Oak Ridge National Laboratory (ORNL) Certification Practice Statement v1.04

April 24, 2018

Revision History

Version	Date	Reviser	Summary of Changes
1.0	12/19/2017	Wayne A. Harris	Initial Version
1.0_BEW	10/9/2017	Bruce Wilson	Architect Review
1.01	4/18/2018	Les Manning	Certificate Administrator Review
1.02	4/19/2018	Tina Carter	Certificate Officer Review
1.03	4/20/2018	Les Manning	Certificate Administrator Responses
1.04	4/24/2018	Eddie Bishop	Information System Security Manager

Contents

1 Introduction 12
1.1 Overview 12
1.2 Document Name and Identification 12
1.3 PKI Participants 12
1.3.1 Certification Authorities 12
1.3.2 Registration Authorities 13
1.3.3 Subscribers 13
1.3.4 Relying Parties 13
1.3.5 Other Participants 14
1.4 Certificate Usage 14
1.4.1 Appropriate Certificate Usages 14
1.4.2 Prohibited Certificate Usages 14
1.5 Policy Administration 14
1.5.1 Organization Administering the Document 14
1.5.2 Contact Person 15
1.5.3 Entity Determining CPS Suitability for the Policy 15
1.5.4 CPS Approval Procedures Contact 15
1.6 Definitions Acronyms 15
2 Publications and Repository Responsibilities 17
2.1 Repositories 17
2.2 Publication of Certification Information 18
2.3 Time or Frequency of Publication 18
2.4 Access Control on Repositories 18
3 Identification and Authentication (I&A) 19
3.1 Naming 19
3.1.1 Types of Names 19
3.1.2 Need for Names to be Meaningful 19
3.1.3 Anonymity or Pseudonymity of Subscribers 19

3.1.4 Rules for Interpreting Various Name Forms 19
3.1.5 Uniqueness of Names 19
3.1.6 Recognition, Authentication, & role of Trademarks 19
3.2 Initial Identity Validation 19
3.2.1 Method to Prove Possession of Private Key 19
3.2.2 Authentication of an Organizational Identity 20
3.2.3 Authentication of Individual Identity 20
3.2.4 Non-verified Subscriber Information 21
3.2.5 Validation of Authority 21
3.2.6 Criteria for Interoperation 21
3.3 Identity and Authentication for Re-Key Requests 21
3.3.1 Identification and Authentication for Routine Re-key 21
3.3.2 Identification and Authentication for Re-Key after Revocation 21
3.4 Identity and Authentication for Revocation Requests 21
4 Certificate Life-Cycle 22
4.1 Certificate Application 22
4.1.1 Who can submit a certificate application 22
4.1.2 Enrollment Process and Responsibilities 22
4.2 Certificate Application Processing 22
4.2.1 Approval or Rejection of Certificate Applications 22
4.2.2 Time to Process Certificate Applications 22
4.3 Certificate Issuance 23
4.3.1 CA Actions during Certificate Issuance 23
4.3.2 Notification to Subscriber of Certificate Issuance 23
4.4 Certificate Acceptance 23
4.4.1 Conduct Constituting Certificate Acceptance 23
4.4.2 Publication of the Certificate by the CA 23
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 23
4.5 Key Pair and Certificate usage 23
4.5.1 Subscriber Private Key and Certificate Usage 23
4.5.2 Relying Party Public key and Certificate Usage 23

4.6 Certificate Renewal 24
4.6.1 Circumstance for certificate renewal 24
4.6.2 Who May Request Renewal 24
4.6.3 Processing Certificate Renewal Requests 24
4.6.4 Notification of New Certificate Issuance to Subscriber 24
4.6.5 Conduct constituting acceptance of a renewal certificate 24
4.6.6 Publication of the renewal certificate by the CA 25
4.6.7 Notification of certificate issuance by the CA to other entities 25
4.7 Certificate Re-Key 25
4.7.1 Circumstance for Certificate Re-Key 25
4.7.2 Who May Request Certification of a New Public Key 25
4.7.3 Processing Certificate Re-Keying Requests 26
4.7.4 Notification of New Certificate Issuance to Subscriber 26
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 26
4.7.6 Publication of the Re-Keyed Certificate by the CA 26
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 26
4.8 Certificate Modification 26
4.8.1 Circumstance for certificate modification 26
4.8.2 Who May Request Certificate Modification 26
4.8.3 Processing Certificate Modification Requests 26
4.8.4 Notification of New Certificate Issuance to Subscriber 26
4.8.5 Conduct Constituting Acceptance of Modified Certificate 26
4.8.6 Publication of the Modified Certificate by the CA 26
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 27
4.9 Certificate Revocation and Suspension 27
4.9.1 Circumstances for Revocation 27
4.9.2 Who Can Request Revocation 27
4.9.3 Procedure for Revocation Request 28
4.9.4 Revocation Request Grace Period 28
4.9.5 Time within Which CA Will Process the Revocation Request 28
4.9.6 Revocation Checking Requirements for Relying Parties 28

4.9.7 CRL Issuance Frequency 28
4.9.8 Maximum Latency for CRLs 29
4.9.9 On-Line Revocation/Status Checking Availability 29
4.9.10 On-Line Revocation Checking Requirements 29
4.9.11 Other Forms of Revocation Advertisements Available 29
4.9.12 Special requirements related to key Compromise 29
4.9.13 Circumstances for Suspension 29
4.9.14 Who Can Request Suspension 29
4.9.15 Procedure for Suspension Request 29
4.9.16 Limits on Suspension Period 29
4.10 Certificate Status Services 29
4.10.1 Operational Characteristics 29
4.10.2 Service Availability 30
4.10.3 Optional Features 30
4.11 End of Subscription 30
4.12 Key Escrow & Recovery 30
4.12.1 Key Escrow and Recovery Policy and Practices 30
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 30
5 Facility, Management, and Operations Controls 30
5.1 Physical Security Controls 30
5.1.1 Site Location and Construction 31
5.1.2 Physical Access 31
5.1.3 Power and Air Conditioning 32
5.1.4 Water Exposures 32
5.1.5 Fire Prevention & Protection 33
5.1.6 Media Storage 33
5.1.7 Waste Disposal 33
5.1.8 Off-Site backup 33
5.2 Procedural Controls 33
5.2.1 Trusted Roles 33
5.2.2 Multiple Roles 35

5.2.3 Identification and Authentication for Each Role 35
5.2.4 Roles requiring separation of duties 35
5.3 Personnel Controls 35
5.3.1 Qualifications, Experience and Clearance Requirements 36
5.3.2 Background check procedures 36
5.3.3 Training Requirements 36
5.3.4 Retraining frequency and requirements 36
5.3.5 Job Rotation Frequency and Sequence 36
5.3.6 Sanctions for Unauthorized Actions 37
5.3.7 Independent Contractor Requirements 37
5.3.8 Documentation supplied to personnel 37
5.4 Audit Logging Procedures 37
5.4.1 Types of events 37
5.4.2 Frequency of Processing Log 37
5.4.3 Retention period for Audit Log 38
5.4.4 Protection of Audit Log 38
5.4.5 Audit log backup procedures 38
5.4.6 Audit Collection System (Internal Vs. External) 38
5.4.7 Notification to Event-Causing Subject 38
5.5 Records Archival 38
5.5.1 Types of records archived 38
5.5.2 Retention period for archive 39
5.5.3 Protection of archive 39
5.5.4 Archive backup procedures 39
5.5.5 Requirements for time-stamping of records 39
5.5.6 Archive collection system (internal or external) 39
5.5.7 Procedures to Obtain & Verify Archive Information 39
5.6 Key Changeover 39
5.7 Compromise and Disaster Recovery 40
5.7.1 Incident and Compromise Handling procedures 40
5.7.2 Computing resources, software, and/or data are corrupted 40

5.7.3 Entity Private Key Compromise Procedures 40
5.7.4 Business Continuity Capabilities after a Disaster 41
5.8 CA & RA Termination 41
6 Technical Security Controls 41
6.1 Key Pair Generation and Installation 41
6.1.1 Key pair generation 41
6.1.2 Private Key delivery to subscriber 42
6.1.3 Public key delivery to Certificate Issuer 42
6.1.4 CA public key delivery to relying parties 42
6.1.5 Key sizes 42
6.1.6 Public key parameters generation and quality checking 43
6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Filed) 43
6.2 Private Key Protection and Crypto-Module Engineering Controls 43
6.2.1 Cryptographic module standards and controls 43
6.2.2 Private Key (m out of n) multi-person control 43
6.2.3 Private Key escrow 43
6.2.4 Private Key backup 43
6.2.5 Private Key archival 44
6.2.6 Private Key transfer into or from a cryptographic module 44
6.2.7 Private Key storage on cryptographic module 44
6.2.8 Method of activating private key 44
6.2.9 Method of deactivating private key 44
6.2.10 Method of destroying private key 45
6.2.11 Cryptographic Module Rating 45
6.3 Other aspects of Key Management 45
6.3.1 Public Key Archival 45
6.3.2 Usage Periods for the Public and Private Keys 45
6.4 Activation Data 45
6.4.1 Activation data generation and installation 45
6.4.2 Activation data protection 46
6.4.3 Other Aspects of Activation Data 46

6.5 Computer Security Controls 46
6.5.1 Specific Computer Security Technical Requirements 46
6.5.2 Computer Security Rating 47
6.6 Life Cycle Technical Controls 47
6.6.1 System Development Controls 47
6.6.2 Security Management Controls 47
6.6.3 Life Cycle Security Ratings 48
6.7 Network Security Controls 48
6.8 Time stamping 48
7 Certificate, CRL, and OCSP Profiles 49
7.1 Certificate Profile 49
7.1.1 Version Number(s) 49
7.1.2 Certificate Extensions 49
7.1.3 Cryptographic Algorithm Object Identifiers 49
7.1.4 Name Forms 49
7.1.5 Name Constraints 49
7.1.6 Certificate Policy Object Identifier 49
7.1.7 Usage of Policy Constraints Extension 49
7.1.8 Policy Qualifiers Syntax and Semantics 49
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 50
7.2 CRL Profile 50
7.2.1 Version Number(s) 50
7.2.2 CRL and CRL entry extensions 50
7.3 OCSP Profile 50
7.3.1 Version Numbers 50
7.3.1 OCSP Extensions 50
8 Compliance Audit and Other Assessment 50
8.1 Frequency of Audit or Assessments 50
8.2 Identity/qualifications of Assessor 51
8.3 Assessor’s Relationship to Assessed Entity 51
8.4 Topics covered by assessment 51

8.5 Actions as a result of findings 52
8.6 Communication of Results 52
9 Other Business and Legal Matters 53
9.1 Fees 53
9.1.1 Certificate Issuance or Renewal Fees 53
9.1.2 Certificate Access Fees 53
9.1.3 Revocation or Status Information Access Fees 53
9.1.4 Fees for Other Services 53
9.1.5 Refund Policy 53
9.2 Financial Responsibility 53
9.2.1 Insurance Coverage 53
9.2.2 Other Assets 53
9.2.3 Insurance or Warranty Coverage for End-Entities 53
9.3 Confidentiality of Business Information 53
9.3.1 Scope of Confidential Information 53
9.3.2 Information Not Within the Scope of Confidential Information 54
9.3.3 Responsibility to Protect Confidential Information 54
9.4 Privacy of Personal Information 54
9.4.1 Privacy Plan 54
9.4.2 Information Treated as Private 54
9.4.3 Information Not Deemed Private 54
9.4.4 Responsibility to Protect Private Information 54
9.4.5 Notice and Consent to Use Private Information 54
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 54
9.4.7 Other Information Disclosure Circumstances 54
9.5 Intellectual Property Rights 55
9.6 Representations and Warranties 55
9.6.1 CA Representations and Warranties 55
9.6.2 RA Representations and Warranties 56
9.6.3 Subscriber Representations and Warranties 56
9.6.4 Relying Party Representations and Warranties 56

9.6.5 Representation and Warranties of Other Participants 57
9.7 Disclaimers of Warranties 57
9.8 Limitations of Liability 57
9.9 Indemnities 57
9.10 Term and Termination 57
9.10.1 Term 57
9.10.2 Termination 57
9.10.3 Effect of Termination and Survival 57
9.11 Individual Notices and Communication 57
9.12 Amendments 57
9.12.1 Procedure for amendment 57
9.12.2 Notification Mechanism and Period 58
9.12.3 Circumstances under which the OID are changed 58
9.13 Dispute Resolution Procedures 58
9.14 Governing Law 58
9.15 Compliance and Applicable Law 58
9.16 Miscellaneous Provisions 58
9.16.1 Entire Agreement 58
9.16.2 Assignment 58
9.16.3 Severability 58
9.17 Other Provisions 58

1 Introduction

Oak Ridge National Laboratory ("ORNL") is a multiprogram science and technology national laboratory sponsored by the U.S. Department of Energy (DOE) and administered, managed, and operated by UT-Battelle as a federally funded research and development center (FFRDC) under a contract with the DOE.

A Certification Practice Statement ("CPS") is defined by the Electronic Commerce and Information Technology Division of the American Bar Association as "a statement of the practices which a certification authority employs in issuing certificates."

The Oak Ridge National Laboratory CPS explains the policies, practices, and procedures that govern the Oak Ridge National Laboratory public key infrastructure ("ORNL PKI").

This document contains the requirements of a Certificate Practice Statement.

1.1 Overview

This Certification Practice Statement (CPS) describes the practices of the Certificate Authorities (CAs) operated by the ORNL Information Technology Services Division (ITSD) under the ORNL Certificate Policy. This CPS is applicable to all entities with relationships with the ORNL CAs, including subscribers, relying parties, and Registration Authorities (RAs).

This CPS provides those entities with a clear statement of the practices and responsibilities of the ORNL CAs, as well as the responsibilities of each entity in dealing with ORNL CAs.

The intent of this CPS is to convey general practices applicable to a broad spectrum of CA implementations at ORNL.

1.2 Document Name and Identification

This CPS is called the Oak Ridge National Laboratory Production Certificate Authority Certification Practice Statement.

This CPS is managed by ORNL ITSD and adheres to the policies established by the ORNL Cyber Security Program Plan (CSPP) and the ORNL Certificate Policy.

1.3 PKI Participants

1.3.1 Certification Authorities

ORNL's Business Systems Operations (BSO) operates several CAs which are tasked with issuing certificates to authorized ORNL subscribers.

ORNL Issuing CAs are implemented on the Microsoft OS platform.

The ORNL CAs are operated by BSO and are authorized through ORNL's Federal Information Systems Modernization Act (FISMA) Authority to Operate (ATO) to create, sign, and issue public key certificates to Entity CAs and Subscribers.

BSO is responsible for all aspects of the issuance and management of a certificate including:

- Control over the registration process
- The identification and authentication process
- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Re-key of ORNL CA signing material

Ensuring that all aspects of the ORNL CA services, operations and infrastructure related to certificates issued under this CPS are performed in accordance with the requirements, representations, and warranties of this CPS.

1.3.2 Registration Authorities

Registration Authorities (RA) are entities that collects and verifies each applicant's identity and information to be entered into the subordinate CA certificate, or into the Subscriber's public key certificate. ORNL RAs performs its function in accordance with the ORNL CPS approved by ITSD and OCIO. The requirements for ORNL RAs are as follows:

- For certificates authorized for use in client or entity authentication, RA requirements are defined by NIST Special Publication 800-63 revision 3 based upon the Identity Assurance Level (IAL) and Authentication Assurance Level (AAL) to be achieved for client authentication.
- RAs must be UT-Battelle employees, staff augmentation subcontractors, or employees of other DOE prime contractors authorized by DOE to conduct RA actions within one or more of ORNL's Information Systems.
- Additional RA requirements may be imposed through ORNL Standards Based Management System policies, ORNL's Cybersecurity Program Plan (CSPP), and ITSD Operating Procedures.

1.3.3 Subscribers

A Subscriber is the entity (the user to whom, or device to which, a certificate is issued) whose Distinguished Name (DN) appears as the subject in a certificate, and who asserts that it uses the key and certificate in accordance with this policy.

This CPS is binding on each Subscriber that applies for and/or obtains Certificates and governs each applicant's performance with respect to their application for, use of, and reliance on, Certificates issued by the CA.

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate to determine the suitability of the certificate for a particular use.

1.3.5 Other Participants

Other participants such as certificate manufacturing authorities, providers of repository services and other entities providing PKI related services.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usages

ORNL PKI certificates will only be used for ORNL business use only.

1.4.1.1 Certificates Issued to Individuals

Individual certificates are used by individuals for digital signature, data encryption and authentication.

1.4.1.2 Certificates Issued to Devices

Certificates are issued to certain devices for the purpose of authentication of network and hardware devices. Device certificates allow for another layer of security by only permitting network access of specifically authorized devices when operated by specifically authorized users.

1.4.1.3 Certificates Issued to Services

Certificates are issued to certain services for the purpose of authentication of specific application services. Service certificates (such as OCSP) often have a need to identify an application, independent of any host server or device.

1.4.2 Prohibited Certificate Usages

Certificates issued by ORNL CAs will only be used for the purposes listed in the section 1.4.

In general, ORNL PKI Certificates are general-purpose Certificates. ORNL PKI Certificates may be used to interoperate with diverse internal Relying Parties. Usage of ORNL PKI Certificates is not generally restricted to a specific business environment.

Nonetheless, certain ORNL PKI Certificates are limited in function. For example, CA Certificates may not be used for any functions except CA functions. Moreover, individual Certificates are intended for client applications and shall not be used as service or organizational Certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The organization administering this Certification Practices Statement at ORNL.

Oak Ridge National Laboratory
1 Bethel Valley Rd, Oak Ridge, TN 37830

As a US Federal entity, ORNL has one or more US Federal Information Systems, as described by the Federal Information Systems Modernization Act (FISMA). Each information system has an Authority to Operate (ATO) issued by a cognizant Authorizing Official (AO).

The ORNL Certificate Authority is a part of the ORNL CSPP, and that ATO designates the Information System Security Manager (ISSM)/Chief Information Security Officer (CISO) and Unclassified Information System Security Officer (ISSO).

Contact Person

The following people are the primary contacts for the ORNL Certification Practices Statement:

- Les Manning (manninglf@ornl.gov)
- Carlos Cunningham (cunninghamcw@ornl.gov)
- Steve Couston (coustonsc@ornl.gov)

1.5.2 Entity Determining CPS Suitability for the Policy

The ORNL unclassified ISSM/CISO will designate the responsible party that is responsible for asserting whether this Certification Practice Statement conforms to the governing Certificate Policy.

1.5.3 CPS Approval Procedures Contact

The ORNL unclassified ISSM/CISO will determine the appropriate procedures for approving any relevant ORNL Certification Practice Statement documents.

1.6 Definitions Acronyms

AD: Active Directory (specifically Microsoft Active Directory)

CA: Certification Authority

CA-MA: CA Management Authority

CP: Certificate Policy

CPS: Certificate Practice Statement

CRL: Certificate Revocation List

CSS: Certificate Status Server

DN: Distinguished Name

ECDSA: Elliptic Curve Digital Signature Algorithm

FIPS: Federal Information Processing Standards

HTTP: Hypertext Transfer Protocol

IETF: Internet Engineering Task Force

LDAP: Lightweight Directory Access Protocol

OCSP: Online Certificate Status Protocol

OID: Object Identifier

PII: Personally Identifying Information

PKCS: Public Key Cryptography Standards

PKI: Public Key Infrastructure

PKI Operational Team: ORNL group primarily responsible for the operations of a given PKI

PSS: Probabilistic Signature Scheme

RA: Registration Authority

RFC: Request for Comments (Internet Engineering Task Force (IETF) standards document)

RSA: Rivest-Shamir-Adleman (encryption algorithm)

RSASSA: RSA Signature Scheme with Appendix

SHA: Secure Hash Algorithm

S/MIME: Secure/Multipurpose Internet Mail Extensions

SSL: Secure Sockets Layer

UPS: Uninterruptible power supply

URL: Uniform Resource Locator

Administrator: One of the four defined Trusted Roles within each CA Management Authority. See section 5.2.1.1 for additional details.

Backup Operator: One of the four defined Trusted Roles within each CA Management Authority.

CA Management Authority: The entity created by an organization that operates a CA under this CPS to manage any non-IT Security operated components and resolve name space collisions.

Certificate Manager: One of the four defined Trusted Roles within each CA Management Authority.

Compliance Auditor: A person with sufficient training, experience, qualifications, and independence from the CA being audited to perform a compliance audit to verify that a CA, and its recognized RAs, comply with all the requirements of the current versions of this CPS and the CA's CPS. All aspects of the CA/RA operation are subject to compliance audit inspections. Note this is not the same function as the Trusted Role of Security Auditor.

Enrollment Agent: A person who satisfies all the trustworthiness requirements for a Registration Authority (RA) and who performs identity proofing as a proxy for the RA.

Management Authority: See CA Management Authority.

Registration Authority: An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates.

Relying Party: A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Security Auditor: One of the four defined Trusted Roles within each CA Management Authority. See section 5.2.1.3 for additional details. Note this is not the same as the Compliance Auditor.

Subscriber: An entity that (1) is the subject named or identified in a certificate issued to that entity, (2) that holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device.

Trusted Certificate: A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

Trusted Role: A CA functional/operational role whose incumbent performs functions that can introduce security problems if not carried out properly (accidentally or maliciously). The primary Trusted Roles defined in this policy are Administrator, Certificate Manager, Security Auditor, and Backup Operator.

Two-Person Control: Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.

2 Publications and Repository Responsibilities

2.1 Repositories

Internally the CPS are made available in its entirety to subscribers and relying parties. Externally the pertinent sections are made available via an ORNL website (http://pkipolicy.ornl.gov/cps.html)

http://pkipolicy.ornl.gov/cps.html

Any changes to the document are made publicly available within 30 days from approval by the ORNL ISSM/CISO.

2.2 Publication of Certification Information

BSO will publish a copy of the ORNL CPs and all applicable ORNL CPS to the repository web site (http://pkipolicy.ornl.gov/cps.html).

BSO will ensure that all AIA and CDPs have appropriate Certificates and Revocation lists.

Directory system access controls are used to protect all directory system information and ensure that publicly accessible and all other Directory system information is protected against unauthorized modification or dissemination.

2.3 Time or Frequency of Publication

Changes to this Certification Practices Statement are made available when they are approved according to Section 1.5 of this Certification Practices Statement.

Publication requirements for CRLs are provided in sections 4.9.7 and 4.9.12

2.4 Access Control on Repositories

The ORNL PKI will make publicly available through the Internet a repository containing certificate status information, CA certificates, CRLs, and any other public information ORNL deems necessary to support the ORNL PKI.

Only authorized personnel have full access to repositories. All others are restricted to read-only access.

3 Identification and Authentication (I&A)

3.1 Naming

3.1.1 Types of Names

ORNL PKI CAs and Subscribers are assigned X.500 Distinguished Names (DNs) for inclusion in the "Issuer Distinguished Name" and "Subject" fields of certificates. Certificates may also assert one or alternate names in the "Subject Alternative Name" field.

3.1.2 Need for Names to be Meaningful

Subscriber certificates will always include meaningful names. The names will identify the person or machine or application to which they are assigned.

- The RFC822 e-mail address of the subject will appear in the alternative name forms field.
- By the use of DN the directory information tree will accurately reflect the organizational structure and common name will observe name space uniqueness requirements.

3.1.3 Anonymity or Pseudonymity of Subscribers

The CA will not issue anonymous certificates. Pseudonymous certificates can be issued to internal subscribers to support its operations. CA certificates will not contain anonymous or pseudonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in RFC 5322, Internet Message Format.

3.1.5 Uniqueness of Names

Names are unambiguously defined. The directory is managed in such a way as to ensure that no two individuals are assigned the same DN, and therefore the same electronic identity.

Name uniqueness is not violated when multiple certificates are issued to the same entity.

3.1.6 Recognition, Authentication, & role of Trademarks

The RA will not knowingly assign names that contain trademarks. The RA need not seek evidence of trademark registrations nor in any other way enforce trademark rights.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Public key certificates bind a public key to the identity of the individual to assure Relying Parties that signing performed by the private key was done by the individual whose public key appears on the certificate, and decryption using the private key can only be performed by the individual whose public key appears on the certificate. This requires that an individual safeguard their private key and any activation data used to access that key.

The CA requires proof of possession of the private key before creating and signing a certificate containing the associated public key. Proof of possession of a private key is handled automatically by CA to Subscriber messages protected by Certificate Management over CORNL (CMC) or PKIX-Certificate Management Protocol (CMP).

For the Subscriber's signature private key, a certificate request operation initiated by the Subscriber is digitally signed using the signature private key itself.

In the case where a key is generated by the CA or RA either directly on the party's hardware or software token, or in a key generator that securely transfers the key to the party's token then proof of possession is not required.

3.2.2 Authentication of an Organizational Identity

The Oak Ridge National Laboratory Technology and its PKI Certificate Officers must verify the information in a certificate request and verify whether or not the requestor is authorized for code signature certificates, device-component certificates, or SSL Certificates.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Human Individual Identity

Identity proofing for ORNL authentication certificates is governed by the identity and authentication assurance levels (IAL and AAL) defined in NIST Special Publication 800-63 revision 3. Each certificate policy (defined by an ORNL-managed OID) specifies the required Identity Assurance Level.

3.2.3.2 Authentication of Machine Individual Subscribers

Machine Users (e.g. routers, firewalls, servers, etc.) may be named as Certificate Subjects.

Some computing and communications devices (routers, firewalls, servers, etc.) are named as certificate subjects.

All devices will have a human sponsor.

The human sponsor is responsible for providing the following registration information:

- Domain membership of the device against Active Directory; or
- Domain authentication of the sponsor against Active Directory. In either case, the domain are a production domain that is security managed and implements all of the standard account controls.
- Equipment identification (e.g. serial number) or service name (e.g. DNS name) ; and
- Equipment public keys; and
- Equipment authorizations and attributes (if any are to be included in the certificate); and
- Contact information to enable the CA or RA to communicate with the sponsor when required.

The identity of the sponsor is validated using:

Authentication using a Federally-issued or ORNL-issued credential having an IAL and AAL meeting or exceeding the IAL and AAL requirements for the certificate policy.

- In-person registration using identity proofing procedures defined by 800-63 rev 3 meeting or exceeding the IAL requirements for the specific certificate type.

3.2.4 Non-verified Subscriber Information

Information that is not verified by a trusted information system (having a FISMA ATO at or above the Moderate baseline) or a trusted role holder (Certificate Officer or Registration Agent) **will not be included** in certificates. This includes, but it not limited to, information included in the Subject Alternative Name (SAN) field.

3.2.5 Validation of Authority

Before issuing CA certificate or signature certificates that assert organizational authority, the CA will validate the individual's authority to act in the name of the organization.

3.2.6 Criteria for Interoperation

No Stipulation

3.3 Identity and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

CA certificate re-key will follow the same procedures as initial certificate issuance.

For all other certificates issued under this CPS, the Subscriber or device identifies themselves for the purpose of routine re-key. The use of current, operational signature key may be used to establish identity and authentication for Subscribers and devices.

3.3.2 Identification and Authentication for Re-Key after Revocation

In the event of certificate revocation, issuance of a new certificate will require identity re-proofing as defined in NIST 800-63 rev 3 at the level appropriate to the IAL for the certificate.

3.4 Identity and Authentication for Revocation Requests

Revocation requests can be made by a Subscriber or another person authorized to act on behalf of the Subscriber (e.g., supervisor, HR department, etc.). All certificate revocation requests are communicated to a Certificate Manager via secure means, either electronically or in person.

A Certificate Manager may process a revocation request from a Subscriber, based on an email revocation request that has been digitally signed by the Subscriber.

A Certificate Manager may process a revocation request based on a digitally signed email from an individual authorized to request revocation on behalf of the Subscriber (e.g. the Subscriber's supervisor, HR representative, etc.). In this case, the Certificate Manager will verify the authority of the requestor to submit the revocation request by validating the digital signature against an authoritative source.

A Certificate Manager will process an in-person revocation request from a Subscriber, following authentication as outlined in Section 3.2.3.1.

4 Certificate Life-Cycle

4.1 Certificate Application

4.1.1 Entities authorized to submit a certificate application

Below is a list of people who may submit certificate applications:

- Any ORNL staff member who is the subject of the certificate or is the authorized sponsor for a device certificate,
- Any authorized representative of An ORNL Organization or entity,
- Any authorized representative of a ORNL CA/RA,
- An ORNL-affiliated person (staff member, collaborator, user facility user, business partner, etc) who is the subject of a certificate to be used in ORNL systems appropriate to that affiliation.

4.1.2 Enrollment Process and Responsibilities

Subscribers will adhere to the Identity and Authentication requirements listed in Section 3.2.

Subscribers are allowed to authenticate directly with the CA or use an RA to perform Identity and Authentication prior to certificates issue. In the event that an RA is used, the RA is responsible to performing Identity and Authentication in accordance with Section 3.2 and recording the transaction.

4.2 Certificate Application Processing

The CA or RA will perform identification and authentication of all required Subscriber information

4.2.1 Approval or Rejection of Certificate Applications

The CA or RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information

A CA or RA will reject a certificate application if:

- Identification and authentication of all required Subscriber information in terms of this agreement are not performed
- The Subscriber fails to furnish supporting documentation upon request

4.2.2 Time to Process Certificate Applications

CAs or RAs begin processing certificate applications within a reasonable time of receipt, not to exceed 30 days.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

A CA verifies the source of a certificate request before issuance. Certificates are checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance, a CA will post the certificate.

4.3.2 Notification to Subscriber of Certificate Issuance

CAs operating under this CPS may inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber. For device certificates, the CA may inform the human sponsor.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

By accepting An ORNL certificate, the Subscriber or CA acknowledges that all information contained in the certificate is accurate and that he or she agrees to the terms and conditions contained in this CPS definition.

Failure to object to the certificate or its contents will constitute acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

All CA certificates are published in a repository accessible to all Relying Parties. This CPS makes no stipulation regarding publication of Subscriber certificates.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Each CA will publish the following information to either an online repository or a web site that is available to Subscribers and Relying Parties.

- A CRL
- The CA's certificate
- A copy of appropriate CPS and CP.

4.5 Key Pair and Certificate usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers who are issued end-entity certificates will protect their private keys from access by other parties. The intended scope of usage for a private key is specified through certificate extensions, including the key usage and the key usage extensions, in the associated certificate.

4.5.2 Relying Party Public key and Certificate Usage

ORNL managed PKI-issued certificates specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy will issue CRLs specifying the current status of all unexpired certificates. It is recommended that relying parties process and comply with this information whenever using ORNL certificates in a transaction.

Relying parties are responsible for examining this CPS to understand all of their rights and obligations under the CPS.

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. The old certificate should be revoked, and will not be further re-keyed, renewed, or modified.

4.6.1 Circumstance for certificate renewal

Subscriber certificates issued under this CPS will *not* be renewed, except during recovery from CA key compromise. In such cases, the renewed certificate will expire as specified in the original subscriber certificate.

CA Certificates and OCSP responder certificates may be renewed so long as the aggregated lifetime of the public key does not exceed the certificate lifetime. The CA may automatically renew certificates during recovery from key compromise.

4.6.2 Who May Request Renewal

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

4.6.3 Processing Certificate Renewal Requests

CAs will ensure that the Subscriber's identity information and public key are properly bound on all digital requests. Changes to a Subscriber's name, prescribing or ordering authority, or affiliation will result in certificate revocation.

CAs will go through the original registration process to obtain a new certificate. That CA will notify all CAs, RAs, and Subscribers who rely on the CA's certificate that it has been changed.

CA certificate renewal requests are approved by the ISSM/CISO.

For all other renewal requests, no stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

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

4.6.5 Conduct constituting acceptance of a renewal certificate

For all issuing CAs operating under this CPS, no stipulation.

By accepting an ORNL certificate, the Subscriber or CA acknowledges that all information contained in the certificate is accurate.

4.6.6 Publication of the renewal certificate by the CA

As specified in Section 2.1, all CA certificates may be published in repositories. This CPS makes no stipulation regarding publication of subscriber certificates, unless noted in section 9.4.3.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate Re-Key

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. The old certificate may or may not be revoked, but will not be further re-keyed, renewed, or modified. Subscribers will identify themselves for the purpose of re-keying.

The ORNL CA human subscriber keys may be configured to be automatically re-keyed prior to expiration of the current key pair, based on possession of the non-expired private key.

Re-key of a certificate does not require a change to the subjectName and does not violate the requirements for name uniqueness.

CA Certificate Re-Key

CA re-keys are manual processes and require a formal script that details the steps taken. The script must show that the required separation of roles was observed. The script will include a notification process for all CAs, RAs and subscribers that rely on the CA's certificate that it has been changed. The completed script is retained by security as an audit trail of the CA re-key operation. All individuals participating during a CA re-key are identified in the script. All CA re-keys are authenticated during the re-key process, using the information in the certificate request and a thumbprint received using a secure out-of-band method; these steps are part of the formal script.

4.7.1 Circumstance for Certificate Re-Key

Examples of circumstances requiring certificate re-key include expiration, loss or compromise, issuance of a new hardware token, and hardware token failure. Per NIST 800-63 rev 3 (Part B, Section 10.2.1), there is no requirement for periodic rekeying.

4.7.2 Who May Request Certification of a New Public Key

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

Subscribers with a currently valid certificate may request certification of a new public key. CAs and RAs may request certification of a new public key on behalf of a subscriber. For device certificates, the human sponsor of the device may request certification of a new public key.

4.7.3 Processing Certificate Re-Keying Requests

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

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

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

4.7.6 Publication of the Re-Keyed Certificate by the CA

All CA certificates are published as specified in section 2.1. This CPS makes no stipulation regarding publication of subscriber certificates, except as noted in section 9.4.3.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but will not be further re-keyed, renewed, or modified.

4.8.1 Circumstance for certificate modification

The ORNL PKI will not support certificate modifications to existing Subscriber certificates. If an individual or devices identity information changes (e.g. name change due to marriage or DNS name change) the Subscriber will enroll for a new certificate presenting information supporting the name change. This CPS therefore treats certificate modification requests as new certificate requests.

4.8.2 Who May Request Certificate Modification

Not Applicable.

4.8.3 Processing Certificate Modification Requests

Not Applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not Applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not Applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not Applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

CAs operating under this CPS will issue Certificate Revocation Lists (CRLs) covering all unexpired certificates issued under this policy. CAs operating under this CPS will make public a description of how to obtain revocation information for the certificates they publish. This information is given to subscribers during certificate request or issuance and are readily available to any potential Relying Party.

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

Certificate suspension for CA certificates is not allowed by this CPS. However, the use of certificate suspension for subscriber certificates is permitted.

4.9.1 Circumstances for Revocation

A certificate is revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Examples of circumstances are:

- Identifying information or affiliation components of any names in the certificate becomes invalid, including the severance of the subscriber's affiliation with ORNL.
- Privilege attributes asserted in the subscriber's certificate are reduced.
- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- There is reason to believe the private key has been compromised.
- The certificate signing method is no longer a NIST approved cryptographic function or the revocation of that approval has been announced.
- The subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.
- The private key is lost or cannot be accessed for any reason; or compromise is suspected, or likely.

Whenever any of the above circumstances occur, the associated certificates are revoked and placed on the CRL.

Revoked certificates are included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. The Certificate Manager can request the revocation of a subscriber's certificate on behalf of any authorized party.

A subscriber may request that its own certificate be revoked. Revocation can also be initiated at the discretion of ORNL security.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate will identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g. digitally or manually signed).

All revocation requests will be reviewed by a Certificate Manager or CA Administrator to ensure they are legitimate and will then revoke the certificate, as follows:

- Authenticate the person requesting revocation
- Verify the person requesting revocation is authorized to request revocation of the certificate in question
- Authenticate revocation request
- Revoke the certificate, specifying revocation reason
- Ensure the revocation request is retained.

Revocation requests should be made in one of the following ways:

- Through the standard ORNL Ticketing System.
- Through incident investigation processes defined in the Incident Management IOP.
- In-person requests to the ISSO, ISSM, or a Certificate Manager.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this CPS. Subscribers are expected to request revocation of any certificate thought to be compromised immediately to the issuing CA.

The ORNL CA revokes certificates upon request as quickly as is practical.

4.9.5 Time within Which CA Will Process the Revocation Request

CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests are processed before the next full CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

Certificate Revocation Lists (CRLs) are issued periodically, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. Certificate status information are published no later than the next scheduled update and certificate overlap is permitted. This will facilitate the local caching of certificate status information for off-line or remote operation.

ORNL CAs that issue certificates to subscribers and/or operate on-line will issue a full CRL at least once every 7 days with an overlap of up to 7 days.

The ‘nextUpdate’ time in the Issuing CA CRL may be no later than 14 days after issuance time.

Delta CRLS are not used.

4.9.8 Maximum Latency for CRLs

CRL's are generally published as soon as they are generated. There is no latency intended between CRL generation and publication into the online ORNL CA CRL Distribution Point.

- All CRLS are published no later than the time specified in the next Update field of the previously issued CRL
- Issuing CA: CRL is Published within 4 hours of generation

4.9.9 On-Line Revocation/Status Checking Availability

As some relying parties may not be able to accommodate on-line communications, all CAs are required to support CRLs. However, CAs under this policy may also operate an OCSP Responder covering the certificates they may issue.

4.9.10 On-Line Revocation Checking Requirements

If available, Relying Party client software may optionally support on-line status checking. Client software using on-line status checking need not obtain or process CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

No alternate methods of revocation advertisements are used.

4.9.12 Special requirements related to key Compromise

When a CA certificate is revoked, a CRL is generated and published within 24 hours of notification.

No additional stipulation for subscriber certificates.

4.9.13 Circumstances for Suspension

For CA certificates, suspension is not permitted.

For subscriber certificates, no stipulation

4.9.14 Who Can Request Suspension

No stipulation for subscriber certificates.

4.9.15 Procedure for Suspension Request

No stipulation for subscriber certificates.

4.9.16 Limits on Suspension Period

No stipulation for subscriber certificates.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

CA online repository contains list of valid certificates and list of revoked certificates (CRL). Both lists are continuously updated.

Note: Relying Parties are bound to their obligations as set forth in the ORNL operating rules and the stipulations of this CPS irrespective of the operational characteristics of certificate status service.

4.10.2 Service Availability

The on-line repository is available on a 24x7 basis, liable to reasonable scheduled maintenance.

Note: Relying Parties are bound to their obligations and the stipulations of this CPS irrespective of the availability of the certificate status service.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Certificates that have expired prior to or upon end of subscription are not required to be revoked.

4.12 Key Escrow & Recovery

This CPS prohibits third party escrow or recovery of CA, and Subscriber signing keys used for purposes set forth in the ORNL operations.

- Certificates used for encryption **are** archived.
- Certificates used for non-repudiation are **never** be archived.

4.12.1 Key Escrow and Recovery Policy and Practices

CAs that support key recovery will identify the document describing the key escrow and recovery policy in the applicable CPS.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No Stipulation

5 Facility, Management, and Operations Controls

5.1 Physical Security Controls

The ORNL CAs are labeled as being for authorized use only. The ORNL CA and CSS equipment are in a controlled facility in building 4512 that is monitored 24 hours per day, 7 days per week, and 52 weeks per year.

ORNL CAs and CSS cryptographic modules, both those active and operational, and those stored in security containers for on-site and off-site backup, are protected against theft, loss, and unauthorized use by the controls specified in section 5.1.2 below. All the physical control requirements specified below apply to the ORNL CAs and any remote workstations used to administer the CA's except where specifically noted (see section 5.1.2.1 below).

5.1.1 Site Location and Construction

The location and construction of the facility housing ORNL CA equipment are consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, will provide robust protection against unauthorized access to the CA equipment and records.

The facility housing the PKI equipment are provide a physically protected environment with controls to deter, detect and prevent unauthorized use of, and disclosure of sensitive information. ORNL PKI operates in our datacenter to support business continuity and disaster recovery, and facilities will have equivalent physical controls. Disaster recovery facilities are located at geographically disparate locations so operations can be resumed if the primary location is disabled.

5.1.2 Physical Access

The CA equipment will always be protected from unauthorized access. The equipment are protected from unauthorized access while the cryptographic module is installed and activated. Physical access controls are implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

The physical security mechanisms for CAs are in place to:

- Permit no unauthorized access to the hardware;
- Store all removable media and paper containing sensitive plain-text information in secure containers;
- Monitor, either manually or electronically, for unauthorized intrusion at all times;
- Maintain and periodically inspect an access log;
- Require a multiple person access control prior to accessing the cryptographic modules.

Removable cryptographic modules are inactivated prior to storage. When not in use, removable cryptographic modules and activation information used to access or enable cryptographic modules used by CAs are placed in secure containers.

An integrated physical access control and intrusion detection system is operational to restrict access to authorized personnel, to detect unauthorized access, and to provide for the audit of all entries to and exits from the controlled areas. Sensors monitor exit and entrance doors. This access control system uses badges managed through ORNL's physical access control system.

Entrance to, and exit from, all controlled areas is monitored by closed circuit television (CCTV) and a system is used to record images or persons passing through the area. There is a CCTV camera outside the PKI Room door monitoring entry and exit from the PKI Room. There are two (2) CCTV cameras inside the PKI Room, monitoring the entry and exit into out of the PKI cage which further protects physical access to the PKI computer systems, including the CA system. In addition, an appropriate camera and time-lapse recorder will record activity in the security zone.

The camera is placed such that persons in the room are recorded, but such that keystrokes typed on the system console may not be recovered by image enhancement. Images/recordings are maintained for a minimum of 90 days.

CA and CSS facilities are checked by ORNL Data Center operations personnel at least once per business day to ensure that the physical protection mechanisms are still operating and ensure that there is no evidence of any breach of the physical security controls. Records of these checks (including the names of the ORNL staff member making the check, along with a date and time) are recorded by the ORNL Physical Access Control System and are provided to the auditor during every compliance audit.

There are 2 security containers (safes which meet GSA security container requirements) stored inside the PKI Room, to implement split knowledge (2 party) controls in the secure storage of PKI materials. The first safe can be accessed ONLY by those authorized personnel in the PKI trusted role.

The second safe can be accessed ONLY by those authorized personnel in the PKI Security Officer trusted role. Each safe has a hard copy log, which documents all entry into the safe, and records the reason the safe was opened, along with the date and time of opening and the time of closing and the person who opened the safe. The log is stored inside of the safe. Each safe also contains an inventory list of the materials that are contained in that safe.

The controls in this section of the CPS are operational and provide the controls for protecting the CA equipment from unauthorized access while the cryptographic module is installed and activated.

5.1.3 Power and Air Conditioning

All controlled access areas in the Security Zone is equipped with:

- An appropriately sized uninterruptible power supply (UPS) sufficient to allow for the systems to complete current actions and shutdown without data loss, and for six (6) hours of uninterruptible power for the directory servers
    - The UPS is sized to permit the CA to lock out input, finish any pending actions and record system state automatically
- Heating, ventilation, and air conditioning appropriate for a commercial data processing facility Emergency lighting

These environmental controls conform to local standards and is appropriately secured to prevent unauthorized access and/or tampering with the equipment.

No liquid, gas, exhaust, etc. pipes traverse the controlled space other than those directly required for the area's HVAC system.

5.1.4 Water Exposures

The ORNL CAs and CSS equipment are installed such that it is not in danger of exposure to water. Sprinklers used for fire control have a contingency plan for recovery should the sprinklers malfunction, or cause water damage outside of the fire area.

5.1.5 Fire Prevention & Protection

The secure facility for the CA equipment is constructed and equipped, and procedures are implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures will meet all local applicable safety regulations.

5.1.6 Media Storage

CA media are stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive, or backup information are duplicated and stored in a location separate from the CAs and are protected from unauthorized access.

5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed and are to be destroyed are destroyed in a process that renders the material unrecoverable. Paper documents are shredded using a cross-cut shredder that complies with NSA/CSS 02-01.

Digital information on digital media that is to be disposed of is first sanitized in compliance with DoD and FIPS standards for information cleaning/sanitization.

Digital media that is to be destroyed is destroyed in accordance with DoD Standard 5220.22- M.

Hard disks are to be mechanically destroyed after all information is sanitized.

Magnetic tape is destroyed by first cutting the tape into at least 4 pieces and then running at least 2 of the pieces through a cross-cut shredder or equivalent process.

5.1.8 Off-Site backup

Full system backups, sufficient to recover from system failure, are to be accomplished not less than once per week. A full system backup is stored at an off-site location (separate from the CA and CSS equipment), with physical controls commensurate with the operational CA.

The off-site backups are stored in locked containers that have 2 separate padlocks. These locked containers are stored off-site. The off-site facility is monitored on a 24 hour per day, 7 days per week, 52 weeks per year basis.

The keys to the padlocks are controlled by 2 separate groups of authorized PKI trusted role personnel only.

5.2 Procedural Controls

5.2.1 Trusted Roles

A Trusted Role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles will extraordinarily responsible, or the integrity of the CA are weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensure that the person filling the role is trustworthy

and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The primary Trusted Roles defined in this policy are Administrator, Certificate Manager, Security Auditor, and Backup Operator. Individual personnel are specifically designated to assume these four roles as defined below. These four roles are employed at the CA, RA, and CSS locations as appropriate.

Additional role creation for the purpose of additional role separation is permitted (e.g. New role of Template Manager to configure certificate templates with Administrator limited to publishing the templates).

Separation of these duties is required for critical CA functions, to prevent one person from maliciously using a CA system without detection.

The most sensitive tasks, such as access to and management of CA cryptographic module and associated key material require multiple trusted persons. Every task that requires a multiple control are administrated with a “k” of “n” person doctrine (where “k” ≥ 2 and “n” > “k”).

CAs will have a verification process that provides an oversight of all activities performed by privileged CA role holders. Those roles are ones (but are not limited to) that can issue certificates, generate keys and administer the CA configuration settings.

5.2.1.1 Administrator

Administrators are responsible for:

- Installation, configuration, and maintenance of the CA and CSS (where applicable)
- Establishing and maintaining CA and CSS system accounts
- Configuring certificate profiles or templates
- Configuring CA, RA, and CSS audit parameters
- Configuring CSS response profiles
- Generating and backing up CA and CSS keys.

Administrators do not issue certificates to subscribers.

5.2.1.2 Certificate Manager (Certificate Officer)

Certificate Managers are responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates
- Verifying the identity of subscribers and accuracy of information included in certificates
- Approving and executing the issuance of certificates
- Requesting, approving and executing the revocation of certificates

5.2.1.3 Security Auditor

Security Auditors are responsible for:

- Reviewing, maintaining, and archiving audit logs
- Performing or overseeing internal compliance audits to ensure that the CA, associated RAs, and CSS (where applicable) are operating in accordance with its CPS

5.2.1.4 Backup Operator

The Backup Operator role are responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.2 Multiple Roles

One person is not allowed to act alone to manage CA servers. Mechanisms such as multiple keys are in place to prevent this from occurring. Along with multiple keys, where possible roles are separated amongst individuals.

Two or more persons are required for the following tasks:

- CA key generation
- CA signing key activation
- CA private key backup.

Where multiparty control is required, at least one of the participants are an Administrator. All participants will serve in a Trusted Role as defined in section 5.2.1.

- Multiparty control will not be achieved using personnel that serve in the Security Auditor Trust Role.

5.2.3 Identification and Authentication for Each Role

All CA personnel will identify and authenticate themselves before being permitted to perform any actions set forth in the section 5.2.1 for that role.

5.2.4 Roles requiring separation of duties

- Roles requiring Separation of duties, meaning multiple individuals, include (but are not limited to):
    - Administrator
    - Certificate Manager
    - Security Auditor
    - Backup Operator
- The CA system will identify and authenticate its users and will ensure that no user identity can assume multiple roles.

5.3 Personnel Controls

Personnel granted privileged CA and RA roles will meet ORNL personnel security requirements. CA personnel will receive appropriate training with respect to their duties.

5.3.1 Qualifications, Experience and Clearance Requirements

All persons filling Trusted Roles are selected on the basis of loyalty, trustworthiness, and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA are set forth in the CPS.

In addition to the above, individuals filling Trusted Roles for the ORNL CA will:

- Have not knowingly been previously relieved of their PKI duties or responsibilities for reasons of negligence or non-performance of duties
- Be appointed in writing by security as appropriate
- Have not knowingly been denied a security clearance, or had a security clearance revoked
- Have not been convicted of a felony offense
- Have successfully completed an appropriate training program or have demonstrated the ability to perform their duties
- Be considered as holding Privileged Accounts, as defined by the ORNL CSP, and follow all requirements for Privileged Account holders (system administrators)
- Be trustworthy

5.3.2 Background check procedures

The ORNL PKI will enforce appropriate personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of its personnel.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA or RA will receive training. Training are conducted in the following areas:

- CA (or RA) security principles and mechanisms
- All PKI software versions in use on the CA (or RA) system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Stipulations of this CPS and CPs.

5.3.4 Retraining frequency and requirements

All individuals responsible for PKI roles are made aware of changes in the CA operation. Any significant change to the operations will have a training (awareness) plan, and the execution of such plan are documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment. Documentation are maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The ORNL PKI can choose to impose sanctions, including termination or suspension if appropriate, if personnel acting in trusted roles perform unauthorized actions or otherwise abuse their authority. Actions that may be taken would be in accordance with established ORNL code of conduct.

5.3.7 Independent Contractor Requirements

- The ORNL PKI operational team may employ contractors as necessary.
- Contractors assuming trusted roles as outlined in this CPS will pass the same background checks as ORNL employees and be subject to the same level of identity verification.

5.3.8 Documentation supplied to personnel

ORNL PKI personnel are provided this Certification Practices Statement. They are also provided with ORNL PKI procedures and other documentation relevant to their job functions.

5.4 Audit Logging Procedures

Audit log files are generated for events related to the security of the ORNL PKI. Where possible, the security audit logs are collected automatically. Where not possible, a logbook, paper form, or other physical mechanism are used.

5.4.1 Types of events

- All security events related to physical and logical access, configuration changes, key generation & usage, certificates creation and any other events that may be required for auditing purposes are recorded.
- At a minimum, each audit record will include the following (either recorded automatically or manually for each auditable event):
    - Type of entry
    - The date and time the event occurred
    - A success or failure indicator when executing the CA's signing process
    - A success or failure indicator when performing certificate revocation
    - Identity of the entity and/or operator that caused the event.
- A message from any source requesting an action by the CA is an auditable event; the message will include the message date and time, source, destination, and contents.
- Procedures specifying integrity controls, event record lifetime and event record access are implemented and maintained.

5.4.2 Frequency of Processing Log

Logs are reviewed only when there is cause for review.

The audit log should be reviewed for abnormalities in support of any suspected violation and for events such as repeated failed actions, requests for privileged information, attempted access of system files, and certificate and revocation/suspension requests that fail authentication and validation criteria.

5.4.3 Retention period for Audit Log

Audit logs are kept for a period of at least one year

5.4.4 Protection of Audit Log

The security audit data will not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing.

CA system configuration and procedures are implemented together to ensure that only authorized people archive or delete security audit data.

Procedures are implemented to protect archived data from deletion or destruction before the end of the security audit data retention period.

Security audit data are moved to a safe, secure storage location separate from the location where the data was generated.

5.4.5 Audit log backup procedures

Audit logs are backed up on a periodic basis.

5.4.6 Audit Collection System (Internal Vs. External)

The audit log collection system may or may not be external to the CA system.

Automated audit processes are invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems are configured such that security audit data is protected against loss (e.g. overwriting or overflow of automated log files).

- Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operation are suspended until the problem has been remedied.

5.4.7 Notification to Event-Causing Subject

No Stipulation

5.5 Records Archival

ORNL maintains and archives adequate records pertaining to the operation of the ORNL PKI.

5.5.1 Types of records archived

CA archive records are sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including those revoked or expired) issues by the CA

At a minimum, the following records are archived based on ORNL standard policies:

- Certificate Policy (each version)
- Certification Practice Statement (each version)
- System and equipment configuration
- Modifications and updates to system or configuration (Change Control records)

- Certificate requests
- Revocation requests
- All certificates issued and published
- Record of a re-key
- All CRLs issued / published
- Applicable Audit Logs

5.5.2 Retention period for archive

Archive records are kept for 10 years and 6 months.

5.5.3 Protection of archive

Only authorized individuals are permitted to add or delete from the archive. Archive media is stored in a safe, secure storage facility separate from the production CA location.

5.5.4 Archive backup procedures

All backups are performed according to ORNL Standard backup policies and procedures.

5.5.5 Requirements for time-stamping of records

All documents archived are marked with the date of their creation or execution.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to Obtain & Verify Archive Information

Only authorized personnel are able to obtain access to the archived information. The integrity of the archived information is verified when it is restored.

5.6 Key Changeover

A CA's private signing key must be changed if there is evidence of compromise. Current best practice indicates that periodic forced changes create more risk than is mitigated, in the absence of suspected key compromise. Once a new private signature key has been generated, only the new key is used to sign CA and subscriber certificates. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key is retained and protected.

CAs will use the following maximum key usage periods. A Subordinate/Issuing CAs may use a shorter CA private key and/or CA certificate validity period.

Key Size	Private Key Usage Period	Certificate Validity Period
4096	Root CA	30 years
4096	Subordinate/Issuing CA	10 years
2048	Subscriber	2 years

Automatic key changeover is not supported; a new certificate request is required. All such requests are processed in the same manner as the initial application.

5.7 Compromise and Disaster Recovery

BSO maintains a ORNL PKI Contingency Plan, which is updated by ORNL standards. The ORNL PKI Contingency Plan defines the acceptable system outage and recovery time periods.

In any key compromise situation, a report is filed as defined in the Incident Management IOP, indicating the circumstances under which the compromise occurred. ORNL Cybersecurity will determine if a possible follow up investigation and potential action is required.

5.7.1 Incident and Compromise Handling procedures

In addition to the requirements defined in the Incident Management IOP, the ORNL ISSM/CISO and the ORNL IT Director are notified if any CA operating under this CPS experiences the following:

- Suspected or detected compromise of the CA systems
- Suspected or detected compromise of a certificate status server (CSS) if (1) the CSS certificate has a lifetime of more than 72 hours and (2) the CSS certificate cannot be revoked
- Physical or electronic penetration of CA systems
- Successful denial of service attacks on CA components
- Any incident preventing the CA from issuing a CRL within prescribed window.

5.7.2 Computing resources, software, and/or data are corrupted

In the event of an inoperative ORNL CA due to equipment damage, software or Operating System failure, or data corruption, where all copies of the CA signature keys are not destroyed, the following steps, at a minimum, are taken to recover a secure environment:

- The ORNL CA infrastructure (hardware and software) are re-built and/or restored from backup as necessary
- An ORNL CA can be reconstituted within documented Recovery window documented in the DR Plan.
- The CA data, encryption certificates and CRLs/ARLs, are restored if the CA becomes unusable and must be restored from backup or if the CA data is suspected to be corrupt.

5.7.3 Entity Private Key Compromise Procedures

If the ORNL PKI discovers or has reason to believe that a CA private key has been compromised, the following actions are taken (per policy)

- The ISSM/CISO and the IT Director are to be notified;
- Immediately cease using the compromised certificate, unless otherwise directed by cognizant law enforcement or incident management personnel for a defined period of time to collect additional information on adversarial action;
- Revoke the certificate and publish the serial number on the appropriate CRL and publish CRL to repositories;

- Revoke all certificates signed with the private key that corresponds to the public key listed in the certificate;
- Take reasonable steps to notify participants to cease using any certificates that are linked to the revoked certificate in question.

5.7.4 Business Continuity Capabilities after a Disaster

The CA has in place an appropriate contingency plan, disaster recovery plan, or business resumption plan that is capable of resuming services in accordance with this CPS. If CA equipment is damaged or rendered inoperative, but CA signature keys are not destroyed, CA operations are reestablished, giving priority to the ability to generate certificate status information.

5.8 CA & RA Termination

In the event of a CA or RA termination, ORNL PKI will provide as much advance notice as circumstance permits to relying parties prior to the termination. The CA will preserve relevant records for a period of time deemed fit for functional and legal purposes

Before the ORNL CA terminates its services, the ORNL CA will:

- Make all reasonable efforts to inform subscribers and cross-certifying CAs
- Make knowledge of its termination widely available
- Cease issuing certificates and CRLs
- Destroy all copies of private keys

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Certificate may only be issued for a public key in the situation where the corresponding private key has been generated in a secure ORNL PKI facility. Where cryptographic modules are used, the private keys are generated in them and remained there in encrypted form, and are decrypted only at the time at which they are being used.

6.1.1.1 CA Key Pair Generation

Hardware tokens (validated for FIPS 140-2 level 2 for cryptographic functions and level 3 for tamper resistance) are used to generate and store the ORNL CA keys.

ORNLCA key pair generation is performed in accordance with a written Key Generation script (procedure) which must create a verifiable audit trail that the security requirements for procedures were followed. The audit trail must identify and document any failures or anomalies in the key generation process, and any corrective actions taken. The documentation of the procedure must be detailed enough to show that appropriate role separation was used.

The CA key pair generation are in compliance with PKCS#1.

The private key will never be exposed outside the module in unencrypted form.

6.1.1.2 Subscriber Key Pair Generation

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

6.1.2 Private Key delivery to subscriber

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply. When CAs or RAs generate keys on behalf of the subscriber, then the private key are delivered securely to the subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements are met:

- Anyone who generates a private signing key for a subscriber will not retain any copy of the key after delivery of the private key to the subscriber.
- The private key(s) are protected from activation, compromise, or modification during the delivery process.
- Delivery are accomplished in a way that ensures that the correct tokens and activation data are provided to the correct subscribers.
    - For hardware modules, accountability for the location and state of the module are maintained until the subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material is encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data are delivered using a separate secure channel. The CA will maintain a record of the subscriber acknowledgement of receipt of the token.

6.1.3 Public key delivery to Certificate Issuer

Where key pairs are generated by the subscriber or RA, the public key and the subscriber's identity are delivered securely to the CA for certificate issuance. The delivery mechanism will bind the subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it is at least as strong as the CA keys used to sign the certificate.

Public keys are delivered to the certificate issuer in such a way that the issuer can determine:

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

6.1.4 CA public key delivery to relying parties

CA public keys are distributed in CA certificates and can be obtained from the ORNL PKI repository, or through automated methods via a registration authority application.

6.1.5 Key sizes

Certificates issued under this CPS will meet or exceed the key sizes listed in the CP.

Root CA -4096Bit RSA

Issuing CA-4096Bit RSA

End Entity Certificate-2048 RSA.

6.1.6 Public key parameters generation and quality checking

No stipulation.

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

See the section 7.1.1 for base certificates and 7.1.2 for certificate extensions.

6.2 Private Key Protection and Crypto-Module Engineering Controls

ORNL has implemented a combination of physical, logical and procedural controls to ensure the security of ORNL CA private keys. Logical and procedural controls are described in the section 6.5, 6.6. Physical access controls are described in the section 5.1.2. Subscribers are required to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic module standards and controls

- Offline CAs will use a FIPS 140-2 Level 2 or higher validated hardware cryptographic module.
- Online CAs, RAs, and CSS will use software or hardware based cryptographic modules.

6.2.2 Private Key (m out of n) multi-person control

There are multiple person controls for CA key generation operations. At a minimum, there are multi person control for operational procedures such that no one person can gain control over the CA private key.

A single person will not be permitted to activate or access any cryptographic module that contains the complete CA private signing key. CA signature keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery are under least two-person control.

6.2.3 Private Key escrow

CA private keys are never escrowed. Subscriber keys may be escrowed to provide key recovery as described in section 4.12.

Under no circumstances are signature keys used to support non-repudiation or digital signature services escrowed by a third party.

6.2.4 Private Key backup

ORNL PKI will not store backups of end-entity or CA private keys, (Except if user certificate is used for Encryption)

The HSM containing the ORNL CA keys are cloned in order to support the high availability CA configuration and Disaster Recovery. Cloning copies the contents of one secure cryptographic token to

another without exposing the keys outside of the HSM. The cloning procedure maintains hardware secured backups and verifiable audits through a direct hardware-to-hardware backup procedure.

To prevent unauthorized use of backup materials, backup tokens maintain the same access controls as the original.

- Issuing CAs are backed up
- Issuing CA Backups are protected with the same level of protection afforded the original.

6.2.5 Private Key archival

CA private signature keys and subscriber private signatures keys will not be archived.

CAs that retain subscriber private encryption keys for business continuity purposes will archive such subscriber private keys, in accordance with section 5.5.

6.2.6 Private Key transfer into or from a cryptographic module

- Software based keys may be exported and transferred in an encrypted fashion between systems to support system upgrades or disaster recovery.
- CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in section 6.2.4.
- At no time will the CA private key exist in plaintext outside the cryptographic module.
- All other keys are generated by and in a cryptographic module.
- In the event that a private key is to be transported from one cryptographic module to another, the private key is encrypted during transport; private keys will never exist in plaintext outside the cryptographic module boundary.

6.2.7 Private Key storage on cryptographic module

No stipulation beyond that specified in FIPS 140-2.

6.2.8 Method of activating private key

- All ORNL PKI participants will take reasonable measures to protect the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.
- Examples of activation data are Windows logon credentials, device PINs, or passwords.
- At no time are passwords be shared.
- All access is authenticated and logged
- All access is authenticated to the cryptographic module before the activation of the private key.

6.2.9 Method of deactivating private key

- ORNL CA keys are deactivated upon system shutdown or stoppage of the CA services.
- Cryptographic modules that have been activated will not be available to unauthorized access.
- After use, the cryptographic module is deactivated (e.g. via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CPS).

- CA cryptographic modules are removed and stored in a secure container when not in use unless the CA hardware itself is secured within a secure container.

6.2.10 Method of destroying private key

- CA keys are destroyed when they are no longer required.
- Software based key will have the disk(s) containing the key zeroed or physically destroyed, along with securely deleting any backup copies of the key.
- Individuals in Trusted Roles will destroy CA, RA, and CSS private signature keys when they are no longer needed.
- Subscribers will destroy their private signature keys, when they are no longer needed or when the certificates to which they correspond expire or are revoked.
- Physical destruction of HSM hardware is not required.
- To ensure future access to encrypted data, subscriber private key management keys should be secured in long-term backups or archived

6.2.11 Cryptographic Module Rating

All ORNL CAs under this CPS have their private key is stored in a FIPS 140-2 Level 2 compliant Hardware Security Module.

6.3 Other aspects of Key Management

6.3.1 Public Key Archival

The CAs public keys are archived as part of the certificate archive process.

6.3.2 Usage Periods for the Public and Private Keys

The usage periods for public and private keys are:

- Root CA key and certificate: 30 years
- Subordinate/Issuing CA key and certificate: 10 years
- Subscriber key and certificate: 2 years
- All certificates signed by a specific CA key pair will expire before the end of that key pair's usage period.

6.4 Activation Data

6.4.1 Activation data generation and installation

- The activation data used to unlock private keys, in conjunction with any other access control, will have an appropriate level of strength for the keys or data to be protected.
- This data is user-selected.
- PED Tokens have to be initialized before they are used for private key generation and access to Hardware Security Module.
- PED Tokens are user-selected.

6.4.2 Activation data protection

Data used to unlock private keys are protected from disclosure by a combination of cryptographic and physical access control mechanisms.

Activation data may be:

- Memorized
- Biometric in nature
- Recorded and secured at the level of assurance associated with the cryptographic module, and will not be stored with the cryptographic module.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

ORNL performs all CA functions using trustworthy systems that meet the requirements of the ORNL CSP.

6.5.1 Specific Computer Security Technical Requirements

Computer security controls are required to ensure CA/RA operations are performed as specified in this CPS. The following computer security functions pertaining to the ORNL PKI are provided by the operating system, or through a combination of operating system, software, and physical safeguards:

- Require authenticated login
- Provide discretionary access control
- Provide a security audit capability
- Enforce access control for CA services and PKI roles
- Require separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object reuse or require separation for CA random access memory
- Require use of cryptography for session communication and database security
- Archive CA history and audit data
- Require a trusted path for identification of PKI roles and associated identities
- Require a recovery mechanism for keys and the CA system
- Enforce domain integrity boundaries for security-critical processes.

For other CAs operating under this CPS, the computer security functions listed below are required. These functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts will include the following functionality:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see section 5.4)
- enforce domain integrity boundaries for security critical processes; and

- Support recovery from key or system failure.

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions;
- enforce domain integrity boundaries for security critical processes; and
- Support recovery from key or system failure.

All communications between any PKI Trusted Role and the CA are authenticated and protected from modification.
ORNL PKI will use industry standard CA software, PKI applications and cryptographic modules.

ORNL PKI systems are secured from unauthorized access. Authorized access to production servers are limited to those individuals with a valid business reason for such access.

PKI systems will comply with the ORNL CSP. The network as a whole are protected by industry standard intrusion detection systems and firewalls.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

CA and RA software adheres to the following development controls:

- Software is designed and developed under a formal, documented development methodology;
- Hardware and software is procured in a fashion that reduces the likelihood that a component was tampered with;
- Hardware and software are shipped and delivered via controlled methods that provide a chain of accountability;
- Proper care are taken to prevent malicious software from being loaded onto the equipment;
- Hardware and software updates are purchased and developed in the same manner as the original equipment, and are installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

- The configuration of the CA and RA are documented and controlled.
- A change management methodology is used for installation and ongoing maintenance of CA and RA systems.
- There is a mechanism for detecting unauthorized modification to the software or configuration.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

ORNL performs all its CA functions using networks secured in accordance with ORNL security policy to prevent unauthorized access and other malicious activities.

All unused network ports and services on the CA system are disabled. Network software present and operational on the CA system is be necessary for the proper functioning of the CA system.

6.8 Time stamping

Certificates, CRLs, and other revocation database entries will contain time and date information. This time are accurate based on the available network time service.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

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

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

7.1.1 Version Number(s)

ORNL CA will issue X.509 Version 3 certificates.

7.1.2 Certificate Extensions

The ORNL PKI supports the use of any defined X.509 v3 Certificate extensions:

- Mandatory Issuing CA certificate extensions:
    - Basic Constraints: Pathlength=0
    - Certificate Policies

7.1.3 Cryptographic Algorithm Object Identifiers

Certificates issued under this CPS use cryptographic functions currently approved by NIST and identified using the OIDs defined in the NIST Computer Object Security Register.

7.1.4 Name Forms

The subject field in ORNL certificates issued are populated with an X.500 distinguished name as specified in section 3.1.1.

The issuer field of ORNL certificates issued under the policies in this document are populated with a non-empty X.500 Distinguished Name as specified in section 3.1.1.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this CPS will assert at least one of the OIDs identified in section 1.2 in the certificate policies extension.

7.1.7 Usage of Policy Constraints Extension

The CAs may assert name constraints in CA certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

ORNL CA will issue X.509 version **2** CRLs in accordance with the **RFC 5280**.

The PKI end entity software will support all the certificate profile basic fields (section 7.1.1) and any certificate extensions defined in section 7.1.2.

Field	Description
Version	2
Signature Algorithm	Algorithm used to sign the CRL
Issuer Name	Entity that signed and issued CRL
Effective Date	Issue date of the CRL
Next Update	Expiration date of the CRL
Next CRL Publish	Date when next CRL are published
Revoked Certificates	List of revoked certificates

7.2.2 CRL and CRL entry extensions

No Stipulation.

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a method to obtain timely information about the revocation status of a certificate. OCSP is not currently planned.

7.3.1 Version Numbers

The OCSP specification as defined by IETF RFC 5019 is supported

7.3.1 OCSP Extensions

All use of standard OCSP request and response extensions will comply with IETF RFC 5019.

8 Compliance Audit and Other Assessment

No external audits are required, only a self-assessment by ORNL CAs that its operation is according to this document. For high assurance environment external relying parties may request an audit review of the PKI infrastructure.

8.1 Frequency of Audit or Assessments

PKIs compliant to any ORNL Certification Practices Statement will undergo a yearly assessment to determine compliance to appropriate Certificate Policies and the relevant Certification Practices Statement that fulfills the provisions outlined in appropriate Certificate Policies

8.2 Identity/qualifications of Assessor

The assessor should be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 Assessor's Relationship to Assessed Entity

The assessor will not hold a trusted role in the PKI being assessed, but is affiliated with the organization.

8.4 Topics covered by assessment

The purpose of an assessment is to verify that a CA and its recognized RAs comply with **all** the requirements of the current versions of this CPS and the CA's CPS.

The compliance audit verifies that the operational and technical controls used by the ORNL CA, operations personnel, including all RA's, satisfy all requirements of the ORNL CP, and the stipulations in this CPS, including all the following topics:

- Identification & Authentication (Section 3)
    - Initial Registration
    - Certificate Renewal, Update, and Routine Re-key
    - Re-key After Revocation
    - Revocation Request
- Certificate Life-Cycle Operational Requirements (Section 4)
    - Application for a Certificate
    - Certificate Issuance
    - Certificate Acceptance
    - Certificate Suspension and Revocation
    - Security Audit Procedures
    - Records Archival
    - Key Changeover
    - Compromise and Disaster Recovery
    - CA Termination
- Facility, Management, and Operational Controls (Section 5)
    - Physical Controls
    - Procedural Controls
    - Personnel Controls
- Technical Security Controls (Section 6)
    - Key Pair Generation & Installation
    - Private Key Protection
    - Other Aspects of Key Pair Management
    - Activation Data
    - Computer Security Controls
    - Life-cycle Technical Controls

    - Network Security Controls
    - Cryptographic Module Engineering Controls
- Certificate, CRL and OCSP Profiles (Section 7)
    - Certificate Profile
    - ARL/CRL Profile
- Specification Administration (Section 8)
    - Specification Change Procedures
    - Publication and Notification Procedures
    - CPS Approval Procedures

All aspects of the CA/RA operation are subject to assessment inspections.

8.5 Actions as a result of findings

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

The assessor will note the discrepancy

The assessor will notify the parties identified in section 8.6 of the discrepancy

The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the ORNL ISSM/CISO and appropriate CA Management Authority.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, The ORNL Audit team may decide to:

- Temporarily halt operation of the CA or RA
- Revoke a certificate issued to the CA or RA
- Take other actions it deems appropriate.

8.6 Communication of Results

The compliance assessor will communicate results of all compliance audits through a Compliance Assessment Report. The report will contain a summary table of topics covered, areas in which the ORNL CAs was found to be non-compliant and a brief description of the problems for each area of non-compliance. The report will also contain the detailed results of the compliance audit for all topics covered, including the topics in which the ORNL CA passed and the topics in which the ORNL CAs failed. BSO, in coloration with other cognizant ORNL organizations, proposes remedies for any topic failure, including expected time for completion.

9 Other Business and Legal Matters

9.1 Fees

No Stipulation

9.1.1 Certificate Issuance or Renewal Fees

No Stipulation

9.1.2 Certificate Access Fees

There are no charges for access to the ORNL CA certificate or to Subscriber certificates.

9.1.3 Revocation or Status Information Access Fees

There are no charges for access to Revocation, CRL or CSS Status information.

9.1.4 Fees for Other Services

ORNL reserves the right to set fees in accordance with this CPS and MOA's for other services provided by ORNL security.

9.1.5 Refund Policy

No Stipulation

9.2 Financial Responsibility

This CPS contains no limits on the use of certificates issued by CAs under this policy. Rather, entities, acting as relying parties, will determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

9.2.1 Insurance Coverage

No Stipulation

9.2.2 Other Assets

No Stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities

No Stipulation

9.3 Confidentiality of Business Information

CAs Information not requiring protection are made publicly available. Public access to organizational information are determined by the respective organization.

9.3.1 Scope of Confidential Information

Each Subscriber's private signing key is confidential to that Subscriber. The CA and RA are not provided any access to those keys.

Information held in audit logs and the archives is considered confidential to the ORNL security and is not released to external parties, unless required by law.

9.3.2 Information Not Within the Scope of Confidential Information

Information included in certificates and CRLs issued by the ORNL CA are not considered confidential.

9.3.3 Responsibility to Protect Confidential Information

The ORNL ISSM/CISO has the responsibility to ensure that controls exist to protect the confidential information in section 9.3.1.

9.4 Privacy of Personal Information

All Subscribers identifying information as defined by local privacy regulations are protected from unauthorized disclosure.

The ORNL PKI does not collect any confidential or private subscriber information

9.4.1 Privacy Plan

Subscribers identifying information is protected from unauthorized disclosure.

9.4.2 Information Treated as Private

Information that is not contained in the public certificates are treated as private

9.4.3 Information Not Deemed Private

Certificates and the information in them are not considered private.

9.4.4 Responsibility to Protect Private Information

Recipients of private information will secure it from unauthorized access and disclosure to third parties and will comply with all applicable local privacy laws.

9.4.5 Notice and Consent to Use Private Information

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

This section is subject to applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

ORNL are entitled to disclose Confidential/Private Information if, in good faith, ORNL believes that:

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

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances

No Stipulation

9.5 Intellectual Property Rights

ORNL will not knowingly violate intellectual property rights held by others.

9.6 Representations and Warranties

The ORNL ISSM/CISO, in collaboration with the ORNL IT Director, will:

- Approve the CPS for each CA that issues certificates under this CP;
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSs;
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CPS.
- Revise this CPS to maintain the level of assurance and operational practicality;
- Publicly distribute this CP
- Coordinate modifications to this CPS to ensure continued compliance by CAs operating under approved CPSs.

9.6.1 CA Representations and Warranties

CAs operating under this CPS will warrant that their procedures are implemented in accordance with this CPS, and any certificate issued that assert the policy OIDs identified in this CPS were issued in accordance with the stipulations of this CPS.

A CA that issues certificates that assert a policy defined in the document will conform to the stipulations of this document, including:

- Providing to the ORNL Audit a CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3.
- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.
- There are no material misrepresentations of fact in the certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS and the applicable CPS, and

- Revocation services and use of a repository conform to all material requirements of this CPS and the applicable CPS in all material aspects.

9.6.2 RA Representations and Warranties

An RA that performs registration functions as described in this CPS will comply with the stipulations of this CPS, and comply with a CPS approved by ORNL Risk Management for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities. An RA supporting this policy will conform to the stipulations of this document, including:

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Ensuring that obligations are imposed on subscribers, in accordance with section 9.6.3, and subscribers are informed of the consequences of not complying with those obligations.
  There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate
- Their Certificates meet all material requirements of this CPS and the applicable CPS
- Revocation services (when applicable) and use of a repository conform to all material requirements of this CPS and the applicable CPS in all material aspects.

9.6.3 Subscriber Representations and Warranties

A subscriber (or human sponsor for device certificates) will:

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private key(s) at all times, in accordance with this CPS, as stipulated any certificate acceptance agreements and local procedures. (Where applicable.)
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notifications are made directly or indirectly through mechanisms consistent with the CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s)
- Promptly cease using a certificate and notify ORNL if any certificate information changes, becomes misleading or there is any actual or suspected misuse or compromise of the private Key associated with the certificate
- Use the certificate only for authorized and legal purposes.

9.6.4 Relying Party Representations and Warranties

Subscribers will use the certificates for only the purpose for which it was intended and check each certificate for validity.

This CPS does not specify the steps a Relying Party should take to determine whether to rely upon a certificate. The Relying Party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e. certificates and CRLs) needed to perform the trust path creation, validation, and CPS mappings that the Relying Party may wish to employ in its determination.

9.6.5 Representation and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

CAs operating under this policy may not disclaim any responsibilities described in this CPS.

9.8 Limitations of Liability

Unless otherwise contractually agreed upon, ORNL has no liability under this CPS.

9.9 Indemnities

To the extent permitted by law, relying parties and subscribers agree to indemnify, defend and hold harmless ORNL and its parent organization (DOE), managers, officers, employees and agents (each an "Indemnified Party") from any claim, liability, cost, expense or loss (including reasonable attorneys' fees and expenses) arising out of any breach of any obligation, representation or warranty hereunder by any of its employees, agents or LRAs, or out of the performance of the duties of any of them under this Agreement, the Applicable Policy Documentation, or any applicable statute or rule of law.

9.10 Term and Termination

9.10.1 Term

This CPS is effective immediately upon publication.

9.10.2 Termination

Termination of this Certification Practices Statement is at the discretion of ORNL

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communication

No Stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

This CPS may be amended by approval of the ORNL ISSM/CISO and the ORNL IT Director.

9.12.2 Notification Mechanism and Period

Proposed changes to this CPS are distributed electronically to the members. If the changes are not deemed substantial, the subscribers are notified at the renewal.

9.12.3 Circumstances under which the OID are changed

If a change in the Certification Practices Statement or Certification Practices is determined to be necessary by security to warrant a change in the currently specified OID for a particular type of certificate, then the revised version of this CPS will also contain a revised OID for that type of certificate.

9.13 Dispute Resolution Procedures

The ORNL Office of the CIO will facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy.

9.14 Governing Law

The laws of the United States of America and the laws of the states in which the Subscriber and Relying Party are domiciled will govern the enforceability, construction, interpretation, and validity of this CPS.

9.15 Compliance and Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting or importing software, hardware or technical information.

9.16 Miscellaneous Provisions

No Stipulation.

9.16.1 Entire Agreement

No Stipulation.

9.16.2 Assignment

No Stipulation.

9.16.3 Severability

Should it be determined that one section of this CPS is incorrect or invalid, the other sections will remain in effect until the policy is updated. Requirements for updating this CPS are described in Section 9.12.

9.17 Other Provisions

No Stipulation.