyAgreement = 0 keyCertSign = 1 cRLSign = 1 encipherOnly = 0 decipherOnly = 0
ExtKeyUsage	Not Present
PrivateKeyUsagePeriod	Not Present

CertificatePolicies
 	
Note that the User Notice Text is the final version. These notices must all be encoded with the appropriate Certificate Policy OID Assurance Level of the State of Washington CA certificate.
	Present and not critical
	
	All applicable certificate policies are defined in this certificate in the policyIdentifier field. That is, this certificate extension defines the policy OIDs for the High, Intermediate, and Standard brand certificates as defined in the CP.
	id-State of Washington ID:: id-cp 4 → 2.16.840.1.113839.0.4 State of Washington ARC 5/31/2000
	End Entity CA OIDs
	High Assurance Level Certificate
	id-HighAssuranceLevel ID::= {id-Stateofwashington 1 } → 2.16.840.1.113839.0.4.1
	Intermediate Assurance Level Certificate
	id-IntermediateAssuranceLevel ID::= { id-Stateofwashington 2} → 2.16.840.1.113839.0.4.2
	Standard Assurance Level Certificate [1]
	id-StandardAssuranceLevel ID::= { id-Stateofwashington 3 } → 2.16.840.1.113839.0.4.3
	
	PolicyQualifier[2] present
	PolicyQualifierInfo ::= SEQUENCE {
	PolicyQualifierId id-qt-unotice
	qualifier ANY DEFINED BY policyQualifierId }
	-- user notice qualifier
	UserNotice ::= SEQUENCE {
	explicitText = {
	HIGH USER Notice
	"CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$50,000.00"
	INTERMEDIATE USER Notice
	"CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$10,000.00"
	STANDARD USER Notice

[1] High and Intermediate Assurance Level certificates do not apply to the browser signing certificates issued from the "Washington State CA B1" CA.

[2] PolicyQualifier is defined for all the State of Washington Policy OIDs and includes a User Notice explicitText. Note that the subordinate Root certificates will have repeated explicitText user notice string, as by definition these are unique per policy OID.

	"CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$1,000.00" }} PolicyQualifierInfo PolicyQualifierId id-qt-cpsuri CpsUri ::= "PolicyQualifierId id-qt-cpsuri{ http://www.digsigtrust.com/certificates/policy/sowindex.html} Repeated for each policy along with userNotice.
policyMappings	Not Present
subjectAltName	Not Present
issuerAltName	Not Present
subjectDirectoryAttributes	Not Present
basicConstraints	Present and critical cA=TRUE pathLenContstraint not present
nameConstraints	Not Present
policyConstraints	Not Present
authorityInfoAccess	Present and not critical accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= {ldap://ldapsow.digsigtrust.com/cn=Washington State CA A1, o=State of Washington PKI,c=US?cACertificate;binary }
cRLDistributionPoint	Present and not critical DistributionPoint field is present and populated with pointer to CRL issued by Superior CA (e.g., URL ldap://ldapsow.digsigtrust.com/cn=Washington State CA A1, o=State of Washington PKI,c=US?certificateRevocationList;binary) reasons and cRLIssuer fields not present

State of Washington Subordinate CA Certificate Profile

2.4 State of Washington Subordinate CA Certificate Profile (for Enterprise Certificates)

This PKI infrastructure utilizes a Certification Authority product for Enterprise Certificates (Entrust CA 5.0). This profile details the Enterprise Certificates CA.

- Sub CA issuing End Entity certificates for "Enterprise Certificates"
  Subject DN: c=US, o=State of Washington PKI, ou=State of Washington CA, cn= Washington State CA B2

Certificate Attribute/Extension	Value/Information
Version	version 3, which is INTEGER 2
SerialNumber	INTEGER
Signature	sha-1WithRSAEncryption OID = 1.2.840.113549.1.1.5
Issuer	cn= Washington State CA B2, ou= State of Washington CA, o=State of Washington PKI, c=US
Validity	Valid for 5 years
Subject	cn= Washington State CA B2, ou= State of Washington CA, o=State of Washington PKI, c=US The naming scheme for additional CAs is the common name will contain the following sequence xy where x is an alphabetic character (A-Z) and defines the level within the CA hierarchy and y is an incremental integer from 1 to 9999 of the CA within this level.
SubjectPublicKeyInfo	rSAEncryption OID = 1.2.840.113549.1.1.1 parameters field present with NULL value RSA public key is a 2048 bit public key. RSA public key shall be encoded using the ASN.1 type RSAPublicKey: RSAPublicKey ::= SEQUENCE { modulus INTEGER, -- n publicExponent INTEGER -- e -- } where modulus is the modulus n, and publicExponent is the public exponent e. The DER encoded RSAPublicKey is the value of the BIT STRING subjectPublicKey.
IssuerUniqueIdentifier	Not Present
SubjectUniqueIdentifier	Not Present
Extensions	
AuthorityKeyIdentifier	Present and not critical keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Root CA certificate
SubjectKeyIdentifier	Present and not critical keyIdentifier is SHA-1 hash of subjectPublicKey

keyUsage[3]	Present and critical digitalSignature = 1 nonRepudiation = 1 dataEncipherment = 0 keyEncipherment = 0 keyAgreement = 0 keyCertSign = 1 cRLSign = 1 encipherOnly = 0 decipherOnly = 0
ExtKeyUsage	Not Present
PrivateKeyUsagePeriod	Not Present

CertificatePolicies
 	
Note that the User Notice Text is the final version. These notices must all be encoded with the appropriate Certificate Policy OID Assurance Level of the State of Washington CA certificate.
	Present and not critical
	
	All applicable certificate policies are defined in this certificate in the policyIdentifier field. That is, this certificate extension defines the policy OIDs for the High, Intermediate, and Standard brand certificates as defined in the CP.
	id-State of Washington ID:: id-cp 4 → 2.16.840.1.113839.0.4 State of Washington ARC 5/31/2000
	End Entity CA OIDs
	High Assurance Level Certificate
	id-HighAssuranceLevel ID::= {id-Stateofwashington 1 } → 2.16.840.1.113839.0.4.1
	Intermediate Assurance Level Certificate
	id-IntermediateAssuranceLevel ID::= { id-Stateofwashington 2} →2.16.840.1.113839.0.4.2
	Standard Assurance Level Certificate [4]
	id-StandardAssuranceLevel ID::= { id-Stateofwashington 3 } →2.16.840.1.113839.0.4.3
	
	PolicyQualifier[5] present
	PolicyQualifierInfo ::= SEQUENCE {
	PolicyQualifierId id-qt-unotice
	qualifier ANY DEFINED BY policyQualifierId }
	-- user notice qualifier
	UserNotice ::= SEQUENCE {
	explicitText = {
	HIGH USER Notice
	"CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$50,000.00"
	INTERMEDIATE USER Notice
	"CA liability is limited by Washington law and the

[3] The keyUsage of the Entrust Subordinate CA may differ slightly as the Entrust Product dictates specific keyUsage bits within enterprise certificates.

[4] Standard certificates do not apply to the Enterprise Certificates issued from the Entrust CA as these certificates do not reside in the subscriber's browser certificate data store.

[5] PolicyQualifier is defined for all the State of Washington Policy OIDs and includes a User Notice explicitText. Note that this Root certificates will have repeated explicitText user notice string, as by definition these are unique per policy OID.

	Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$10,000.00” **STANDARD USER Notice** “CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$1,000.00” }} PolicyQualifierInfo PolicyQualifierId id-qt-cpsuri CpsUri ::= “PolicyQualifierId id-qt-cpsuri{ http://www.digsigtrust.com/certificates/policy/sowindex.html} Repeated for each policy along with userNotice.
policyMappings	Not Present
subjectAltName	Not Present
issuerAltName	Not Present
subjectDirectoryAttributes	Not Present
basicConstraints	Present and critical cA=TRUE pathLenContstraint not present
nameConstraints	Not Present
policyConstraints	Not Present
authorityInfoAccess	Not Present
cRLDistributionPoint	Present Not Critical CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1,CN=Washington State CA B2, OU=State of Washington CA,O=State of Washington PKI,C=US

State of Washington Subordinate CA Certificate Profile

2.5 State of Washington Subscriber Signature Certificate Profile

The following profile defines signing certificates that will be utilized within the State of Washington PKI for authentication and digital signing. Although the sample subjects DNs below illustrate possible Business and State Agency DNs, currently the only type of certificate that will be issued will be an individual subscriber certificate.

subject DN: c=US,o= State of Washington PKI,ou= State of Washington,cn= John Q. Public :0B5FOQAAANX[OPutAAAAIA--
subject DN: c=US,o= State of Washington PKI, ou= State of Washington, ou= Labor and Industry,cn= John A. Doe :0B5FOQAAANX[OPutAAAAIA--
subject DN: c=US,o= State of Washington PKI, ou= State of Washington, ou= Business Name ,cn= John A. Doe :0B5FOQAAANX[OPutAAAAIA--

Certificate Attribute/Extension	Value/Information
version	Version 3, which is INTEGER 2
serialNumber	INTEGER
Signature	sha-1WithRSAEncryption OID = 1.2.840.113549.1.1.5
issuer	cn= Washington State CA B1, ou= State of Washington CA, o=State of Washington PKI, c=US **OR** cn= Washington State CA B2, ou= State of Washington CA, o=State of Washington PKI, c=US
validity	Valid for 1 Year
subject	cn= John A. Doe :B5FOQAAANX[OPutAAAAIA--, ou=Labor and Industry, ou= State of Washington, o= State of Washington PKI, c=US A unique identifier is appended to the CN attribute as CN:unique identifier. The unique identifier is a 128 bit Universal Unique Identifier number Base64[6] encoded and published as a multivalued RDN to the subject DN. This will be used to ensure uniqueness in the Distinguished Name in case the common name is used more than once. 'cn' will be in the format 'First Name, Middle Initial Last Name' as shown above ou' is recommended to define state agency or business name in the case of a business certificate. If no affiliation (e.g., public citizen) then leave blank
subjectPublicKeyInfo	RSAEncryption OID = 1.2.840.113549.1.1.1 Parameters field present with NULL value

[6] The base64 encoding is a variant encoding utilizing the following character set "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789[ ]-"where we have replaced the +/= characters with the [ ]- characters eliminating directory reserved character conflicts with + / and = characters.

	RSA public key is a 1024 bit public key. RSA public key shall be encoded using the ASN.1 type RSAPublicKey: RSAPublicKey ::= SEQUENCE { Modulus INTEGER, -- n PublicExponent INTEGER -- e -- } Where modulus is the modulus n, and publicExponent is the public exponent e. The DER encoded RSAPublicKey is the value of the BIT STRING subjectPublicKey.
issuerUniqueIdentifier	Not Present
subjectUniqueIdentifier	Not Present
Extensions	
authorityKeyIdentifier	Present and not critical keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Subordinate CA certificate
subjectKeyIdentifier	Present and not critical keyIdentifier is SHA-1 hash of subjectPublicKey
keyUsage[7]	Present and critical digitalSignature = 1 nonRepudiation = 1 dataEncipherment = 0 keyEncipherment = 0 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
extKeyUsage	Not Present
privateKeyUsagePeriod	Not Present
certificatePolicies **Note that the User Notice Text is the final version. These notices must individually be encoded with the appropriate certificate Assurance Level of the certificate supplied to the user.**	Present and not critical This certificate extension defines the policy OID for the High, Intermediate, and Standard brand certificates define in the CP, the value of the OID is placed in the policyIdentifier field of this extension. The policy OID is a choice of: **High Assurance Level Certificate** id-HighAssuranceLevel ID::= {id-Stateofwashington 1 } → 2.16.840.1.113839.0.4.1 **Intermediate Assurance Level Certificate** id-IntermediateAssuranceLevel ID::= { id-Stateofwashington 2} → 2.16.840.1.113839.0.4.2 **Standard Assurance Level Certificate**[8] id-StandardAssuranceLevel ID::= { id-

[7] Standard certificates keyUsage will be set to have the following key usage bits - digital signature, nonRepudiation, dataEncipherment and keyEncipherment.

[8] Standard certificates do not apply to the Enterprise Certificates issued from the Entrust CA as these certificates do not reside in the subscriber's browser certificate data store.

	Stateofwashington 3 } → 2.16.840.1.113839.0.4.3
	
	PolicyQualifier[9] present
	PolicyQualifierInfo ::= SEQUENCE {
	PolicyQualifierId id-qt-unotice
	qualifier ANY DEFINED BY policyQualifierId }
	-- user notice qualifier
	UserNotice ::= SEQUENCE {
	explicitText = {
	HIGH USER Notice
	"CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$50,000.00"
	INTERMEDIATE USER Notice
	"CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$10,000.00"
	STANDARD USER Notice
	"CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$1,000.00"}}
	PolicyQualifierInfo
	PolicyQualifierId id-qt-cpsuri
	CpsUri ::= "PolicyQualifierId id-qt-cpsuri{ http://www.digsigtrust.com/certificates/policy/sowindex.html}
	Repeated for each policy along with userNotice.

policyMappings	Not Present
subjectAltName	Present and not critical Include RFC822 name = user email Address
issuerAltName	Not Present
subjectDirectoryAttributes	Not Present
basicConstraints	Not Present
nameConstraints	Not Present
policyConstraints	Not Present
authorityInfoAccess[10]	Present and not critical accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation ::= { http://ocspsow.digsigtrust.com } accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= { ldap://ldapsow.digsigtrust.com/cn=Washington State CA B1,ou=State of Washington CA,o=State

[9] PolicyQualifier is defined for all the State of Washington Policy OIDs and includes a User Notice explicitText for the particular assurance level certificate.

[10] The authorityInformationAccess extension is defined to allow for the future implementation of OCSP for certificate validation and is added to minimize future changes to the PKI infrastructure.

	of Washington PKI?cACertificate;binary } **OR** ldap://ldapsow.digsigtrust.com/cn=Washington State CA B2,ou=State of Washington CA,o=State of Washington PKI?cACertificate;binary }
cRLDistributionPoints[11]	Present and not critical DistributionPoint field is present and populated with pointer to CRL issued by Subordinate CA (e.g., URL ldap://ldapsow.digsigtrust.com/cn=Washington State CA B1,ou= State of Washington ,o=State of Washington PKI, c=US?certificateRevocationList;binary) **OR** Distribution Point Name: Full Name: Directory Address: CN=CRL1,CN=Washington State CA B2, OU=State of Washington CA,O=State of Washington PKI,C=US reasons and cRLIssuer fields not present

State of Washington Subscriber Signature Certificate Profile

[11] Entrust CA product automatically specifies the cRLDistributionPoint and is not under the control of DST to define. The cRLDistributionPoint is based on the Distinguished Name of the Certification Authority with the addition of a CN CRLx where x increments starting at 1 and going up as more than 750 revoked certificates are added on to the CRL1 then CRL2 is started.

2.6 State of Washington Subscriber Confidentiality Certificate Profile

The following profile defines encryption certificates that will be utilized within the State of Washington PKI for encryption. Although the sample subject DNs below illustrates possible Business and State Agency DNs, currently the only type of certificate that will be issued will be an individual subscriber certificate.

subject DN: c=US,o= State of Washington PKI, ou= State of Washington, cn= John Q. Public :0B5FOQAAANX[OPutAAAAIA--
subject DN: c=US,o= State of Washington PKI, ou= State of Washington, ou= Labor and Industry,cn= John A. Doe :0B5FOQAAANX[OPutAAAAIA--
subject DN: c=US,o= State of Washington PKI, ou= State of Washington, ou= Business Name ,cn= John A. Doe :0B5FOQAAANX[OPutAAAAIA--

Certificate Attribute/Extension	Value/Information
Version	version 3, which is INTEGER 2
SerialNumber	INTEGER
Signature	sha-1WithRSAEncryption OID = 1.2.840.113549.1.1.5
Issuer	cn= Washington State CA A1, ou= State of Washington CA, o=State of Washington PKI, c=US **OR** cn= Washington State CA A2, ou= State of Washington CA, o=State of Washington PKI, c=US
Validity	Valid for 1 year
Subject	cn=John A. Doe :0B5FOQAAANX[OPutAAAAIA--, ou=Labor and Industry, ou=State of Washington, o=State of Washington PKI, c=US A unique identifier is appended to the CN attribute as (CN:unique identifier). The unique identifier is a 128 bit Universal Unique Identifier number Based64[12] Encoded and published as a multivalued RDN to the subject DN. This will be used to ensure uniqueness in the Distinguished Name in case the common name is used more than once. 'cn' will be in the format 'First Name, Middle Initial, Last Name' as shown above. 'ou' is recommended to define state agency or business name in the case of a business certificate. If no affiliation (e.g., public citizen) then leave blank.
SubjectPublicKeyInfo	rSAEncryption OID = 1.2.840.113549.1.1.1 parameters field present with NULL value RSA public key is a 1024 bit public key.

[12] The base64 encoding is a variant encoding utilizing the following character set "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789[ ]-"where we have replaced the +/= characters with the [ ]- characters eliminating directory reserved character conflicts with + / and = characters.

	RSA public key shall be encoded using the ASN.1 type RSAPublicKey: RSAPublicKey ::= SEQUENCE { modulus INTEGER, -- n publicExponent INTEGER -- e -- } where modulus is the modulus n, and publicExponent is the public exponent e. The DER encoded RSAPublicKey is the value of the BIT STRING subjectPublicKey.
IssuerUniqueIdentifier	Not Present
subjectUniqueIdentifier	Not Present
Extensions	
authorityKeyIdentifier	Present and not critical keyIdentifier is the identifier defined in the subjectKeyIdentifier extension of the Subordinate CA certificate
subjectKeyIdentifier	Present and not critical keyIdentifier is SHA-1 hash of subjectPublicKey
keyUsage	Present and critical DigitalSignature = 0 nonRepudiation = 0 dataEncipherment = 1 keyEncipherment = 1 keyAgreement = 0 keyCertSign = 0 cRLSign = 0 encipherOnly = 0 decipherOnly = 0
extKeyUsage	Not Present
privateKeyUsagePeriod	Not Present
certificatePolicies **Note that the User Notice Text is the final version. These notices must individually be encoded with the appropriate certificate Assurance Level of the certificate supplied to the user.**	Present and not critical This certificate extension defines the policy OID for the High, Intermediate, and Standard brand certificates define in the CP, the value of the OID is placed in the policyIdentifier field of this extension. The policy OID is a choice of: **High Assurance Level Certificate** id-HighAssuranceLevel ID::= {id-Stateofwashington 1 } → 2.16.840.1.113839.0.4.1 **Intermediate Assurance Level Certificate** id-IntermediateAssuranceLevel ID::= { id-Stateofwashington 2} → 2.16.840.1.113839.0.4.2 **Standard Assurance Level Certificate** [13] id-StandardAssuranceLevel ID::= { id-Stateofwashington 3 } → 2.16.840.1.113839.0.4.3 PolicyQualifier[14] present

[13] Standard certificates do not apply to the Enterprise Certificates issued from the Entrust CA as these certificates do not reside in the Subscriber's browser certificate data store.

	PolicyQualifierInfo ::= SEQUENCE {
	PolicyQualifierId id-qt-unotice
	qualifier ANY DEFINED BY policyQualifierId }
	-- user notice qualifier
	UserNotice ::= SEQUENCE {
	explicitText = {
	HIGH USER Notice
	"CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$50,000.00"
	INTERMEDIATE USER Notice
	"CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$10,000.00"
	STANDARD USER Notice
	"CA liability is limited by Washington law and the Certificate Policy. Relying Party must verify Digital Signature and validate the Certificate used to create it. Recommended Reliance Limit =$1,000.00"}}
	PolicyQualifierInfo
	PolicyQualifierId id-qt-cpsuri
	CpsUri ::= "PolicyQualifierId id-qt-cpsuri{ http://www.digsigtrust.com/certificates/policy/sowindex.html}
	Repeated for each policy along with userNotice.

policyMappings	Not Present
subjectAltName	Present and not critical include RFC822 name = user email Address
issuerAltName	Not Present
subjectDirectoryAttributes	Not Present
basicConstraints	Not Present
nameConstraints	Not Present

[14] PolicyQualifier is defined for all the State of Washington Policy OIDs and includes a User Notice explicitText for the particular assurance level certificate.

policyConstraints	Not Present
authorityInfoAccess[15]	Present and not critical accessMethod ::={1.3.6.1.5.5.7.48.1} accessLocation ::= { http://ocspsow.digsigtrust.com } accessMethod ::={1.3.6.1.5.5.7.48.2} accessLocation ::= { ldap://ldapsow.digsigtrust.com/cn=Washington State CA B1,ou=State of Washington CA,o=State of Washington PKI?cACertificate;binary } **OR** ldap://ldapsow.digsigtrust.com/cn=Washington State CA B2,ou=State of Washington CA,o=State of Washington PKI?cACertificate;binary }
cRLDistributionPoints[16]	Present and not critical distributionPoint field is present and populated with pointer to CRL issued by Subordinate CA (e.g., URL= ldap://ldapsow.digsigtrust.com/cn=Washington State CA B1,ou= State of Washington CA, o=State of Washington PKI, c=US?certificateRevocationList;binary) **OR** Distribution Point Name: Full Name: Directory Address: CN=CRL1,CN=Washington State CA B2, OU=State of Washington CA,O=State of Washington PKI,C=US reasons and cRLIssuer fields not present

State of Washington Subscriber Confidentiality Certificate Profile

3. Early Adopters certificates differences

There are several minor differences to the certificates within the early adopters program that are documented as follows.

- Certificate validity period for all end entity certificates is 120 days
- The end entity certificates subject DN utilized an "OU=Early Adopter Test Certificate" instead of "OU=State of Washington".
- Early adopter certificates Certificate Policy extension user notice consisted of the following string for all three certificate assurance levels.

"Demo/Test Certificate for State of Washington PKI, No Reliance: All liability limited by Washington law."

[15] The authorityInformationAccess extension is defined to allow for the future implementation of OCSP for certificate validation and is added to minimize future changes to the PKI infrastructure.

[16] Entrust CA product automatically specifies the cRLDistributionPoint and is not under the control of DST to define. The cRLDistributionPoint is based on the Distinguished Name of the Certification Authority with the addition of a CN CRLx where x increments starting at 1 and going up as more than 750 revoked certificates are added on to the CRL1 then CRL2 is started.

Certificate Policy

for the

State of Washington

Public Key Infrastructure

Appendix B

Globally Unique Identifier

Creation of a Globally Unique Identifier

A Globally Unique Identifier (GUID), also called a Universally Unique Identifier, is appended to the Common Name (CN) attribute to create a unique Distinguished Name (DN), expressed by the following notation: "DN=CN:GUID". The GUID is a 128-bit unique number Base64 encoded used to ensure uniqueness in the Distinguished Name in case the Common Name is used more than once. The base64 encoding is a variant encoding and must result in a 24 character long string utilizing the following character set:

> ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789[ ]-
> where the + / = characters have been replaced with the [ ] - characters, respectively, eliminating directory reserved character conflicts with + / and = characters.

No other characters may be used. The GUID must be unique within the domain of Certificates issued by an Issuing CA, and must be unique across all other CA domains issuing certificates subject to this Policy.

Subscriber's Unique Name

Within the state of Washington PKI, a GUID is associated with the Subscriber's Common Name, and with the Issuing CA's Subscriber Account. Accounts are created when applicants register their information with an Issuing CA and a certificate is issued to them. Accounts remain active as long as Subscribers renew their certificate(s). An account is closed when the certificate expires before it is renewed, or when it is revoked. The GUID assigned to that account becomes invalid and the link between the GUID and the Subscriber's information disappears. However, when a certificate must be revoked due to suspected compromise, and a new certificate is immediately issued, or when an Issuing CA elects to revoke and re-issue in lieu of suspension as provided for in the State of Washington Certificate Policy (CP), the same GUID will be assigned to the Subscriber.

One person may have multiple accounts simultaneously, which means that one person may have multiple GUIDs. Having multiple GUIDs per person allows software applications to differentiate an individual performing roles in work and non-work settings.

First Time Certificate

When an application is approved and a certificate is ready for manufacturing, a GUID is created and inserted in the certificate. If the assurance level is standard, only one certificate is manufactured and the GUID is inserted in it. If assurance level is intermediate or high, two certificates, one encryption and one signing, are created and both will contain the same GUID.

Renewals

When a certificate is renewed, the new certificate(s) is(are) manufactured using the same GUID. Those two sets of certificates will have the same GUID for a short period of time. This overlap is due to the issuance of new certificate(s) before the original set is expired.

Upgrades

When an upgrade is requested prior to renewal, new certificates are manufactured using the same GUID. In this instance, multiple certificates will have the same GUID. The Subscriber may keep multiple certificates until the first set of certificates expires. From that time on, only the currently valid certificate(s) will have the same GUID.

Encryption Key Recoveries

When a key recovery is requested, two new certificates are manufactured using the GUID from the previous certificates. The previous certificates are revoked. In this instance, only two certificates will have the same GUID.