



**DIGITALSIGNATURETRUST**  
Guaranteeing Identity in Digital Transactions

**Certification Practice Statement**

**State of Washington**

Date Published:  
October 12, 2000

## Table of Contents

<b>1 INTRODUCTION .....</b>	<b>1</b>
1.1 OVERVIEW.....	1
1.2 IDENTIFICATION .....	11
1.3 COMMUNITY AND APPLICABILITY .....	11
1.4 CONTACT DETAILS.....	14
<b>2 GENERAL PROVISIONS.....</b>	<b>14</b>
2.1 APPORTIONING LEGAL RESPONSIBILITIES AMONG PARTIES.....	14
2.2 LIMITATION ON LIABILITY.....	20
2.3 FINANCIAL RESPONSIBILITY .....	21
2.4 INTERPRETATION AND ENFORCEMENT .....	22
2.5 FEES .....	24
2.6 NOTICE AND PUBLICATION .....	24
2.7 COMPLIANCE AUDITS.....	25
2.8 PRIVACY AND DATA PROTECTION POLICY.....	26
2.9 INTELLECTUAL PROPERTY RIGHTS.....	28
2.10 VALIDITY OF CERTIFICATES .....	28
<b>3 IDENTIFICATION AND AUTHENTICATION .....</b>	<b>28</b>
3.1 INITIAL REGISTRATION .....	28
3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY.....	30
3.3 RE-KEY AFTER REVOCATION.....	31
3.4 REVOCATION REQUEST .....	31
<b>4 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS .....</b>	<b>31</b>
4.1 CERTIFICATE REQUEST.....	31
4.2 CERTIFICATE APPLICATION VALIDATION.....	33
4.3 CERTIFICATE ISSUANCE .....	33
4.4 CERTIFICATE ACCEPTANCE .....	33
4.5 CERTIFICATE USAGE .....	34
4.6 ROUTINE CERTIFICATE RENEWAL.....	34
4.7 PROCESSING A REQUEST FOR A NEW KEY.....	34
4.8 CERTIFICATE MODIFICATIONS .....	34
4.9 CERTIFICATE REVOCATION.....	35
4.10 CERTIFICATE STATUS SERVICES.....	37
4.11 END OF SUBSCRIPTION.....	37
4.12 PRIVATE KEY RECOVERY .....	37
<b>5 CA FACILITY AND MANAGEMENT CONTROLS .....</b>	<b>37</b>
5.1 PHYSICAL CONTROLS .....	37
5.2 PROCEDURAL CONTROLS.....	38
5.3 PERSONNEL CONTROLS.....	39

5.4 SECURITY AUDIT PROCEDURES .....	40
5.5 RECORDS ARCHIVAL .....	41
5.6 KEY CHANGEOVER .....	42
5.7 COMPROMISE AND DISASTER RECOVERY .....	42
5.8 CA TERMINATION .....	43
5.9 CUSTOMER SERVICE .....	43
<b>6 TECHNICAL SECURITY CONTROLS .....</b>	<b>43</b>
6.1 KEY PAIR GENERATION AND INSTALLATION .....	43
6.2 CA PRIVATE KEY PROTECTION .....	43
6.3 OTHER ASPECTS OF KEY PAIR MANAGE-MENT .....	45
6.4 ACTIVATION DATA .....	45
6.5 COMPUTER SECURITY CONTROLS .....	45
6.6 LIFE CYCLE TECHNICAL CONTROLS .....	46
6.7 NETWORK SECURITY CONTROLS .....	46
6.8 CRYPTO-GRAPHIC MODULE ENGINEERING CONTROLS .....	46
<b>7 CERTIFICATE AND CRL PROFILES .....</b>	<b>46</b>
7.1 CERTIFICATE PROFILE .....	46
7.2 CRL PROFILE .....	48
<b>8 POLICY ADMINISTRATION .....</b>	<b>49</b>
8.1 CHANGE PROCEDURES .....	49
8.2 PUBLICATION AND NOTIFICATION POLICIES .....	49
8.3 CPS APPROVAL PROCEDURES .....	49
8.4 WAIVERS .....	49

# 1 INTRODUCTION

## 1.1 OVERVIEW

This Certification Practice Statement (CPS) describes the practices employed by Digital Signature Trust Co. (DST) to fulfill the requirements of the State of Washington Certificate Policy (CP). It describes the practices followed by DST in generating, issuing and revoking the types of Certificates identified in the CP and in this CPS. Many of the topics covered by this CPS are specifically addressed in the State of Washington CP, which is incorporated herein by reference. Unless otherwise indicated, all references to numbered sections refer to this CPS.

DST issues Certificates with three different assurance levels and Recommended Reliance Limits for the State of Washington PKI: High (\$50,000), Intermediate (\$10,000) and Standard (\$1,000). Within these assurance levels, Certificates are issued to certify a Private Key as being either for encryption (Confidentiality Key) or for digital signature (Digital Signature Key) purposes. DST issues only High and Intermediate Assurance Level Certificates for Confidentiality Keys.

### 1.1.1 Overview

DST's liability for the Certificates it issues for the State of Washington PKI and for its operations as a CA is limited by Washington law. Subscribers and Relying Parties not located in the State of Washington may obtain and/or rely upon Certificates issued under the State of Washington Certificate 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 separate agreement with DST.

Relying Parties that rely on a Certificate issued under the State of Washington CP that do not consent to Washington State jurisdiction and the Electronic Authentication Act, and who have not executed a private Relying Party Agreement with DST are subject to forfeiture of claims as provided in section 2.1.4.5.

As an Issuing CA for the State of Washington PKI, DST must maintain a CA license in the State of Washington. Information regarding the status of DST's license may be obtained from the State of Washington's Secretary of State, [http:// www.secstate.wa.gov](http://www.secstate.wa.gov).

1.1.2	General Definitions	Capitalized terms and acronyms used herein and in related agreements and other documents incorporating this CPS have the following meanings. Where substantive conflict occurs between the definition of a term as provided in this CPS and the definition in the State of Washington CP, the definition provided in the State of Washington CP will govern interpretation of the term.
	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).
	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, permittee 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 applications for Certificates, and conduct I&A of applicants in accordance with all applicable laws and the Policy.
	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 Root Key	The Private Key used to sign the CA Certificate and certify the CA's Public/Private Key Pair.
	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.
	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)** 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 the 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 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 the Certificate 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)	Also called a Universally Unique Identifier (UUID), a Globally Unique Identifier is a 128-bit (16-octets, represented in hexadecimal) long numeric string that is unique across time and space because it is calculated by an algorithm that uses Coordinated Universal Time (UTC) and the IEEE 802 Internet addressing scheme as variables. A GUID is associated with the Subscriber's account at the time that the account is created.
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).
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 entity authorized by DIS under the Certificate Policy who issues and manages Certificates asserting the State of Washington Certificate Policy.

**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 part of this CPS and applies only between DST and the State in its capacity as a party to the Master Contract.

**Online Certificate Status 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 that is legally recognized in its jurisdiction of origin (e.g., a company, corporation, partnership, sole proprietorship, government department ("Government Agencies"), 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	The State of Washington Certificate Policy, used interchangeably with State of Washington 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 the State of Washington CP and for resolving disputes between parties subject to the 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 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 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 Repository	<u>See</u> Repository.
Reasonable Reliance	<p>Reliance on a Digital Certificate is considered reasonable under the following conditions. The Relying Party has:</p> <ul style="list-style-type: none"> <li>• 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,</li> <li>• Complied with the requirements of the Certificate User Notice set forth in Section 7.1.8; and</li> <li>• Used the Certificate for purposes appropriate under the State of Washington CP, 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.</li> </ul>
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.

**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.

**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 the Policy.

**Relying Party** A Relying Party is an Individual or Organization who relies on a certificate issued under the terms of the Policy. A Relying Party's actions in reliance upon a certificate are reasonable when their actions constitute Reasonable Reliance as specified in the Policy.

**Relying Party Agreement** A Relying Party Agreement is an agreement between DST and any Individual or Organization under which the Individual or Organization has agreed to be bound by the Policy and this CPS.

**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.

**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, permittee 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 the 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 IDENTIFICATION**

Certificates issued by DST in accordance with the State of Washington CP have a base arc of: {joint-iso-ccitt (2) country (16) USA (840) organization (1) DST(113839) CP (0) StateofWashington (4)}. Specifically, the OIDs for the three assurance levels of Certificates issued under the State of Washington CP are 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

**1.3 COMMUNITY AND APPLICABILITY**

The relationships among the State of Washington, DST, Subscribers, Relying Parties and other parties are governed by the terms and conditions of the following documents: the Master Contract, where applicable, the State of Washington CP, this CPS, Subscriber Agreements, and Relying Party Agreements, where applicable.

- 1.3.1 The Policy Management Authority A committee comprised of individuals appointed by the Director of the Washington State Department of Information Services that advises the State of Washington Department of Information Services on policy matters and resolves disputes between parties served by the Certificate Policy.

- 1.3.1.1 Registration Authorities (RAs) DST will conduct in-person registration of potential Subscribers of High Assurance Certificates through Licensed Notaries, who while acting in their role as Licensed Notaries are not RAs of DST. DST

may, however, employ the services of insured depository institutions and insured credit unions, as those terms are defined in Title 12 of the United States Code (or affiliates or subsidiaries of such) to serve as Registration Authorities. DST's RAs are only responsible for duties assigned to them by agreement with DST.

- 1.3.1.2 Certificate Manufacturing Authorities (CMAs) No stipulation.
- 1.3.2 Repositories DST performs the role and functions of the Repository of the Certificates it issues under the State of Washington CP.
- 1.3.3 End entities
  - 1.3.3.1 Subscribers DST issues Certificates 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 may be an Individual or an Organization that Reasonably Relies on a Certificate in accordance with the State of Washington CP or a Relying Party Agreement with DST.
- 1.3.4 Applicability and Applications
  - 1.3.4.1 Determination of Acceptability of Certificate Type by Relying Party DST issues Certificates of three assurance levels under the State of Washington CP: Standard Assurance Level Certificates with a Recommended Reliance Limit of \$1,000; Intermediate Assurance Level Certificates with a Recommended Reliance Limit of \$10,000; and High Assurance Level Certificates with a Recommended Reliance Limit of \$50,000.

Relying Parties are responsible for determining whether a Certificate's assurance level is appropriate for the particular purpose or transaction. 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 CPS and the State of Washington CP;
- 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 trustworthy 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.

1.3.4.2 Purposes Certificates issued by DST may be used 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 issued by DST 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.

1.3.4.4 Cross-certification No Stipulation.

<b>1.4</b>	<b>CONTACT DETAILS</b>	Questions regarding the implementation and administration of this CPS should be directed to: Attn: Legal Department Digital Signature Trust Co. 255 North Admiral Byrd Road Salt Lake City UT 84116-3703 legal@TrustDST.com or 1-888-294-7831
<b>2</b>	<b>GENERAL PROVISIONS</b>	
<b>2.1</b>	<b>APPORTION- ING LEGAL RESPONSI- BILITIES AMONG PARTIES</b>	
2.1.1	CA Obligations, Representations and Liability	In issuing and managing Certificates, DST is primarily responsible for: <ul style="list-style-type: none"> <li>• Acceptance of completed applications and enrollment materials for Certificates from potential Subscribers and RAs;</li> <li>• Identification and authentication of Subscribers and RAs;</li> <li>• The manufacturing and issuance of Certificates;</li> <li>• Publication, suspension, revocation and renewal of Certificates; and</li> <li>• Management of CA operations and infrastructure related to Certificates in accordance with the requirements, representations, and warranties of the State of Washington CP.</li> </ul>
2.1.1.1	Notification of certificate issuance and revocation	DST notifies Subscribers when their Certificate has been issued or revoked and publishes Certificates and CRLs in accordance with the practices set forth herein.
2.1.1.2	Accuracy of representations	By issuing a Certificate, DST certifies and warrants to Subscribers, and to all Relying Parties who Reasonably Rely on the information contained in the Certificate during its operational period and in accordance with the State of Washington CP, that:

- It has issued, and will manage, the Certificate in accordance with the CP;
- It has complied with the requirements of the CP and this CPS when authenticating the Subscriber and issuing the Certificate;
- That it knows of no misrepresentations of fact in the Certificate and has taken reasonable steps to verify the information in the Certificate;
- Information provided to it during the certificate application process has been accurately transcribed to the Certificate; and
- The Certificate meets all material requirements of this CPS and the CP.

2.1.1.3	Time between certificate request and issuance	Following completion of I&A, DST issues Certificates within three business (3) days.
2.1.1.4	Certificate revocation and renewal	Procedures for the expiration, revocation and renewal of a Certificate may be found in the relevant Subscriber Agreement and applicable sections of the Certificate Policy.
2.1.1.5	Protection of Private Keys	DST's practices in protecting its Private Keys and Activation Data are set forth in Parts 4 and 6.
2.1.1.6	Restrictions on Issuing CA's Private Key use	DST uses its CA Private Signing Key only to sign Certificates and CRLs.
2.1.1.7	Assure Compliance	DST's compliance with its I&A obligations is presumed to have been determined as set forth in Section 3.1.
2.1.1.8	Consequences of Breach	EXCEPT AS EXPRESSLY PROHIBITED BY THE STATE OF WASHINGTON CP, DST DISCLAIMS ALL LIABILITY TO THE MAXIMUM EXTENT ALLOWED BY RCW § 19.34.280 AND WASHINGTON LAW, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND OF ACCURACY OF INFORMATION PROVIDED.
2.1.2	RA Obligations, Representations and Liability	DST may delegate portions of the I&A process described in Section 3.1 to Registration Authorities.

- |         |   |  |
|---------|---|--|
| 2.1.2.1 | Notification of certificate issuance and revocation       | DST, and not RAs, is responsible for notifying Subscribers and Relying Parties of the issuance or revocation of Certificates.  |
| 2.1.2.2 | Accuracy of representations                               | When an RA submits Subscriber information to DST, it certifies that it has properly authenticated the identity of that Subscriber.   |
| 2.1.2.3 | Protection of Private Keys                                | An RA must protect its Private Key(s) and request revocation in the event that an RA's Private Key is lost, stolen or otherwise compromised.   |
| 2.1.2.4 | Restrictions on Private Key use                           | An RA's keys used to access and operate RA Applications may not be used for any other purpose.   |
| 2.1.2.5 | RA Security and Operations Manual                         | All RAs must comply with all RA-related instructions received from DST.  |
| 2.1.2.6 | Consequences of Breach                                    | An RA shall indemnify, hold harmless and defend DST against damages and claims arising from or pertaining to the alleged or proven failure of the RA to comply with the terms of the State of Washington CP and any applicable agreement with DST; PROVIDED, HOWEVER that DST will retain primary responsibility for any such damages and claims.  |
| 2.1.3   | Subscriber Obligations, Representations and Liability     | Subscribers must agree to the obligations outlined below. For the State of Washington PKI, Subscriber Agreements for Standard and Intermediate Assurance Level Certificates are comprised of an online, click-wrap agreement. Additionally, the application process for High Assurance Level Certificates includes a printed, signed and notarized form. Subscribers' obligations under the Subscriber Agreements consist of the following:  |
| 2.1.3.1 | Standard Assurance Level Certificate Subscriber Agreement | <ul style="list-style-type: none"> <li>• Provide current, complete, true and non-misleading information as appropriately required by DST;</li> <li>• Generate a Key Pair for Digital Signature purposes and submit the corresponding Public Key to DST;</li> <li>• Review the proposed contents of the Certificate to be issued; notify DST of any errors or problems, and represent and warrant to DST that all information provided by the Subscriber to DST, and all information contained in the Certificate and identifying the Subscriber, are current, complete, true and not misleading;</li> <li>• Pay the applicable fees for Certificate issuance and renewal;</li> </ul> |

- Not use the Certificate for any prohibited purpose;
- Protect the Private Key by (i) storing the Private Key in a browser; (ii) protecting access to the Private Key by a PIN or password; and (iii) taking other reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, the Private Key, any Activation Data and the computer system or media on which the Private Key is stored;
- Request revocation of the Certificate if (i) the name in the Certificate is no longer current, complete or true; or (ii) the Subscriber ever discovers or suspects that the Private Key has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way;
- Cease using the Certificate under any circumstances requiring revocation;
- Indemnify DST and its directors, officers, employees and agents for loss or damage arising from or pertaining to wrongful or negligent acts or omissions of the Subscriber, including (i) material misrepresentation or omission of facts by the Subscriber; (ii) Subscriber violation of the Subscriber Agreement; (iii) compromise or unauthorized use of the Certificate, due to the compromise of the Private Key, unless prior to such unauthorized use the Subscriber has appropriately requested revocation of the Certificate; or (iv) the Subscriber's misuse of the Certificate or the Private Key; and
- Attempt to resolve disputes by negotiation and/or mediation, and submit irresolvable disputes to the PMA for resolution.

- 2.1.3.2 Intermediate Assurance Level Certificate Subscriber Agreement
- Provide current, complete, true and non-misleading information as appropriately required by DST;
  - Generate a Key Pair for Digital Signature purposes and submit the corresponding Public Key to DST (the Key Pair for encryption/decryption may be generated either by the Subscriber or by DST (to support Encryption Key Recovery));
  - Review the proposed contents of the Certificate(s) to be issued to the Subscriber; notify DST of any errors or problems, and represent and warrant to DST that all information provided by the Subscriber to DST, and all information contained in the Certificate and identifying the Subscriber, are current, complete, true and not misleading;
  - Pay the applicable fees for Certificate issuance and renewal;
  - Not use the Certificate(s) for any prohibited purpose;
  - Protect the Private Key(s) by (i) storing the Private Key only in (a) a Hardware Token, or (b) a Software Cryptomodule that requires the entry of Activation Data in order to access Key information; (ii) protecting access to Hardware Token or Software Cryptomodule by a Strong PIN or Password; and (iii) taking other

reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, the Private Key, any Activation Data and the computer system or media on which the Private Key is stored;

- Request revocation of the Certificate if (i) the name in the Certificate is no longer current, complete or true; or (ii) the Subscriber ever discovers or suspects that the Private Key has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way;
- Cease using the Certificate under any circumstances requiring revocation;
- Indemnify DST and its directors, officers, employees and agents for loss or damage arising from or pertaining to wrongful or negligent acts or omissions of the Subscriber, including (i) material misrepresentation or omission of facts by the Subscriber; (ii) Subscriber violation of the Subscriber Agreement; (iii) compromise or unauthorized use of the Certificate due to the compromise of the Private Key, unless prior to such unauthorized use the Subscriber has appropriately requested revocation of the Certificate; or (iv) the Subscriber's misuse of the Certificate or the Private Key; and
- Attempt to resolve disputes by negotiation and/or mediation, and submit irresolvable disputes to the PMA for resolution.

- 2.1.3.3 High Assurance Level Certificate Subscriber Agreement
- Provide current, complete, true and non-misleading information as appropriately required by DST;
  - Generate a Key Pair for Digital Signature purposes and submit the corresponding Public Key to DST (the Key Pair for encryption/decryption may be generated either by the Subscriber or by DST (to support Encryption Key Recovery));
  - Complete an "Identification Form and Acknowledgement," and appear before a Licensed Notary with the required two forms of identification;
  - Review the proposed contents of the Certificate(s) to be issued to the Subscriber; notify DST of any errors or problems, and represent and warrant to DST that all information provided by the Subscriber to DST, and all information contained in the Certificate and identifying the Subscriber, are current, complete, true and not misleading;
  - Pay the applicable fees for Certificate issuance and renewal;
  - Not use the Certificate(s) for any prohibited purpose;
  - Protect the Private Key(s) by (i) storing the Private Key only in (a) a Hardware Token, or (b) a Software Cryptomodule that requires the entry of Activation Data in order to access Key information; (ii) protecting access to Hardware Token or Software Cryptomodule by a Strong PIN or Password; and (iii) taking other

reasonable security measures to prevent unauthorized access to, or disclosure, loss, modification, compromise, or use of, the Private Key, any Activation Data and the computer system or media on which the Private Key is stored;

- Request revocation of the Certificate if (i) the name in the Certificate is no longer current, complete or true; or (ii) the Subscriber ever discovers or suspects that the Private Key has been or is in danger of being lost, disclosed, compromised or subjected to unauthorized use in any way;
  - Cease using the Certificate under any circumstances requiring revocation;
  - Indemnify DST and its directors, officers, employees and agents for loss or damage arising from or pertaining to wrongful or negligent acts or omissions of the Subscriber, including (i) material misrepresentation or omission of facts by the Subscriber; (ii) Subscriber violation of the Subscriber Agreement; (iii) compromise or unauthorized use of the Certificate due to the compromise of the Private Key, unless prior to such unauthorized use the Subscriber has appropriately requested revocation of the Certificate; or (iv) the Subscriber's misuse of the Certificate or the Private Key;
- and
- Attempt to resolve disputes by negotiation and/or mediation, and submit irresolvable disputes to the PMA for resolution.

2.1.4	Relying Party Obligations, Representations and Liability	Prior to relying on or using a Certificate issued by DST, 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 State of Washington CP;
2.1.4.2	Verification responsibilities	For Digital Signatures, verify that the Digital Signature was created using the Private Key corresponding to the Public Key listed in the Certificate that was valid at the time of such signing,
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); and
2.1.4.4	Reasonable Reliance	Rely on the Certificate only under circumstances constituting Reasonable Reliance as defined in 1.1.2 of the State of Washington CP.

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 DST or an 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 the Policy, then the Relying Party forfeits any claim in excess of that which would be permitted under Washington law.
2.2	<b>LIMITATION ON LIABILITY</b>	UNLESS OTHERWISE PROHIBITED BY FEDERAL LAW, OR OTHERWISE STIPULATED IN A RELYING PARTY AGREEMENT BETWEEN DST AND THE RELYING PARTY, PARTIES THAT CHOOSE TO RELY ON ANY CERTIFICATE ISSUED UNDER THIS CPS CONSENT TO THE LIMITATIONS OF LIABILITY ESTABLISHED BY WASHINGTON LAW AND THE STATE OF WASHINGTON CP, REGARDLESS OF JURISDICTION, CHOICE OF LAW POLICIES, PLACE OF PERFORMANCE, DOMICILE OF PARTIES OR MINIMUM CONTACTS, INCLUDING THE FOLLOWING PROVISIONS WHICH PROVIDE THAT NEITHER DST NOR ANY RA SHALL BE LIABLE FOR:
2.2.1	Policy Compliance as a Defense	Any loss caused by reliance on a false or forged Certificate, if DST or its RA complied with all material requirements of the State of Washington CP;
2.2.2	Application of Recommended Reliance Limits	<p>Any loss in excess of the Recommended Reliance Limits stated below that is caused by reliance upon (1) a misrepresentation in a Certificate of a fact that DST or any RA is required to confirm, or (2) for any breach of the representations made by DST and/or RA in the State of Washington CP, and/or (3) for failure to comply with the requirements for issuance of a certificate under the laws of the State of Washington:</p> <ul style="list-style-type: none"> <li>• High Assurance Level Certificate – Recommended Reliance Limit: \$50,000.00;</li> <li>• Intermediate Assurance Level Certificate – Recommended Reliance Limit: \$10,000.00; and</li> <li>• Standard Assurance Level Certificate – Recommended Reliance Limit: \$1,000.00.</li> </ul>
2.2.3	No Personal Injury	Any damages for personal injury, pain and suffering, or emotional distress;

- |       |                          |  |
|-------|--------------------------|--|
| 2.2.4 | No Consequential Damages | 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      | 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 by DST, to the extent permitted by law, any damages awarded shall be reduced 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 RESPONSIBILITY***

2.3.1.1    Financial Assurance

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

2.3.1.1.2    Registration Authorities    RAs shall maintain adequate financial assurance in the form and amount deemed appropriate by DST.

2.3.1.2    Insurance

2.3.1.2.1    An Issuing CA    DST shall maintain the following insurance coverage, naming the State of Washington as an additional insured, and covering DST, 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 DST may require RAs to obtain and maintain professional liability error and omissions and crime coverage insurance in the form and amount deemed appropriate by DST.
- 2.3.1.3 Consequences of failure to meet Financial Responsibilities See Section 2.3.1.3 of the State of Washington CP.
- 2.3.1.4 Indemnification DST reserves the right to 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 DST loss, either financially or in reputation. However, the indemnification shall not relieve DST from its primary responsibilities to others who are not parties to the indemnification agreement.
- 2.3.1.4.1 Issuing CA DST 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 DST against any claims arising from or pertaining to wrongful or negligent acts or omissions of an 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 By issuing a Certificate, DST and its RA do not become an agent, fiduciary, trustee, or other representative of a Subscriber or Relying Party.

**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 CPS unless otherwise provided in an agreement with DST.

2.4.2 Specific Provisions: severability, survival, merger, and notice DST will include provisions governing severability, survival, merger or notice in its agreements with Subscribers and Relying Parties, as appropriate.

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 CPS 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 DST and an RA and pertains to the interpretation of this CPS or the State of Washington CP, 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** DST charges fees to entities governed by the Master Contract in accordance with the fee structure of the Master Contract. Other parties not governed by the Master Contract shall pay fees as provided in a published fee schedule or separate agreement with DST. Notice of any fee charged to a Subscriber or Relying Party must be brought to the attention of that entity.

DST may establish and charge other reasonable fees. DST may charge a fee for key recovery services for Confidentiality Keys, except as provided by the Master Contract. However, no fee may be charged for access to review the provisions of this CPS or the State of Washington CP.

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 DST operates a secure on-line Repository available to Relying Parties that contains (1) issued Certificates that reference the Washington State Certificate Policy, (2) a Certificate Revocation List ("CRL") or on-line certificate status database, (3) DST's Certificate for its CA Private Signing Key, (4) past and current versions of this CPS, (5) a copy of the State of Washington CP, and (6) other relevant information relating to State of Washington Certificates.

2.6.2 Frequency of publication Certificates are published following the Subscriber acceptance procedure specified in Section 4.4. The CRL is published as specified in Section 4.9.

2.6.3 Access controls DST does not impose access controls on the State of Washington CP, its CA Certificate, or past and current versions of this CPS. DST may impose access controls on Certificates and certificate status information, in accordance with the State of Washington CP.

2.6.4 Location DST's X.500 directory and LDAP interface can be located as follows: ldap://ldapsow.digsigtrust.com/cn=Washington State CA A1, ou=State of Washington CA, o=Digital Signature Trust Co.?cACertificate;binary }

2.6.5 Revocation Information In addition to obtaining information from the location identified in 2.6.4, a party may obtain revocation information from a CRL located as follows: ldap://ldapsow.digsigtrust.com/cn=Washington State CA A1, ou=Washington State CA, o=Digital Signature Trust Co., c=US?certificateRevocationList;binary).

## **2.7 COMPLIANCE AUDITS**

- 2.7.1 Frequency DST shall submit to compliance audits as frequently as required to maintain its license under Washington law.
- 2.7.2 Identity and Qualifications of Auditor DST operates under the regulatory oversight and auditing of the Office of the Comptroller of the Currency (the "OCC"). DST also retains the services of internationally-recognized and well-respected accounting and information security firms who examine and audit DST's computer facilities and operations for security, fault tolerance and service commitments. DST assures that the auditor chosen annually will be qualified and sufficiently familiar with Washington law and DST's practices to perform an audit acceptable to the State of Washington.
- 2.7.3 Auditor's Neutrality DST's auditor(s) shall have no other relationship with DST that could constitute a conflict of interest. These relationships include financial, legal, social or other relationships that could result in a conflict of interest.
- 2.7.4 Scope of Audit The scope and substance of the compliance audits performed on DST's CA operations shall meet those required under Washington law to maintain licensure as a Certification Authority.
- 2.7.5 Communication of Results The results of any inspection or audit are reported to DST 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, the State of Washington CP or any other contractual obligations to the State, DST shall develop a plan to cure such noncompliance, subject to DIS approval. In the event DST 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 DST or an RA are considered confidential and shall be used only for the purpose of providing CA Services. Regardless of whether Private and/or personally identifiable Information is collected by DST or an RA, DST will have primary responsibility for ensuring that such information is kept in confidence in accordance with the CP.
- 2.8.1 Sensitivity of Types of Private Information.
- 2.8.1.1 Private/Confidential Information DST shall not disclose any Subscriber Information that is considered private and/or confidential by the State of Washington CP 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 Private Keys shall be kept confidential. Any key information disclosure by a Subscriber is at the Subscriber's own risk. Any Private Keys held by DST 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 CA or RA equipment is handled as sensitive, and access is restricted to those with an official need-to-know in order to perform their official duties. Private Keys used to sign Certificates asserting security privileges are classified at the same level as the privileges that are to be asserted. In any cases where DST does not independently verify security privilege information, RAs are required to perform such verification.
- 2.8.1.1.3 Audit Information Audit information is considered sensitive and may not be disclosed to anyone for any purpose other than for auditing and mandatory reporting requirements, or as 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 confidential. However, such information may not be used by any Individual or Organization other than as permitted by the State of Washington CP or as allowed by agreement of the party whose information is used with DST.

Information pertaining to CA management of Certificates, such as compilations of certificate information, shall be treated as confidential by any party subject to the 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   | DST collects only such personal Subscriber information as is necessary for the issuance of a Certificate. DST requests non-certificate information to properly identify Subscribers (e.g., business or home addresses and telephone numbers).   |
| 2.8.3 | Permitted Use of Private Information by Acquirer.          | Personal information collected for the purposes of Certificate issuance, maintenance and revocation is used only for such purposes.   |
| 2.8.4 | Permitted Distribution of Private Information by Acquirer. | DST may distribute personal information with a Subscriber's express written consent, or as required by law or court order.  |
| 2.8.5 | Opportunity of Owner to Correct Private Information.       | DST makes personal information available to, and subject to correction by, the Subscriber following an appropriate request by the Subscriber;   |
| 2.8.6 | Release of Information to Law Enforcement Officials.       | DST does not disclose Certificate or Certificate-related information to any law enforcement agency, except when: (a) authorized by the State of Washington CP; (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. Unless prohibited by law, DST shall give all interested persons or parties reasonable prior written notice before making any disclosure of Certificate or Certificate-related information. Except as provided herein, DST will not disclose confidential information notwithstanding the status of a Certificate (current or revoked) or the status of DST.                        |

2.8.8 Other information releases Except as provided above, DST will not disclose private and/or confidential information, unless it obtains the Subscriber's express written consent.

**2.9** **INTELLECTUAL PROPERTY RIGHTS** This CPS is copyrighted by DST.

**2.10** **VALIDITY OF CERTIFICATES**

2.10.1 Acceptance. See Section 4.4.

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 Relying Parties may elect to rely, at their own risk, 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 is not deemed "Reasonable Reliance."

**3** **IDENTIFICATION AND AUTHENTICATION**

**3.1** **INITIAL REGISTRATION** DST receives applications directly from potential Subscribers or through Authenticating RAs either electronically via e-mail or Web site as provided in Section 4.1.2. A Subscriber's account with DST is created when an applicant registers his or her information with DST and a certificate is issued. Upon account creation, a GUID is associated with the Subscriber's account. A Subscriber's account GUID remains the same as long as the Subscriber renews the Certificate as provided below in Section 3.2, or if DST elects to revoke and re-issue a Certificate in lieu of suspension.

3.1.1 Types of names The format of allowed names is set forth in Section 3.1.1 of the State of Washington CP.

3.1.2 Need for names to be meaningful See Section 3.1.2 of the State of Washington CP.

- 3.1.3 Rules for interpreting various name forms See Section 3.1.3 of the State of Washington CP.
- 3.1.4 Uniqueness of names See Section 3.1.4 of the State of Washington CP.
- 3.1.5 Name claim dispute resolution procedure See Section 3.1.5 of the State of Washington CP.
- 3.1.6 Recognition, authentication, and role of trademarks See Section 3.1.6 of the State of Washington CP.
- 3.1.7 Method to prove possession of Private Key Proof of Possession for the Digital Signature Key is accomplished when the Subscriber submits a signed request for a Certificate containing the Public Key of the Key Pair signed with the Private Key.

For Confidentiality Keys, DST generates both a Key Pair and a Certificate for the Confidentiality Key. DST inserts the Public Key to create the Certificate, and sends the Certificate to the Subscriber along with the Private Confidentiality Key. DST securely stores a copy of the Subscriber's Private Confidentiality Key to provide key recovery services and protect against the loss of data.

In the case where the Private Key is generated directly on a Hardware Token, or in a key generator that benignly transfers the Key to the Hardware Token, 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 Hardware Token when the Key is generated, then DST immediately delivers the Hardware Token to the Subscriber via a trustworthy and accountable method.

- 3.1.8 I&A Procedures DST's procedures for conducting I&A are as stated in Section 3.1.8 of the State of Washington CP. Section 4.1.2 of this CPS describes the information collected by DST for Third Party Identity Proofing.
- 3.1.9 Electronic Devices DST will issue Certificates to Electronic Devices in accordance with Section 3.1.9 of the State of Washington CP, only after it has

established the identity and authority of the Individual responsible for the Electronic Device in accordance with the requirements of Section 3.1.8 of the State of Washington CP.

**3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY**

- 3.2.1 Certificate re-key Beginning three months prior to the scheduled expiration of a Certificate, a Subscriber may request Certification of a new Key Pair by DST, provided that the original Certificate has not been suspended or revoked. The Subscriber's identity does not need to be verified (no I&A is required). In such case, the Subscriber's account GUID remains unchanged and the same GUID will appear in the subsequent Certificate. Renewal of a Certificate establishing a Subscriber's affiliation with an Organization shall require verification that the affiliation still exists
- 3.2.2 Certificate renewal Beginning three months prior to the scheduled expiration of a Certificate, a Subscriber may request Certificate renewal. At such time, the Subscriber will be notified via e-mail and instructed on certificate renewal or, in the case of automatic renewal, client software may initiate the renewal process without additional Subscriber intervention. For Confidentiality Keys, the process may involve re-certification of the archived Private Confidentiality Key. In the cases of certificate renewal, as with re-keying pursuant to 3.2.1, the Subscriber's account GUID remains unchanged and appears in the new Certificate.
- 3.2.3 Certificate update Except as otherwise provided, when Certificates are updated, the updated Certificates are manufactured using the same GUID as the current existing Certificates when presented to DST by the Subscriber with the update request.

**3.3 RE-KEY AFTER REVOCATION** Revoked or expired Certificates may not be renewed. Applicants without a valid Certificate must be re-authenticated by DST or an RA, just as with a first-time application. The Subscriber's 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 no longer exists except when DST chooses to revoke a Certificate in lieu of suspension, in which case the newly issued Certificate will contain the same GUID.

**3.4 REVOCATION REQUEST** All revocation requests are verified by DST before any revocation is performed. A Subscriber may request a revocation of their own certificate, a Sponsoring Organization may request the revocation of a certificate they approved, or DST may determine that a Private Key has been compromised and revoke a Certificate. In all cases, DST promptly notifies the Subscriber of the revocation.

#### **4 CERTIFICATE LIFE CYCLE OPERATIONAL REQUIREMENTS**

**4.1 CERTIFICATE REQUEST** After properly authenticating a certificate request, DST will issue a Certificate to the appropriate Cryptomodule (Software Cryptomodule or Hardware Token) or browser and perform the appropriate lifecycle management for the Certificate (e.g., renewals, revocations and encryption key recovery) as appropriate.

**4.1.1 Who Can Request a Certificate** The certificate application process may be initiated by the persons identified in Section 3.1.

**4.1.2 Certificate Request Process** The process to request a Certificate will depend on the type of certificate to be issued, but will include at least the following:

- Information sufficient to successfully complete I&A required by Section 3.1;
- the Public Key for each Certificate requested;
- proof that the Public Key forms a functioning Key Pair with the Private Key; and
- a point of contact for verification of any roles or authorizations requested.

The applicant will submit the following initial identity information to DST through a Web site using an encrypted session to ensure the accuracy and confidentiality of the information:

Name (also former last name if changed in last 12 months)

Home Address (street address)

Social Security Number

Date of Birth

Photo ID Number

Government entity issuing Photo ID

Photo ID Expiration Date

E-mail Address

Work Phone (Daytime Phone)

Home Phone

Contemporaneously with initial registration, the applicant also creates a passphrase of at least eight (8) characters to be used for certificate retrieval.

- 4.1.2.1 High Assurance Level Certificates Upon completing the steps identified in Section 4.1.2, the applicant for a High Assurance Level Certificate must print out an Identification Form and Acknowledgment ("ID Form"). The applicant takes the ID Form to a Licensed Notary and must present the Licensed Notary with the two forms of identification specified in Section 3.1.8 of the State of Washington CP. One of the forms of identification must be the current, state-issued ID card or drivers license that the applicant reported to DST on the application screen. The Licensed Notary notarizes the ID Form and attaches photocopies of the two forms of ID to the ID Form. The applicant sends the notarized ID Form to DST, and DST acknowledges receipt of the ID Form via e-mail to the applicant. Upon successful completion of I&A, information is sent to the applicant explaining how to generate the Key Pairs and receive Certificates for the Key Pairs. If the Key is to be stored in a Hardware Token, Activation Data is sent to the applicant separately from the Hardware Token. If the Keys are to be stored in a Software Module, Activation Data is sent to the applicant through separate communication channels. The passphrase created by the applicant at the time of certificate application is used in conjunction with the Activation Data to receive the Certificates.
- 4.1.2.2 Intermediate Assurance Level Certificates Following successful completion of the steps identified in Section 4.1.2 and successful I&A of the applicant for an Intermediate Assurance Level Certificate, information is sent to the applicant explaining how to generate the Key Pairs and receive Certificates for the Key Pairs. If the Keys are to be stored in Hardware Tokens, Activation Data is sent to the applicant separately from the Hardware Token. If the Keys are to be stored in a Software Module, Activation

Data is sent to the applicant through separate communication channels. The passphrase created by the applicant at the time of certificate application is used in conjunction with the Activation Data to receive the Certificates.

4.1.2.3 Standard Assurance Level Certificates Following successful completion of the steps identified in Section 4.1.2 and successful I&A of the applicant for a Standard Assurance Level Certificate, DST sends an activation code to the applicant and explains how to use the activation code in conjunction with the passphrase created at the time of certificate application to generate the Key Pair and receive the Certificate for the Key Pair.

4.1.3 Time to Process a Certificate Request See Section 2.1.1.3, above.

4.1.4 Application for Cross-certificate No Stipulation.

**4.2 CERTIFICATE APPLICATION VALIDATION** No Stipulation.

**4.3 CERTIFICATE ISSUANCE**

4.3.1 Applicant Notification DST notifies only certificate applicants via U.S. mail and/or e-mail that their Certificate is ready for retrieval.

4.3.2 Issuance by CA The Out-of-Band notification process, linked to the Certificate applicant's physical U.S. postal mail address, is used to initiate the delivery of the Certificate to the Subscriber. The applicant is instructed to return to the DST Web site and retrieve the Certificate using both the passphrase created by the applicant during initial registration and the Activation Data provided by DST.

4.3.3 Notification of Certificate Issuance to Subscribers Upon delivery of the Certificate to the Subscriber, DST notifies the Subscriber via the Web site used for certificate retrieval that the Certificate has been successfully issued.

**4.4 CERTIFICATE ACCEPTANCE**

4.4.1 Certificate Acceptance by the Subscriber Subscribers are advised via Subscriber Agreements that failing to notify DST of any problems or errors with a Certificate within a reasonable time of downloading or retrieving it, or by using a

Certificate, they accept the Certificate, warrant the accuracy of its contents and agree to the obligations of Section 2.1.3.

- 4.4.2 Notification of Certificate Issuance to Others Notification of certificate issuance to others is effectuated by publication of the Certificate in DST's Repository.
- 4.5 CERTIFICATE USAGE** Certificates may be used only as allowed by the State of Washington CP.
- 4.6 ROUTINE CERTIFICATE RENEWAL** Routine certificate renewal may be performed by automatic renewal or re-certification 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, DST does not perform complete re-certification of the Subscriber through complete I&A.
- 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 necessary 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 DST uses the same notification procedures for a new key certification with an existing Subscriber as it does with a request from a new Subscriber.
- 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's 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 CPS, the State of Washington CP, or any other agreement, regulation, or law applicable to the Certificate. 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 any material information on the Certificate changes or becomes obsolete; whenever the Private Key, or the media holding the Private Key, associated with the Certificate is known or suspected of being compromised; whenever an affiliated Individual is no longer affiliated with a Sponsoring Organization. For the purposes of this section, the State of Washington as a whole is deemed to be a Sponsoring Organization, so that a transfer of one department to another is not a termination in affiliation.

DST will 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 the State of Washington CP, this CPS or any other agreement, regulation, or law applicable to the Certificate; if knowledge or reasonable suspicion of compromise is obtained; if DST determines that the Certificate was not properly issued; or if there are any other grounds for revocation.

### **4.9.2 Who Can Request Revocation**

DST may revoke Certificates, 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 another authorized party, provided that notice and cause are given. 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 All certificate revocation requests should be promptly communicated to DST, either directly or through an RA. A request for revocation should be accompanied by adequate proof of identity, either by using the Private Key for the Certificate to be revoked or by personally contacting DST or an RA and providing adequate proof of identity.
- Revocation Request Grace Period DST will 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 In accordance with RCW §19.34.250, DST shall suspend a Certificate only upon receiving an order of suspension from the Secretary of State. If necessary due to technical requirements, DST's suspension procedure may be to temporarily revoke and then reissue the Certificate at no charge to the Subscriber. In such case, the Subscriber's account GUID remains unchanged and the same GUID will appear in the new Certificate. In the event of a suspension, DST shall give notice to the Subscriber as soon as practicable after a decision to suspend pursuant to an order from the Secretary of State.
- 4.9.4 Time to Process a Revocation Request Upon revocation of a Certificate, DST promptly updates the status of the Certificate in its database and publishes a new CRL.
- 4.9.5 Certificate Revocation Lists
- 4.9.5.1 CRL Issuance Frequency DST issues a new CRL every 24 hours, even if there are no changes or updates to be made (Periodic CRLs). However, CRLs may be issued more frequently (Interim CRLs). DST posts an Interim CRL within six hours after it has been notified of key compromise or received a revocation request. The superceded CRL is then removed from the directory system. All CRLs issued by DST for the State of Washington PKI have a validity period of no more than 36 hours.
- 4.9.5.2 CRL Latency DST will publish an Interim CRL as soon as possible following the revocation of a Certificate.
- 4.9.6 On-line Revocation/ Status Checking DST's certificate database is updated immediately upon revocation and should be checked prior to reliance on a Certificate.

Online Revocation/Status Checking Availability DST supports OCSP. Relying Party applications require a compatible OCSP requester to use the OCSP capabilities of the certificate database.

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 No Stipulation.

**4.10 CERTIFICATE STATUS SERVICES** All Certificates are created with a CRL Distribution Point (CDP) (see Sections 2.6.5 and 7.2.2) and an Authority Info Access (AIA) (for using OCSP). The CDP and AIA contain the locations where the Certificate can be validated. (See Section 2.6.4).

**4.11 END OF SUBSCRIPTION** No Stipulation.

**4.12 PRIVATE KEY RECOVERY** See Section 6.2.3.

## 5 CA FACILITY AND MANAGEMENT CONTROLS

### 5.1 PHYSICAL CONTROLS

5.1.1 Site location and construction DST's CA operations are housed in a secure, cement/masonry hardened building, which has been designed and constructed to meet Seismic Level 4 building standards.

5.1.2 Physical access The building exterior doors and interior rooms housing CA equipment are equipped with cipher locks. When not in use, DST's CA Cryptomodules are inactivated and placed in locked containers. Activation Data used to access or enable the Cryptomodules or CA equipment is stored separately in secure containers. All CA systems may only be activated under the dual control of two separate individuals.  
The secure facility housing DST's CA systems is also equipped with physical intrusion detection, closed circuit video surveillance and a full-time security guard (24 hours/day, 7days/week, 365

days/year), who is stationed within 100 yards of the building and monitors access and makes regular checks for attempts at physical entry into the facility.

- 5.1.3 Power and air conditioning DST uses best business practices to provide its CA facility with power and air conditioning necessary to create a reliable operating environment. All CA equipment is supported by an Uninterruptible Power Supply system, backed by a diesel generator with a multiple-day fuel supply. Air conditioning is provided by a system of multiple, independent air handlers that continually monitor and adjust temperature and humidity for optimum operating conditions.
- 5.1.4 Water exposures DST uses best business practices to protect its CA facility from water exposure. The building is built above all known flood plains and moisture detectors in order to detect even minor flooding.
- 5.1.5 Fire prevention and protection DST uses best business practices in fire prevention and protection. The facility is equipped with a chemical fire-suppression system that uses a moisture-free, environmentally-safe fire suppressant.
- 5.1.6 Media storage DST uses best business practices for media storage. Data storage media is regularly archived and stored separately from CA equipment in a fireproof vault constructed of concrete and steel and drilled deep into a solid granite mountain with a full-time guard (24 hours/ day, 7 days/week, 365 days/year).
- 5.1.7 Waste disposal DST uses best business practices for the destruction and disposal of waste. Prior to disposal, all confidential, private or sensitive material is shredded on-site or otherwise destroyed so that it is unrecoverable.
- 5.1.8 Off-site backup CA system backups are made on a periodic schedule and stored off site in accordance with Section 5.1.6.

## **5.2 PROCEDURAL CONTROLS**

- 5.2.1 Trusted Roles DST personnel in charge of operating, and overseeing the operation of, CA systems are considered to be in trusted roles. People selected to fill these roles are subjected to background checks and other requirements as described below. DST also separates and distributes the functions performed by these persons so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the CA system.

- |         |   |   |
|---------|---|---|
| 5.2.1.1 | Certification Authority (CA)                    | DST's procedural controls are determined by its Risk Management Committee, which reports to DST's Board of Directors. The Risk Management Committee is comprised of representatives from various departments within DST (e.g., Legal, Operations, Technology, Engineering, Product Development, Management, etc.). DST's internal procedures are not publicly available. However, they are made subject to review by DST's auditors on a regular basis.   |
| 5.2.1.2 | Registration Authority (RA)                     | The responsibilities and controls for RAs are described in the Registration Authority Agreement between DST and its RAs.  |
| 5.2.2   | Number of Persons Required per Task             | DST uses best commercial practices and separates all critical and security-sensitive operations with a system of checks and balances to ensure that one Individual acting alone cannot circumvent safeguards. <u>See e.g., Section 6.2.2.</u><br><br>To ensure that no single Individual may gain access to a Subscriber's Confidentiality Keys, DST requires dual authorization to access the Activation Data necessary to perform key recovery.<br><br>Under no circumstances does DST allow a person performing a trusted role to perform his or her own auditor function. |
| 5.2.3   | Identification and Authentication for Each Role | In accordance with DST's security policies, DST's CA personnel must first authenticate themselves prior to obtaining physical and logical access to the CA system.  |

**5.3 PERSONNEL CONTROLS**

- |       |   |   |
|-------|---|---|
| 5.3.1 | Background Qualifications Experience and Clearance Requirements | All persons performing trusted roles must undergo a background check. Persons in trusted roles with critical responsibilities for the operation of the CA system are certified as "Operative Personnel" as required by Washington law.            |
| 5.3.2 | Background Check Procedures                                     | DST outsources its background checks to a well-recognized company with over ten years of experience in pre-employment background screening. DST and the outsourcing company perform background checks of individuals in trusted roles as follows: |

criminal and civil lawsuit history checks are performed through a

national database search of County, State and Federal courthouse records;  
 DST performs a work/job reference check of individuals by contacting references over the telephone to obtain information regarding years known and personal or professional impressions and relationships with coworkers; and  
 a financial status check is performed through national credit bureau databases.

- 5.3.3 Training Requirements  
 DST ensures that all Operative Personnel receive comprehensive training in: DST's security principles and mechanisms; security awareness; PKI software versions in use on the CA system; PKI duties they are expected to perform; and disaster recovery and business continuity procedures.
- 5.3.4 Retraining Frequency and Requirements  
 DST's Director of Training conducts retraining as required and reviews the requirements of Section 5.3.3 at least once a year.
- 5.3.5 Job Rotation Frequency and Sequence  
 No Stipulation.
- 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 the CA or as an RA, DST suspends that person's access to the CA/RA system.
- 5.3.7 Contracting Personnel Requirements  
 DST's contractors are subject to duties of confidentiality and are contractually required to perform their duties in accordance with this CPS.
- 5.3.8 Documentation Supplied to Personnel  
 DST provides its employees with the documentation necessary to define and support the duties and procedures of persons filling trusted roles.

**5.4 SECURITY  
 AUDIT  
 PROCEDURES**

- 5.4.1 Types of Event Recorded  
 DST's CA equipment records events related to the CA server (installation, modification, accesses), and the application (requests, responses, actions, publications, and error conditions).  
 The information recorded includes: the type of event, the time the event occurred, success or failure, the source and destination of a

message, or the disposition of a created object (e.g., a filename). Where possible, audit data is automatically collected; when this is not possible a logbook, paper form, or other physical mechanism is used. Auditing capabilities of all CA equipment is enabled during installation.

- 5.4.2 Frequency of Processing Log DST's Director of Security reviews the audit logs weekly for all unexplained or significant events. Such reviews involve verifying that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken following these reviews are documented.
- 5.4.3 Retention Period for Audit Log Audit logs are kept on the CA equipment until they are removed for archival. Deletion and archival of the audit log from the CA equipment is performed by the Director of Security.
- 5.4.4 Protection of Audit Log The audit log is not open for reading or modification except by those processes that perform audit processing. The audit log is moved to a safe, secure storage location as identified in Section 5.1.6.
- 5.4.5 Audit Log Backup Procedures Audit logs and audit summaries are backed up, or copied if in manual form.
- 5.4.6 Audit Collection System (internal vs. external) DST's audit processes run independently of the CA system and are invoked at system startup, and cease only at system shutdown.
- 5.4.7 Notification To Event-Causing Subject No Stipulation.
- 5.4.8 Vulnerability Assessments DST reviews vulnerability assessments and revises its system following the discovery of system vulnerabilities.

## **5.5 RECORDS ARCHIVAL**

- 5.5.1 Types of Event Recorded The events recorded and archived by DST are as stated in Section 5.5.1 of the State of Washington CP.
- 5.5.2 Retention Period for Archive DST retains archive records in accordance with Section 5.5.2 of the State of Washington CP.

5.5.3	Protection of Archive	DST protects the archive record in accordance with Section 5.5.3 of the State of Washington CP.
5.5.4	Archive Backup Procedures	DST archive backup procedures meet the requirements of Section 5.5.4 of the State of Washington CP.
5.5.5	Requirements for Time-Stamping of Records	DST provides time stamping of all validation activity within the DST repository.
5.5.7	Procedures to Obtain and Verify Archive Information	During any audits required by the State of Washington CP, the auditor shall verify the integrity of the archives.
<b>5.6</b>	<b>KEY CHANGEOVER</b>	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. The procedures to renew a Certificate are provided in Section 3.2.
<b>5.7</b>	<b>COMPROMISE AND DISASTER RECOVERY</b>	
5.7.1	Computing Resources Software and/or Data Are Corrupted	DST will perform tape back-ups on a daily basis. Back-up tapes and back-up Hardware Tokens will be stored off-site in a secure location. In the event of disaster whereby both principal and back-up CA operations become inoperative, DST's CA operations will be re-initiated on appropriate hardware using backup copies of software and Hardware Tokens.
5.7.2	Secure Facility After a Natural or Other Type of Disaster	DST will implement a completely redundant hardware configuration at its principal site. In the event of a disaster whereby DST's main CA operations are physically damaged or otherwise become inoperative, DST's CA operations will switch over to a geographically-diverse hot site or be recovered from archives. Pre-disaster vendor agreements will provide for a drop shipment of hardware following a major incident.
5.7.3	Entity Public Key Is Revoked	In the event that DST's CA Certificate must be revoked, DST will follow the procedures of Section 5.7.3 of the State of Washington CP.

- 5.7.4 Entity Private key Is Compromised In the case of DST key compromise, DST will follow the procedures of Section 5.7.4 of the State of Washington CP, revoke all Certificates, and communicate the revocation of DST's Certificate in a manner to ensure maximum dissemination of the revocation notice. Subsequently, DST will rekey and re-issue all Certificates. All CRLs will be signed using the new key.
- 5.7.5 Entity Public Key Is Downgraded In the event that DST's CA Certificate is downgraded, DST will follow the procedures of Section 5.7.5 of the State of Washington CP.
- 5.8 **CA TERMINATION** In the event of CA termination, DST will follow the procedures of Section 5.8 of the State of Washington CP.
- 5.9 **CUSTOMER SERVICE** DST provides the following kinds of Customer Service:  
 a Web Site with access to Frequently Asked Questions (FAQ) and an online help desk;  
 an e-mail help desk service at [helpdesk@digsigtrust.com](mailto:helpdesk@digsigtrust.com);  
 and telephone-based customer service, 5 a.m. and 5 p.m. Pacific Time, Monday through Friday, excluding New Year's Day, Memorial Day, Independence Day, Thanksgiving Day and Christmas Day.

## 6 TECHNICAL SECURITY CONTROLS

- 6.1 **KEY PAIR GENERATION AND INSTALLATION** The technical security controls for Key Pair generation used by DST are as stated in Section 6.1 of the State of Washington CP.
- 6.2 **CA PRIVATE KEY PROTECTION** DST protects its Private Keys in accordance with the provisions of the State of Washington CP.
- 6.2.1 Standards for cryptographic module See Section 6.2.1 of the State of Washington CP, which is incorporated by reference.
- 6.2.2 Private key multi-person control See Section 6.2.2 of the State of Washington CP, which is incorporated by reference.

- 6.2.3 Private key escrow DST can archive the Confidentiality Key for Subscribers to help prevent the loss of valuable information and documents. Signature Keys are never escrowed, stored or archived by DST. A Subscriber can request a key recovery directly from DST or through an RA. Key recovery is supported only when dual key pairs and certificates are issued, one for signing and one for encryption.
- 6.2.4 Private key backup Subscribers may back-up their own Digital Signature Private Keys. 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 See Sections 3.1.7, 5.2.2 and 6.2.3.
- 6.2.6 Private key entry into cryptographic module DST's Private Keys are generated and kept inside Cryptomodules evaluated to at least FIPS 140-1 Level 3.
- 6.2.7 Method of activating Private Key DST's Private Keys are activated by Activation Data stored securely and separately from Cryptomodules. See Section 5.1.2 above.
- 6.2.8 Method of deactivating Private Key DST's Cryptomodules are programmed to deactivate automatically and passively after a period of non-use. However, Cryptomodules that have been activated will not be left unattended or otherwise active to unauthorized access. After use, they will be deactivated via logout procedures.
- 6.2.9 Method of destroying Private Key Private Keys are destroyed when no longer needed in accordance with FIPS 140-1-certified destruction methods. DST uses the "zeroize" function to securely destroy Keys no longer needed in the Cryptomodule.

6.3	<b>OTHER ASPECTS OF KEY PAIR MANAGEMENT</b>	DST will sign Certificates for the State of Washington PKI with an RSA 2048-bit Private Signing Key. The certificate lifetimes for DST's Private Signing Keys for the State of Washington PKI are five years.
6.4	<b>ACTIVATION DATA</b>	DST uses a multiple-user, manually-held key share PIN device to activate its Private Keys.
6.5	<b>COMPUTER SECURITY CONTROLS</b>	
6.5.1	Specific computer security technical requirements	<p>DST's CA servers include the following functionality, provided by the operating system, PKI application and/or physical safeguards:</p> <ul style="list-style-type: none"> <li>• Access control to CA services and PKI roles;</li> <li>• Enforced separation of duties for PKI roles;</li> <li>• Identification and authentication of PKI roles and associated identities;</li> <li>• Object re-use or separation for CA random access memory;</li> <li>• Use of cryptography for session communication and database security;</li> <li>• Archival of CA and End-Entity history and audit data;</li> <li>• Audit of security related events;</li> <li>• Self-test of security related CA services;</li> <li>• Trusted path for identification of PKI roles and associated identities; and</li> <li>• Recovery mechanisms for keys and the Issuing CA system.</li> </ul>
6.5.2	Computer security rating	DST's servers are configured to meet C2 compliance requirements and are operated at a C2 equivalence. As a minimum, DST's CA systems implement discretionary access control, object reuse controls, individual identification and authentication, and a protected audit record.

- 6.6 **LIFE CYCLE TECHNICAL CONTROLS** The delivery and installation of DST's CA equipment meets the standards specified in Section 6.6 of the State of Washington CP.
- 6.7 **NETWORK SECURITY CONTROLS** DST implements a three-tiered network infrastructure comprised of firewalls and intrusion detection systems configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by DST's CA system.
- 6.8 **CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS** Requirements for cryptographic modules are as stated above in section 6.2.

**7 CERTIFICATE AND CRL PROFILES**

- 7.1 **CERTIFICATE PROFILE** DST issues X.509 v.3 Certificates. Certificates issued pursuant to the State of Washington CP contain the relevant OID indicating the assurance level of the Certificate.

7.1.1 Version number and base fields DST issues Certificates in accordance with the following PKIX Certificate Profile:

Version Version of X.509 certificate, version 3(2)

Serial Number Unique serial number for certificate

Signature DST's Digital Signature on the Certificate

Issuer DST

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

Subject Public Key Information The Subscriber's Public Key.

7.1.2	Certificate Extensions	
7.1.2.1	Certificate Policies	The certificatePolicies is populated in all Certificates with one of the policy OIDs identified in Section 1.2 and is set as non-critical.
7.1.2.2	Policy Constraints	Values as required by the State of Washington CP.
7.1.2.3	Critical extensions	Extensions and values as required by the State of Washington CP.
7.1.2.4	Supported Extensions	The following extensions are present and supported in DST's Certificate Profile:  authorityKeyIdentifier;  subjectKeyIdentifier;  keyUsage;  certificatePolicies;  subjectAltName;  authorityInfoAccess; and  cRLDistributionPoints.
7.1.3	Algorithm object identifiers	Certificates are issued with the following certificate attributes, associated algorithms and OIDs, including but not limited to:  signature, sha-1WithRSAEncryption, OID = 1.2.840.113549.1.1.5; and  subjectPublicKeyInfo, RSAEncryption, OID = 1.2.840.113549.1.1.1.
7.1.4	Name forms	All Subscriber DNs are X.501 printable strings.
7.1.5	Name constraints	The Subscriber's and Issuer's DN are in every State of Washington Certificate issued by DST.
7.1.6	Certificate Policy Object Identifier (CP)	There are three levels of assurance in the State of Washington CP. Each level of assurance has its own OID, identified in Section 1.2 of this CPS and in the CP. The Certificates DST issues for a given

OID) assurance level assert the corresponding OID for that assurance level.

7.1.7 Usage of Key Usage extension The values for the Key Usage extension for Certificates DST issues are as required by the State of Washington CP, viz., the Key Usage extension is marked as "present and critical." The Key Usage Extension values are as follows:

Digital Signature

digitalSignature = 1  
nonRepudiation = 1  
dataEncipherment = 0  
keyEncipherment = 0  
keyAgreement = 0  
keyCertSign = 0  
cRLSign = 0  
encipherOnly = 0  
decipherOnly = 0

Confidentiality

digitalSignature = 0  
nonRepudiation = 0  
dataEncipherment = 1  
keyEncipherment = 1  
keyAgreement = 0  
keyCertSign = 0  
cRLSign = 0  
encipherOnly = 0  
decipherOnly = 0

7.1.8 Policy qualifiers syntax and semantics A Policy Qualifier is defined for all State of Washington Policy OIDs and includes a User Notice explicitText populated with the following language: "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.00" where X is the Recommended Reliance Limit for the Certificate's Assurance Level.

**7.2 CRL PROFILE**

7.2.1 Version numbers DST issues X.509 version two (2) CRLs.

7.2.2 CRL and CRL entry extensions DST supports the CRLDistributionPoint and AIA (Authority Information Access) CRL extensions.

## 8 POLICY ADMINISTRATION

- 8.1 CHANGE PROCEDURES** This CPS will be reviewed by DST from time to time. Errors, updates, or suggested changes to this document should be communicated to the Contact identified in Section 1.3. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change
- 8.1.1 List of Items that Can Change Without Notification Editorial and typographical corrections, changes to contact details and other minor changes that do not materially impact Subscribers or Relying Parties may be changed without notice and are not subject to the notification requirements herein.
- 8.1.2 List of Items Subject to Notification Requirement All changes to this CPS that may materially affect Subscribers or Relying Parties are subject to the notification requirement.
- 8.1.3 Comment Period, Process and Procedure Impacted Subscribers or Relying Parties may file comments with DST 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** A copy of this CPS is available in electronic form on the Internet at <http://www.digsigtrust.com/certificates/policy.html>, and via e-mail from [info@digsigtrust.com](mailto:info@digsigtrust.com). In the event that DST considers making changes to this CPS that are subject to the notification requirement of Section 8.1.2, DST will post the proposed changes on its Web site, the final date for receipt of comments, and the proposed effective date of change.
- 8.3 CPS APPROVAL PROCEDURES** The Department of Information Services will, with guidance of the Policy Management Authority, and in the exercise of reasonable discretion, determine the suitability and acceptability of this CPS for issuance of Certificates asserting the State of Washington CP.
- 8.4 WAIVERS** No stipulation.