X.509 Certification Practice Statement

For The

U.S. Higher Education Root (USHER)

CA1 Certification Authority

1 June 2007

Version 1.0.1

Signature Page

This Certification Practice Statement (CPS) has been developed by the U.S. Higher Education Root (USHER) Policy Authority (USHER PA). It becomes the official USHER CA1 CPS when signed by the Chair of the USHER Policy Authority.

The global Object Identifier (OID) for this document is { 1.3.6.1.4.1.24726.3.1 }. See section 1.2 for this and other OID assignments defined for this CPS.

Jim Jokl

Jim Jokl, Chair of the USHER Policy Authority

JUNE 1, 2007

Date

Revision History

Document Date	Revision Details
0.1	Original RFC 3647 version

Table of Contents

1. INTRODUCTION

This Certification Practice Statement (CPS) defines the processes and operations used to implement the U.S. Higher Education Root (USHER) CA1 Certification Authority (CA), and any subordinate CAs, in accordance with the USHER Foundation Level Class of Certification Authorities Certificate Policy (USHER Foundation Level CP). The USHER CA1 CA is the root of the USHER Foundation Level Class of CAs and operates under a self-signed authority certificate. CA1 in turn issues CA authority certificates to CAs that are subordinate to CA1 (Subordinate PKI CA) and CAs operated by other entities that have entered into a binding agreement with USHER (Cooperating PKI domain CA). USHER also may accept and store in its repository other CA authority certificates naming CA1 as provided for in the USHER CP.

USHER (as used in the remainder of this document), is defined to mean the USHER PA or other delegated authority, such as the USHER Operating Authority (OA), Registration Authority (RA), business office, or other entity representing USHER services. Cooperating PKI domains at the Foundation level are encouraged to publish their own CP and/or CPS since USHER provides no oversight to these subscribing CAs at this level of assurance, and relying parties must make their own determination of trustworthiness.

This CPS describes the operation of the USHER CA1 Certification Authority and any CAs subordinate to it at the Foundation assurance level. All description of the purposes and uses of USHER certificates and the requirements and stipulations about how the USHER CAs are to be operated may be found in the USHER CP identified above. **THE USHER PA ASSUMES NO LIABILITY FOR ANY LEVEL OF ASSURANCE ASSERTED BY A CA NOT MANAGED BY USHER.**

This USHER CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647 (November 2003), Certificate Policy and Certification Practice Statement Framework.

1.1 OVERVIEW

1.1.1 Certification Practice Statement (CPS)

This CPS documents the internal practices and procedures used by USHER. It covers the operation of systems and the management of facilities of the USHER CA1 and subordinate CAs, and the USHER repository used to facilitate interoperability between USHER Subscribers.

1.1.2 Relationship Between the CP and CPS

This CPS states how the requirements of the USHER Foundation Level CP are met for the USHER CA1 CA and any of its subordinate CAs. The USHER Policy Authority (PA) is responsible for reviewing and approving this CPS. The USHER Foundation Level CP from which this CPS is derived is identified with global Object Identifier 1.3.6.1.4.1.24726.1.1. A copy can be acquired at: **http://www.usherca.org/docs/Foundation-CP.pdf**

1.1.3 Relationship Between the CPS and a Subordinate PKI Domain CP

Subordinate PKI domains certified by USHER CA1 are managed by the USHER OA in accordance with the same USHER Foundation Level CP and therefore operate as defined by this CPS.

1.1.4 Relationship Between the CPS and a Cooperating PKI domain CP

There is no relationship between the contents of a Cooperating PKI domain CP and this CPS. Appropriate operation of a Cooperating PKI Domain is established through execution of the USHER subscriber agreement.

1.1.5 Scope of Services

USHER accepts applications for USHER membership from higher education institutions and their partners. USHER determines eligibility for membership and verifies that an appropriate entity has requested this membership. Once the applicant agrees to operate based on the USHER Expected Practices and signs the USHER subscription agreement (Agreement), USHER issues authority certificates to all CAs in the Cooperating PKI domain as requested by the subscriber.

1.1.6 Definition of Terms used in this CPS

In this CPS, the following terms define the scope of USHER services and its Subscribers.

A Cooperating PKI Domain is one that has been verified by the USHER PA and/or OA as eligible to participate in an USHER Foundation Level CA service. Once an Agreement has been duly authorized by both USHER and a Cooperating PKI Domain, that domain is considered a Subscribing PKI Domain (Subscriber).

A Subordinate PKI Domain is one that follows the policy of the USHER Foundation CP and the practices outlined in this CA1 CPS and is operated by the USHER OA.

Other terms are defined in Section 1.6 of this CPS.

1.1.7 Interoperation with CAs External to Higher Education

Organizations external to higher education may be granted eligibility for USHER services if sponsored by a higher education USHER subscriber and approved by the USHER PA. In this case, the USHER OA will follow all procedures applicable to Cooperating PKI domain CAs as described in section 1.1.6 above.

1.2 IDENTIFICATION

The OIDs used by USHER are registered under the Internet Assigned Numbers Authority (IANA) arc as described in the USHER CP. The Object Identifier (OID) assigned to this CPS by the USHER PA is found on the signature page of this CPS. Subsequent major revisions of this CPS shall have new OID assignments under the id-usher-cps-ca1 arc, i.e., 1.3.6.1.4.1.24726.3.1.1 et. seq.

1.3 PKI PARTICIPANTS

Primarily, institutions of higher education may participate. Other organizations may also become Subscribers if they are both sponsored by a subscribing institution of higher education and approved by the USHER PA as described in section 1.1 above. USHER CAs also may issue certificates to individuals and infrastructure components as directed by the PA or OA.

1.3.1 PKI Authorities

1.3.1.1 Internet2 and AIRE

USHER is a service under a single-member LLC known as the Advanced Infrastructure for Research and Education (AIRE). Internet2 is the single member of this LLC.

1.3.1.2 Policy Authority (PA)

The USHER PA is the governing body for USHER. The seven (7) members of the PA are appointed by AIRE to represent the interests of subscribing PKI domains. The USHER PA approves the USHER CP and this CPS, sets standards for USHER membership, directs and oversees the USHER OA, and resolves issues that might arise concerning USHER services. Decisions of the PA require an affirmative vote by a simple majority of PA members for approval with the exception of approval of the USHER CP and CPS which requires an affirmative vote by at least five (5) of the seven (7) members (70%) of the PA.

1.3.1.3 Operational Authority (OA)

The USHER Operational Authority (OA) is the organization that is responsible for the implementation of all the details of this CPS and the day to day operation of the CA. The Manager of the OA (OM) is hired by Internet2 and assigned by AIRE. The staff of the OA are approved by the OM and hired by Internet2. Consultants or other advisors may help with specific projects or technical designs. The OA is located at the Internet2 offices in Ann Arbor, MI. See section 9.17.1 for the address.

1.3.1.3.1 USHER Operational Authority Administrators

USHER CA1 will have a designated OA Administrator who is responsible for configuring PA-approved certificate profiles and administering the technical components within the USHER OA.

1.3.1.3.2 USHER Operational Authority Officer and Manager

USHER CA1 will have a designated Officer to facilitate the dual access controls on its key material and perform RA functions, and a designated Manager (OM) to manage the personnel and roles of USHER operations. This may be a single individual.

1.3.1.4 PKI Domain Principal Certification Authority (Principal CA)

The USHER CA1 CA is the Principal CA for any cross-certification with USHER.

1.3.1.5 U.S. Higher Education Root (USHER) Certification Authority

The USHER CA manages the life cycle of all certificates it issues, including authority certificates for USHER subscribing organizations. Upon acceptance of a certificate issuing request, the CA manufacturers the appropriate certificate in accordance with one of the profiles approved by the PA. The certificate is published in the USHER CA repository and delivered to the subscriber or sponsoring individual, as appropriate. Re-key, renewal, update, modification and revocation are handled by the OA according to the requirements of the CP.

1.3.1.6 Related Authorities

The USHER CA uses Internet2 personnel for its operational, organizational support, and management services. USHER also relies on the services of other trusted community members for the storage of certain back-up and archive components as described later herein.

1.3.2 Registration Authorities

The USHER OA oversees and delegates to AIRE the Registration Authority responsibilities and role of USHER CA1 RA. The USHER PA has approved the use of the AIRE Registration Authority Processes document for the RA requirements for USHER CA1.

1.3.3 Subscribers

Subscribers are as defined in section 1.1.6 and as appropriate to the context of this CPS, may also be: subordinate USHER CAs; certain personnel who require strong digital credentials in order to work with USHER; and certain infrastructure components that are part of the USHER system.

1.3.3.1 Certificate Subjects Who are Natural Persons

USHER OA personnel responsible for the operation of an USHER CA, or any other natural person with approval from the USHER PA for a specific purpose, will (if required) be issued an administrative certificate with a unique identifier in the subjectName field that identifies the person as known to the USHER RA. Verification of uniqueness will be a manual process by the OA Manager before the credential is issued.

1.3.3.2 Certificate Subjects That Are Not Natural Persons

USHER CA1 may issue device certificates to support the operation of its infrastructure as requested by the USHER OA Manager. The USHER PA has delegated this responsibility to the OA Manager.

1.3.3.3 Certificate Subjects That Are Subordinate PKI Domain CAs

USHER CA1 will issue (if required) a CA authority certificate to another CA operated by USHER for the purpose of issuing PKI certificates to a subset of USHER subjects. The PA will authorize issuance of such certificates.

1.3.3.4 Certificate Subjects That Are Cooperating PKI Domain CAs

USHER CA1 will issue authority certificates to a Cooperating PKI domain CA that has met USHER eligibility requirements, has signed an Agreement, and has agreed to abide by the USHER Expected Practices, when directed by the USHER PA.

1.3.4 Relying Parties

This CPS makes no stipulation with respect to Relying Parties. **However, Relying Parties are reminded that they alone are responsible for whether they rely on the validity or contents of any certificate issued by USHER or any USHER recognized CA.**

1.3.5 Other Participants

The USHER PA may from time to time authorize issuance of an USHER PKI certificate to other entities. Such issuance will be carried out by the OA as directed by the PA.

1.4 USHER CERTIFICATE USAGE

CA1 authority certificates will be issued per the details outlined in Key Usage Purposes, Section 6.1.7. Usage for Relying Parties is further defined in Section 1.4 of the USHER Foundation Level CP. **USHER does not monitor nor attempt to enforce Key Usage restrictions nor does it place any restrictions on what a Cooperating PKI domain CA might do with the USHER certificate it receives other than that stated in section 1.4.2 below.**

1.4.1 Appropriate Certificate Uses

No stipulation.

1.4.2 Prohibited Certificate Usage

USHER CA1 certificates must not be used for purposes that violate U.S. law or the law of the country in which the target end-entity (e.g., application or host, addressee of an e-mail) is located. Remediation, termination, and revocation are governed by the USHER Expected Practices and the Agreement.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The USHER PA is responsible for approving this CPS as compliant with the USHER Foundation Level CP. The USHER OA is responsible for all aspects of the implementation of this CPS.

1.5.2 Contact person

Questions regarding this CPS shall be directed to the Chair of the USHER PA, whose address can be found on the USHER website (see Section 9.17.1).

1.5.3 Entity Determining CPS Suitability for the Policy

The USHER PA shall review the CPS for conformance to the CP and oversee its implementation by the USHER OA.

1.5.4 CPS Approval Procedures

Approval of this CPS shall require affirmative vote by the USHER PA as described in section 1.3.1.2 above.

1.6 ACRONYMS AND DEFINITIONS

1.6.1 Acronyms

AIRE	Advanced Infrastructure for Research and Education LLC, a single-member LLC under the aegis of Internet2
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
IANA	Internet Assigned Numbers Authority (see http://www.iana.org)
IETF	Internet Engineering Task Force (see http://www.ietf.org)
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OID	Object Identifier

PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
USHER	U.S. Higher Education [PKI] Root
USHER OA	U.S. Higher Education Root [CA] Operational Authority
USHER PA	U.S. Higher Education Root [CA] Policy Authority
WWW	World Wide Web

1.6.2 Definitions

Agreement	AIRE will enter into a Subscriber Agreement (Agreement) with an applicant PKI domain's policy authority (or equivalent duly authorized entity) setting forth the respective responsibilities and obligations of both parties.
Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or

	decryption events).
Applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Archive	Long-term, physically separate storage.
Attribute Authority	An entity, recognized by the USHER PA or comparable PKI domain body as having the authority to verify the association of attributes to a certificate subject entity.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to evaluate compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Authority Certificate	An x.509 certificate asserting in the certificate Basic Constraints that cA = “true” and in the KeyUsage that keyCertSign = “true”. Such a certificate constitutes the authority by which a Certification Authority may operate, as defined by the issuer of that certificate.
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a natural person.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CRLs.

CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to Subscribers.
Certificate Policy (CP)	A Certificate Policy is a definition of the principles and requirements for the operation and management of a PKI certification authority. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise, recovery, and administration of digital certificates. Indirectly, a certificate policy also can inform the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements.
Client (application)	A system entity, usually a computer process acting on behalf of a natural person, that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Component	A device, machine, or module such as a server, laptop computer, or software application. A component often requires a PKI certificate in order to perform its operations securely.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cooperating PKI Domain (CA)	PKI domains that are Subscribers to an USHER Foundation Level CA and whose policies and practices are in no way audited or otherwise verified for compliance by USHER.
Cross-Certificate	A certificate used to establish a trust relationship between two

	Certification Authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Device	Most often, a device is a piece of computer hardware such as a server or computer. See also definition for Component
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Direct Contact	Communication made by the OA or RA to a particular individual via in-person or telephone conversation or email with acknowledged response of reception by the contact.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue".
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Employee	Any person employed by a PKI domain.
Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Hardware Security Module	A secure container for an encrypted private key that does not

(HSM)	allow the key to be removed.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for establishing the requirements for protection of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Internet2	Internet2 as used in this document refers to the public name of the University Corporation for Advanced Internet Development and/or any successor organization that subsumes its obligations.
Key Escrow	A deposit of a private key and other pertinent information pursuant to an escrow agreement or similar contract, whereby one or more agents hold a private key for the benefit of the owner, Subscriber, employer, or other party, upon provisions set forth in the escrow agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Mutual Authentication	Occurs when parties at both ends of a communication activity

	authenticate each other (see authentication).
Natural Person	A human belonging to the mammalian species Homo sapiens. For details about natural persons as they relate to CA1, see section 1.3.3.1.
Non-Repudiation	Refers to the assurance that the recipient is provided with proof that the sender's digital signature corresponds to only the sender and not to any other entity that might cause a signature to be provided.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
Physically Isolated Network	A network that is not connected to entities or systems outside a physically controlled space.
PKI Certificate	A digital representation specified by ISO x.509 of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subject, (3) contains the Subject's public key, (4) identifies its validity period, and (5) is digitally signed by the certification authority issuing it.
PKI domain	A PKI domain as used in this CPS refers to a rooted hierarchical Public Key Infrastructure operating under a common CP, or a set of congruent CPs for which levels of assurance are mapped in a consistent manner against the PKI domain CA's LOAs.
PKI domain CA	A CA that acts on behalf of a PKI domain, and is under the operational control of a PKI domain PA/OA.
PKI Sponsor	Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Authority (PA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For

	the USHER Foundation Level Class of CAs, the PA is the USHER PA.
Principal CA	The Principal CA is a CA designated by a PKI domain to be certified by the USHER CA1 CA.
Privacy	Restricting access to Subscriber or Relying Party information in accordance with Federal or State law, PKI domain, and institutional policy.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, personnel, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate with the new public key.
Relying Party	A person or other 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 the information they provide.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CPS; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization.

Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	Administrative CAs under the purview of the USHER PA and which must abide by this CPS.
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity and (2) holds a private key that corresponds to the public key listed in the certificate. Additional information regarding Subscribers as defined by this CPS can be found in section 1.3.3.
Superior CA	In a hierarchical PKI, a CA which has certified the certificate public key of another CA, and which constrains the activities of that CA. (See subordinate CA).
Technical non-repudiation	The contribution that PKI mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Token	Hardware or software that contains or can be used to generate cryptographic keys. Examples of hardware tokens include smart cards and memory cards. Software tokens include both software cryptographic modules that store or generate keys, and storage devices or messages that contain keys (e.g., PKCS #12 messages).

Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
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."
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
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. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
USHER Certification Authority (USHER CA)	The USHER Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certification Practice Statements) that are used to provide CA authority certificates and end-entity certificates to qualified Subscribers..
USHER Operational Authority (USHER OA)	The USHER Operational Authority is the organization selected by the USHER Policy Authority to be responsible for operating the USHER Certification Authority infrastructure.
USHER Policy Authority (USHER PA)	The USHER PA is responsible for setting, implementing, and administering policy decisions regarding trust interoperability among PKI domains using the USHER CA.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

The USHER OA shall use reasonable practices to create and maintain a secure, reliable repository of CA records and an on-line server where public information is made available. Portable media (e.g., USB flash drive, CD, etc.) will be used for posting information from the offline USHER CA1 CA into its online repository.

2.1 REPOSITORIES

USHER CA1 will provide a web-based repository for publishing the root certificate, CRLs, and valid Subscriber certificates. The USHER CA1 repository will be protected in a manner prescribed by other secure Internet2 websites. In addition, critical documents such as CRLs are digitally signed to indicate USHER's authorization and enable verification of the integrity of their contents.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The USHER OA shall publish the CA1 root certificate, its current CRL, and a list of the valid Subscriber Authority certificates it has issued.

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificate status information is published as specified in section 4.9.7. A revised version of the CP and/or this CPS will be made publicly available subsequent to any approvals.

2.4 ACCESS CONTROLS ON REPOSITORIES

The USHER CA1 repository will have READ ONLY access to the public. Only USHER OA authorized operators will have WRITE, MODIFY or DELETE access to the repository.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

USHER CA1 will sign only certificates that contain an X.500 Distinguished Name (DN) in the Issuer and Subject name fields of the certificate. USHER CA1 will use certificate profiles approved by the USHER PA when issuing certificates.

3.1.2 Need for Names to be Meaningful

The USHER CA1 OA shall ensure that meaningful, easily understandable Distinguished Names (DNs) (as defined or approved by the USHER PA) are in the CSRs used to generate the certificates it issues.

3.1.3 Anonymity or Pseudonymity of Subscribers

N/A

3.1.4 Rules for Interpreting Various Name Forms

N/A

3.1.5 Uniqueness of Names

The USHER OA will only issue certificates with the approval of the USHER PA, which is responsible for maintaining name uniqueness across the USHER domain. The USHER OA will verify name uniqueness prior to certificate issuance.

3.1.6 Recognition, Authentication and Role of Trademarks

N/A

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

USHER CA1 accepts signed PKCS10 CSRs, which are reviewed and validated per the requirements in the appropriate Certificate Profile.

3.2.2 Authentication of Organization Identity

The USHER RA verifies the eligibility of all applicant organizations based on criteria approved by the USHER PA before permitting certificate requests. Requests for USHER CA1 certificates must include all information as outlined in the appropriate certificate profile. The USHER OA or

RA verifies the information provided in the certificate application to the best of its ability using trusted sources such as Department of Education Regional Accreditation Agency listings and/or Subscriber trusted Executive attestation for sponsored partners. If there are uncertainties about the organization's eligibility or identity, the PA will investigate and resolve the issues in the best interests of USHER.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Individual Identities

Certificates may be issued to natural persons for USHER-related business processes and include Internet2 and OA staff, USHER PA members, technical advisors and consultants, and trusted officers at subscribing organizations. The identities of individuals associated with USHER are verified by the OA Manager (OM) or the Chair of the PA either in person or through direct contact.

Trusted officers at each Subscriber organization include a delegated Executive named in the Agreement, and a delegated Administrator appointed by the Executive. The USHER CA1 RA verifies the identity information of trusted officers of Subscribing Organizations in accordance with the AIRE Registration Authority Process document which outlines out-of-band verification processes through direct contact. Additionally, the USHER RA records the process that was followed for each identity proofing. Minimally, the process will document the following:

- The identity of the person performing the identification;
- A signature by that person indicating that he or she verified the identity of the Subscriber's trusted officers in an out-of-band manner; and
- The date of the verification.

3.2.3.2 Authentication of Component Identities

USHER CA1 may issue certificates to subjects that are not natural persons as described in Section 1.3.3.2 and will verify that the component is under the control of the USHER OA before certificate issuance.

3.2.4 Non-Verified Subscriber Information

Information that is not verified is not included in Subject Name or Alternate Subject Name certificate fields.

3.2.5 Validation of Authority

The USHER CA1 RA verifies that the individual requesting a certificate is authorized to act in the name of the subscribing organization as described in section 3.2.3.1 above.

3.2.6 Criteria for Interoperation

N/A

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-Key

3.3.1.1 Certificate Re-Key

When an USHER CA1 issued authority certificate re-key is requested, the USHER OA identifies and authenticates the subscriber's trusted officer either by:

(a) Performing the initial registration identification process defined in Section 3.2, or

(b) If it has been less than ten years since a PKI domain Principal CA officer was identified as required in Section 3.2, verifying that the request is submitted using the currently valid credentials issued to the Subscriber's trusted officer by the USHER OA.

For USHER business-related certificates (see section 3.2.3.1), natural person or component end-entity certificates are re-keyed routinely if the entity's current certificate has not yet expired. Otherwise, initial authentication procedures are followed per section 3.2.3.1.

In all cases of certificate issuance, secure physical access procedures are followed as outlined in section 5.1.2.

3.3.1.2 Certificate Renewal

USHER CA1 issued authority certificates may be renewed pursuant the practices outlined in section 3.3.1.1.

3.3.1.3 Certificate Modification

USHER CA1 allows for the modification of previously issued authority certificates pursuant the practices outlined in section 3.3.1.1. Any new information is verified as described in section 3.2.2.

3.3.2 Identification and Authentication for Re-Key After Revocation

After a certificate issued by USHER CA1 has been revoked, the Subscribing organization may request a new authority certificate pursuant the practices outlined in section 3.3.1.1.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The USHER OA verifies revocation requests by authenticating the request either by direct contact based on the trusted officer's previously verified contact information, or use of the officer's USHER-issued credentials as described in section 3.3.1.1. A revocation request signed by the certificate's associated private key also is accepted and processed, regardless of whether or not the request has been authenticated.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 USHER CERTIFICATE APPLICATION

Prior to the Subscriber's submission of a PKCS#10 CSR, candidates for USHER authority certificates must either submit a signed copy of the USHER Subscriber Agreement to the USHER business office or must submit an online application found on the USHER website. See section 9.17.1 for addresses.

After eligibility criteria have been satisfied by the applicant organization, an Agreement must be signed with the applicant organization, and its trusted officers must be identity-proofed. Only after eligibility, Agreement, and registration can a CSR be securely and officially accepted and a certificate issued.

Natural persons or components with natural person sponsors will be issued certificates only after identity verification by the USHER OM. The OM will perform and log either in-person verification or direct contact with previously known persons to establish proof of identity before accepting certificate signing requests.

PA approval of all eligibility criteria is required by the USHER OA in order to issue all USHER CA1 certificates.

4.1.1 Who Can Submit a Certificate Application

Any USHER Agreement must be executed by an individual who has been designated by the organization as authorized to act on behalf of the organization for USHER membership. The Agreement will specify the trusted Executive officer who may make the actual CA certificate requests or who may delegate that task to a trusted Administrator.

4.1.2 Enrollment Process and Responsibilities

Prior to issuance, the applicant PKI domain will meet eligibility criteria and enter into an Agreement with AIRE setting forth their respective responsibilities. See section 4.1 for details.

4.2 CERTIFICATE APPLICATION PROCESSING

After application, eligibility, agreements, and registration of trusted officers (detailed in section 4.1 above), the Certificate Signing Request (CSR) will be checked manually to ensure it contains the correct information. If there are any unacceptable variances based on the Agreement and/or other reliable sources of information, then a new CSR will be requested. Once an acceptable CSR has been securely received, the Subscriber authority certificate will be issued.

4.2.1 Performing Identification and Authentication Functions

See Section 3. of this CPS.

4.2.2 Approval or Rejection of Certificate Applications

USHER may approve or reject an applicant organization based on applicability to the community or some other criteria that will be explained to the applicant. The USHER OA may reject a CSR that is malformed, not unique, unverifiable, or incorrect. The USHER PA determines all other rejection cases.

4.2.3 Time to Process Certificate Applications

No stipulation. Applications and CSRs will be processed as soon as practicable.

4.3 CERTIFICATE ISSUANCE

This certificate issuance section relates to Subscribers of the USHER CA1 CA.

4.3.1 CA Actions during Certificate Issuance

Upon receiving a request for a certificate from a verified, trusted Subscriber Officer with a valid digital credential, an officer of the USHER RA matches the CSR with any provisions detailed in the corresponding Agreement and certificate profile, and verifies that the CSR and accompanying information is correct and accurate, before issuing a certificate.

To issue a certificate, the system holding the offline CA is made operational, the CSR is imported from portable media, and pre-configured CA scripts are used to issue the certificate. After issuance, the certificate is copied back to the portable media for distribution to the Subscriber. The CA system is then powered down. These actions take place by trusted operators in a secure setting and in accordance with physical access protections in section 5.1.2.

The certificate then is made available to the Subscriber for review. If after one month the Subscriber has not confirmed that the certificate is correct, the certificate is revoked.

4.3.2 Notification to the Subscriber by the CA of Issuance of Certificate

The Subscriber is notified via email and must verify the contents of the certificate before it will become active and published. The certificate is delivered to Subscriber via email.

4.4 CERTIFICATE ACCEPTANCE

Once an USHER CA1 certificate has been issued, its acceptance by the Subscriber completes the OA's issuance responsibility

4.4.1 Conduct constituting certificate acceptance

Subscriber must confirm to the USHER OA that the content of the certificate is valid.

4.4.2 Publication of the Certificate by the CA

After the certificate has been accepted, the USHER-issued certificate is published to the USHER repository.

4.4.3 Notification of Certificate Issuance by the CA to other entities

The USHER OA notifies the Policy Authority via email when USHER CA1 issues an authority certificate to a Subscriber. The OA notifies all current USHER CA1 Subscribers regarding new authority certificates by sending an email to the Subscriber email distribution list after USHER receives confirmation of the validity of that certificate.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key is specified in the associated certificate. Subscribers also are required to comply with any requirements set forth in the Agreement.

4.5.2 Relying Party Public key and Certificate Usage

No stipulation. The Relying Party must decide pursuant to its own policies what actions to take.

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.

4.6.1 Circumstance for Certificate Renewal

If an entity has a currently valid certificate, that certificate may be renewed pursuant the practices and policy outlined in Section 3.3.1.1 if allowed under the certificate profile under which the certificate has been issued. This is accomplished by submitting a CSR with the same public key to the OA.

4.6.2 Who may request Renewal

See section 3.3.1.1.

4.6.3 Processing Certificate Renewal Requests

See section 4.3.1.

4.6.4 Notification of new certificate issuance to Subscriber upon Renewal

Same procedures as detailed under Section 4.3.2

4.6.5 Conduct constituting acceptance of a Renewal certificate

Same procedures as detailed under Section 4.4.1.

4.6.6 Publication of the Renewal certificate by the CA

Same procedures as detailed under Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to other entities

Same procedures as detailed under Section 4.4.3.

4.7 CERTIFICATE RE-KEY

USHER Subscribers may request a certificate with a new key if they suspect that the current key pair has been compromised or has become vulnerable to discovery. See also section 6.3.2.

When the USHER CA1 CA updates its private signature key and thus generates a new root certificate, the OA notifies all Subscribers that the Root Certificate has been re-keyed by direct contact (see Definitions) with the trusted Executive officer listed in each Agreement or the designated Administrator. A new CA1 root certificate is conveyed to Subscribers as described in Section 2.

4.7.1 Circumstance for Certificate Re-key

Re-key for all valid USHER certificates is performed upon request.

4.7.2 Who may request certification of a new public key

See section 3.3.1.1.

4.7.3 Processing certificate Re-keying requests

See section 4.3.1.

4.7.4 Notification of new certificate issuance to Subscriber

Same procedures as detailed under Section 4.3.2.

4.7.5 Conduct constituting acceptance of a Re-keyed certificate

Same procedures as detailed under Section 4.4.1.

4.7.6 Publication of the Re-keyed certificate by the CA

Same procedures as detailed under Section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other Entities

Same procedures as detailed under Section 4.4.3.

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 updated.

4.8.1 Circumstance for Certificate Modification

See section 4.8.

4.8.2 Who may request Certificate Modification

See section 3.3.1.1

4.8.3 Processing Certificate Modification Requests

See section 4.3.1.

4.8.4 Notification of new certificate issuance to Subscriber

Same procedures as detailed under Section 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

Same procedures as detailed under Section 4.4.1.

4.8.6 Publication of the modified certificate by the CA

Same procedures as detailed under Section 4.4.2

4.8.7 Notification of certificate issuance by the CA to other Entities

Same procedures as detailed under Section 4.4.3.

4.9 CERTIFICATE REVOCATION & SUSPENSION

USHER CA1 issues CRLs covering all unexpired certificates revoked under this policy and posts those CRLs to its online repository. Revocation requests must be authenticated by verifying that they are signed by the key associated with the certificate being asked to be revoked or that they originate from the Subscribers' trusted officers. Natural person or component end-entity certificate revocation may be requested by the subject or by the PA or the OA Manager.

4.9.1 Circumstances for Revocation

Subscribers may request certificate revocation at any time, for any reason. Special conditions are required for USHER PA-approved revocation: as outlined in the Agreement or if the USHER PA receives sufficient evidence of compromise, loss of, or loss of control of a Subscriber's private key. Failure of the Subscriber to verify the contents of its newly issued certificate within one

month's time also is grounds for revocation as stated in section 4.3.1. Termination of USHER CA1 also warrants revocation, per section 5.8.

For subordinate PKI domain CAs, the USHER OA may request revocation approval from the Chair of the USHER PA if an emergency has occurred that impacts the integrity of the USHER CA1 or subordinate CA.

4.9.2 Who Can Request Revocation

The certificate Subject or trusted officers of subscribing organizations may request revocation. The USHER PA and/or USHER PA Chair may also request revocation as outlined above. Only the USHER PA may direct the USHER OA to revoke the USHER CA1 root or any of its subordinate CA authority certificates.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate from a Subscriber must identify the certificate to be revoked and allow the request to be authenticated (digitally or manually). If a reason is provided and Subscriber requests that the reason be published in the CRL, the USHER CA1 CA will publish the reason upon revocation. The "hold" reason is not supported as a publishable reason.

Authentication of certificate revocation requests is performed by one of three methods:

- by verifying that the request was signed by the key associated with the certificate being asked to be revoked;
- by verifying that the request originated from one of the Subscriber's trusted officers (this may be done by direct telephone contact after an initial request is made);
- or by the trusted officer logging into an USHER interface with an USHER-issued credential.

If the revocation request is valid, the USHER OA revokes the certificate by placing its serial number and other identifying information on a published CRL.

Revocation of an USHER CA1 certificate is accomplished in accordance with Section 4.9.7 *CRL Issuance Frequency*. A certificate that is revoked remains in the published status information until the certificate expires and at least for one additional CRL beyond that point.

Further, and separate from the publication of the status information, prompt electronic notification is given by the USHER OA to all other USHER CA1 Subscribers by email distribution list.

4.9.4 Revocation Request Grace Period

N/A

4.9.5 Time within which CA must Process the Revocation Request

Authenticated revocation requests will be processed as soon as is practicable and before the next CRL is published. Revocation requests received and authenticated within two hours of CRL issuance are processed with the following CRL.

4.9.6 Revocation Checking Requirement for Relying Parties

No stipulation.

Practice note: Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

USHER CA1 issues CRLs at least every 31 days or as soon as is practicable after a revocation request is made, whichever is sooner. In all cases, new CRLs are posted on or prior to the "next publication date" in the current CRL. The penultimate CRL always is available as well. All older CRLs are removed from the repository.

4.9.8 Maximum Latency for CRLs

CRLs are published as soon as practicable after they are created.

4.9.9 On-line Revocation/Status Checking Availability

On-line revocation and/or status checking (OCSP) is not available at this time..

4.9.10 On-line Revocation Checking Requirements

N/A

4.9.11 Other Forms of Revocation Advertisements Available

N/A

4.9.12 Special Requirements Related To Key Compromise

In the event of a Subscriber's key compromise or loss, an updated CRL will be published at the earliest practicable time.

4.9.13 Circumstances for Suspension

Suspension shall not be used by USHER CA1.

4.9.14 Who can Request Suspension

N/A – see Section 4.9.13.

4.9.15 Procedure for Suspension Request

N/A – see Section 4.9.13.

4.9.16 Limits on Suspension Period

N/A – see Section 4.9.13.

4.10 CERTIFICATE STATUS SERVICES

No on-line certificate status services are offered at this time.

4.10.1 Operational Characteristics

N/A

4.10.2 Service Availability

N/A

4.10.3 Optional Features

N/A

4.11 END OF SUBSCRIPTION

See the Subscriber Agreement.

4.12 KEY ESCROW & RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Under no circumstances will USHER CA1's or a Subordinate CA's signature keys be escrowed by a third party. For information regarding back up of private keys, see section 5.1.8. For a definition of Key Escrow, see the Definitions. Cooperating PKI domain private keys are never in the possession of USHER.

Subscriber key management keys are permitted by the policy but are not escrowed at this time.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

N/A

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

CA equipment belonging to the USHER CA1 CA always is installed and activated in an offline mode (i.e., disconnected from any network). When not in use, the CA equipment is stored in a strong physical safe with dual access controls and restricted physical access. The CA equipment

consists of a dedicated laptop PC with networking disabled and with USB external storage capability for moving CSRs into the system and CRLs and certificates out of the system. The specific make and model of the dual-key safe, the locations of the safe deposit boxes and a list of their contents, as well as a list of all USHER-authorized personnel is contained in the USHER Operations Manual.

5.1.1 Site Location and Construction

The location of the USHER CA1 CA equipment is in a limited-access facility within the Internet2 Ann Arbor office which is monitored by surveillance cameras.

5.1.2 Physical Access

CA equipment is powered down and stored in a safe with dual access controls and restricted physical access. Removable cryptographic modules are inactivated prior to storage. CA equipment is used only within the controlled physical access space and may not be removed except for maintenance as defined below. A Log book is used to record each occurrence of CA equipment access.

Activation PIN data is either memorized or recorded and stored in a separate safe at a different location. Any physical keys are kept locked in a safe location unknown to the other officers responsible for maintaining the separation of duties. The safe is further secured in a facility with limited access privileges. Access logs are archived in an offsite safe deposit box.

5.1.2.1 CA Equipment Maintenance or Replacement

Should USHER CA equipment require maintenance, the following procedures will be undertaken:

- If repairs or maintenance involve hardware other than the hard drive, the hard drive will be removed and stored securely in the safe while repairs are being made.
- There will be no attempt to recover data from a failed hard drive
- If maintenance involves replacing the hard drive, a new hard drive will be installed, applications will be securely installed, and back up data will be restored. The retired hard disk will be permanently destroyed.

Software updates shall be performed by the Administrator and logged. Only original, vendor supplied, or USHER created software may be installed.

5.1.3 Power and Air Conditioning

The USHER CA1 CA is operated when required on a per session basis, using a laptop with a fully charged battery as back-up power. Air conditioning is sufficient for human activity.

5.1.4 Water Exposures

CA1 equipment is stored above the surrounding area's maximum water line. Floor drains are in place in the vicinity of any nearby water supply lines.

5.1.5 Fire Prevention and Protection

CA1 equipment is protected by applicable fire prevention building code compliance.

5.1.6 Media Storage

CA1 archive media is stored in an offsite safe deposit box. Back-up media is stored in the CA safe.

5.1.7 Waste Disposal

Sensitive information is shredded prior to disposal.

5.1.8 Off-site Backup

Signing keys and CA software are backed up and stored on USB tokens and/or CD ROMs and are kept separately in protected safes and/or bank safe deposit boxes. Specific locations are detailed in the USHER Operations Manual.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

For the USHER CA1 CA, at least two trusted operators are required to maintain separation of duties required for the security and integrity of the system. Each Cooperating PKI domain shall identify at least one individual responsible and accountable for the operation of each CA in that PKI domain as specified in section 4.1.1.

5.2.1.1 Administrator

The USHER administrator role is responsible for: installation, configuration, and maintenance of the CA; establishing and maintaining CA system accounts; configuring certificate profiles or templates and audit parameters; generating and backing up the CA; executing issuance of CRLs and certificates to Subscribers when authorized by an officer; generating logs; routine operation of the CA equipment; and operations such as system backups and recovery or changing archival recording media. The Administrator for USHER is assigned by the OA Manager.

5.2.1.2 Officer

The officer role is responsible for the issuance of certificates, that is: determining eligibility of new Subscribers; verifying the identity of Subscribers' trusted officers; verifying the accuracy of information included in certification requests; approving the issuance of certificates; requesting or approving the revocation of certificates; overseeing internal compliance audits to determine

whether the USHER CA is operating in accordance with its CPS; and archiving logs. The Officer for USHER is assigned by the OA Manager.

5.2.2 Number of Persons Required Per Task

Two or more persons are required for the following tasks:

- CA key generation
- CA signing key activation
- CA disaster recovery or key (re)generation

Logs are used to record the identities of those involved.

5.2.3 Identification and Authentication for Each Role

USHER personnel are verified by USHER as stated in section 3.2.3.1. Each trusted officer from Subscribing PKI domains is verified by the USHER RA as stated in section 3.2.3.1. For USHER OA operations, an individual manually logs his or her critical actions while performing the assigned role.

5.2.4 Roles Requiring Separation of Duties

No one individual will assume both the Officer and Administrator roles.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

Appointment of all persons filling Trusted Roles for the USHER Foundation Level CA are documented in writing. Background investigations, as outlined in Section 5.3.2, are administered for all individuals appointed to Trusted Roles under this CPS.

Appointments are made by the OA Manager, positively confirming the individual's qualification. The activation of the individual as a Trusted Role is considered complete when training has been completed and USHER systems have been configured to recognize that individual as authorized for that role.

No individual is placed into a trusted role for USHER CA1 critical operations or Disaster Recovery implementation procedures, other than by the above process.

5.3.2 Background Check Procedures

All personnel must be qualified as demonstrated by education and/or employment. In addition, personnel in trusted roles must not have any felony convictions within the last 20 years or any other criminal convictions within the last 10 years.

Applicants for Trusted Roles must submit the following investigative information to Internet2 Human Resources:

- Social Security Number
- Educational history
- Employment history
- Professional and personal references
- A signed statement agreeing to adhere to the Internet2 Personal Code of Conduct (found in the Internet2 Staff Handbook), which includes prohibiting: willful or negligent misuse, destruction, or damage of property; disregard of established procedures, policies, or standards; and the intentional transfer of information to unauthorized sources.
- A signed background information document, declaring all felony and misdemeanor convictions.

5.3.3 Training Requirements

The OA Manager assigns an appropriate individual to train each CA trusted operator in his/her role. Such training includes information appropriate to his/her role, including the following:

- CA/RA security principles and mechanisms
- Relevant stipulations of the USHER Foundation Level CP and this CPS
- Details of operating procedures and manuals appropriate to the trusted operator's role and duties
- Software versions in use on CA and RA systems
- Relevant disaster recovery and business continuity procedures

Additional detail about each item in this list may be provided during training, depending on the operators' role in the system. For example, System Administrators will receive more technical information about the PKI software than persons entrusted with Registration Authority duties.

5.3.4 Retraining Frequency and Requirements

Training is developed and delivered to all appropriate individuals before any new system is made operational or any significant change is made to CA or RA procedures, except for emergency changes to procedures made in response to a particular, recognized vulnerability. In this event, training will be delivered to each trusted operator individually before he or she is allowed to perform routinely the modified procedure.

5.3.5 Job Rotation Frequency and Sequence

N/A

5.3.6 Sanctions for Unauthorized Actions

Penalties for accidental violation of the Certificate Policy or Certification Practices Statement may result in disciplinary action up to and including termination of Trusted Role status.

Penalties for intentional violation of the Certificate Policy or this CPS by USHER Trusted Roles may result in additional sanctions by AIRE and/or Internet2 in consultation with the USHER PA.

5.3.7 Independent Contractor Requirements

Contractors and their subcontractors, if any, fulfilling trusted roles are subject to personnel requirements compatible with those stipulated in these procedures.

Contractors, including vendors, who provide any services must establish procedures to ensure that they and any subcontractors comply with the USHER Foundation Level CP and this CPS wherever appropriate.

PKI identity certificates that are issued to contractors or any third party personnel in order to perform their duties for USHER are revoked as soon as practicable upon termination of the contract or their assignment to those duties.

5.3.8 Documentation Supplied to Personnel

The USHER OA makes available to the CA personnel the certificate policies it supports, relevant parts of the CPS, and any relevant operational procedure documentation, statutes, policies and contracts.

5.4 AUDIT LOGGING PROCEDURES

The USHER CA1 CA platform currently does not support system-integrated automatic logging. Instead, USHER CA1 actions are recorded in a physical log book in ink. Any changes or additions to a log entry are noted as addenda to the appropriate log entry.

Registration Authority procedures verifying applicant organizations and their trusted officers are logged both on paper and in a securely restricted digital file. RA process papers are filed in a locked, fire-proof cabinet. Digital log files are printed once per month, signed, and archived in the CA1 safe. Older paper logs are archived offsite in a bank safe deposit box.

Logs defined in this section shall be maintained in accordance with Section 5.5.2 *Retention period for archive*.

5.4.1 Types of Events Recorded

At a minimum, system logs are kept for USHER Foundation Level CA operating systems. Logs also are kept for:

- Physical access to the CA

- Certificate life cycle events, specifically certificate signing, re-key, renewal, and modification; and issuance of certificate revocation lists
- Configuration changes to the CA system, including software upgrades
- Unexpected events
- Events that affect the security of the system
- Events that may require a change in operational procedures
- Registration authority events that qualify the applying organization for eligibility of subscription to USHER services
- Registration authority events that establish contact with Subscribers' trusted officers and verify their personal data

5.4.2 Frequency of Processing Log

The OA Manager or an appointed individual performs audits and detailed log reviews only when required for cause.

5.4.3 Retention Period for Audit Log

Logs are retained onsite for at least two months as well as being retained in the manner described below. The individual who removes audit logs from the USHER CA1 CA system is an official different from any individual who performs the Administrator role.

5.4.4 Protection of Audit Log

The following steps are taken to protect audit logs from inappropriate access or modification:

- Physical logbooks (with bound and numbered pages) are protected from inappropriate access by maintaining them in the dual-key safe, available only to authorized operators or the auditor;
- Electronic RA logs are protected by file access controls and are printed, reviewed, and signed regularly.

Audit data shall be placed into tamper-evident containers located at a secure, offsite storage location every quarter.

5.4.5 Audit Log Backup Procedures

Logs are stored on-site and archived off-site in accordance with sections 5.4.3 and 5.4.4 above.

5.4.6 Audit Collection System (Internal vs. External)

USHER CA1 archive records shall be sufficiently detailed to establish the proper operation of USHER Foundation Level CAs or the validity of any certificate (including those revoked or expired) issued by the USHER CA1 CA..

5.4.7 Notification to Event-Causing Subject

No requirement.

5.4.8 Vulnerability Assessments

The Operational Authority Manager performs annual self assessments of security controls. Any issues of concern are brought to the attention of the PA.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

Archives are made of audit logs and will contain the same events as those listed in Section 5.4.1.

5.5.2 Retention Period for Archive

Archive records are kept for a minimum of five (5) years. Provisions will be made to transfer records to new media as appropriate, and to ensure that software required to read the records is available for as long as the records are maintained.

5.5.3 Protection of Archive

The USHER OA maintains an offsite records archive containing copies of all physical log books and digitally archived data (redundant media) for the required retention period.

Archived media and log books are transferred by the Officer and placed into the permanent archive location. This archive storage location is a bank safe deposit box.

The archiving Officer adds each item to the archive manifest, logs the date and time of receipt, and signs the manifest. The archive manifest is stored within the secure location. Any item removed from the archive must be signed out in a similar manner.

No original or archived version of a log or system record will be released to a third party, unless required by law. For copies of items released to a third-party auditor or governmental authority, the OA Officer confirms and documents the identity of the individual taking possession of the material. The receiving individual must provide their signature on a written receipt to confirm their receipt of the material. Archive items removed for copying, audit, or inspection are returned and logged into the archive by the OA Officer immediately upon completion of the activity.

5.5.4 Archive Backup Procedures

N/A.

5.5.5 Requirements for Time-Stamping of Records

N/A.

5.5.6 Archive Collection System (Internal or External)

N/A.

5.5.7 Procedures to Obtain and Verify Archive Information

N/A.

5.6 KEY CHANGEOVER

The USHER CA1 root certificate has a validity period of 20 years and an operational life of approximately ten years, with final determination resting with the USHER PA. When a root certificate key changeover is scheduled, all subordinate and cooperating CAs will be notified in advance. Each will be issued a new authority certificate signed by the new USHER root private key. The old root and CA authority certificates will remain valid until their defined expiration date or a key compromise if it occurs. All new USHER-issued certificates will be signed by the new root's private key.

5.7 COMPROMISE & DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

Review of audit logs and any other available means are used to determine if any incidents have taken place. In the event of a compromise, the OA will reestablish operational capabilities as quickly as possible by use of stored back-ups and disaster recovery procedures. The USHER PA will be notified of incidences as specified in section 5.7.1 of the USHER Foundation Level Class of Certification Authorities CP.

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

If USHER CA1 equipment is damaged or rendered inoperative but the signature keys are not destroyed, the CA operation will be reestablished as quickly as possible, giving priority to the ability to generate certificate status information.

5.7.3 Entity Private Key Compromise Procedures

If USHER CA1 signature keys are compromised or lost (such that compromise is possible even if not certain): the USHER PA and all Cooperating PKI domains will be notified via direct contact and at the earliest feasible time; a new CA1 key pair will be generated in accordance

with procedures set forth in section 6.1.1.1 of this CPS; and new CA authority certificates will be issued to Subscribers. The USHER OA also will investigate and report to the USHER PA the cause of the compromise or loss and the measures taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a complete disaster whereby an USHER Foundation Level CA installation is physically damaged and all copies of the signature key are destroyed as a result, the USHER PA and all of its Subscriber PKI domains will be notified at the earliest feasible time, and the USHER PA shall take whatever action it deems appropriate, including but not limited to reestablishing the USHER CA1 CA equipment, generating new keys and a root certificate, and re-issuing all Subscriber certificates.

The USHER CA1 CA repository servers are mirrored so as to remain operational in the event of a physical disaster at any single USHER CA site.

5.8 CA OR RA TERMINATION

As soon as possible and no later than 90 days prior cessation of services, the CA will advise all other organizations to which it has issued certificates of its termination by posting a notice in its repository and by direct contact with each trusted officer at the Subscribing CA sites. Before cessation of services, all certificates will be revoked.

Practice Note: This section does not apply if the CA1 CA has ceased issuing new certificates but continues to issue CRLs until all certificates have expired. Such actions require the CA to continue to conform to all relevant aspects of this CPS (e.g., audit logging and archives).

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION & INSTALLATION

6.1.1 Key Pair Generation and Installation

6.1.1.1 CA1 Root Key Pair Generation

The USHER CA1 CA key generation process is scripted and was submitted for approval by the USHER PA. The script ensures that full key material is never in the control of a sole entity, and that 2048 bit keys are generated in a secure manner. The actual procedure itself generates auditable evidence to confirm that the documented procedures were followed.

6.1.1.2 Subscriber Key Pair Generation

Subscribers generate their own key pairs.

6.1.2 Private Key Delivery to Subscriber

N/A

6.1.3 Public Key Delivery to Certificate Issuer

Certificate issuance is based on a PKCS#10 certificate signing request (CSR) from the requester using USHER-issued credentials.

6.1.4 CA Public Key Delivery to Relying Parties

USHER CA1 publishes a public repository of all valid Subscriber certificates.

6.1.5 Key Sizes

Authority certificates issued to Subordinate PKI Domains will use at least 2048 bit RSA (or better) cipher keys. USHER CA1 CA will sign certificate requests from Cooperating PKI domains that contain 2048 bit RSA keys for authority certificates with up to 20 year validity periods. 1024 bit key CSRs also may be signed upon special approval from the USHER Policy Authority but will have a shorter, 10-year validity period. Keys for natural person or component PKI certificates will be 1024 bits or better.

6.1.6 Public Key Parameters Generation and Quality Checking

For USHER generated keys, parameter quality checking (including primarily testing for prime numbers) is performed in accordance with FIPS 186.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

CA public keys are certified for the following uses: Certificate Signing(5), CRL Signing(06). USHER natural person certificates include key usage for encryption and signature in support of Secure Multipurpose Internet Mail Extensions (S/MIME) and other applications, and key encipherment.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards & Controls

The USHER CA1 CA private key is protected by storing it in an Aladdin eToken or similar FIPS 140 rated security module. The private key is generated in a secure manner in software and imported into the module for ordinary use. To facilitate secure procedures for a change in vendor hardware security modules (HSM) if required, the software-based key is then split based on a secret sharing scheme and the fragments are appropriately dispersed to safe locations.

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

Use of an USHER CA1 CA private signing key requires two operators from distinct roles as set forth in Section 5.2 of this CPS. Each operator holds a separate key granting its share of access to the dual-key safe.

6.2.3 Private Key Escrow

The USHER CA1 CA signature keys are not escrowed by third parties.

The USHER CA1 CA does not perform any key escrow functions for Cooperating PKI domain CAs.

6.2.4 Private Key Backup

6.2.4.1 Backup of USHER CA and PKI Domain CA Private Signature Key

The USHER CA1 CA private signature keys are backed-up under multi-person controls. A single copy of the signature key is stored at the USHER CA1 CA location; additional copies are kept at USHER CA1 CA backup locations.

Additional backup for USHER CA1 CA private signature keys is performed by splitting the private key into five shares. The five shares are each dispersed and entrusted to a safe location within the USHER community (as detailed in the USHER Operations Manual). Any three of the five shares are needed to reassemble the private key in case of disaster or a change of token vendor.

6.2.4.2 Backup of Subject Private Signature Key

N/A

6.2.5 Private Key Archival

USHER CA1 private signature keys are not escrowed or archived. The CA private keys may be backed up in accordance with Section 6.2.4.1.

6.2.6 Private Key Transfer into or from a Cryptographic Module

USHER CA1 CA private keys are generated securely, imported into, and remain in a cryptographic module using vendor supplied software for that module. Once installed, the key can not be extracted from the module.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS-140.

6.2.8 Method of Activating Private Key

The relevant USHER administrator must be authenticated to the cryptographic module via use of the cryptographic module passphrase before the activation of any private key(s). The interface used to enter the passphrase does not disclose its contents to any observers.

6.2.9 Method of Deactivating Private Key

Cryptographic modules used to store USHER Foundation Level CA private keys are deactivated after each use by removing the module from the laptop. The cryptographic module is stored in the safe when not in use.

6.2.10 Method of Destroying Private Key

For USHER CA1 CA private keys – which are on hardware cryptographic modules – destruction will be accomplished by executing a "zeroize" command in software on the device. If no such command is provided, the module will be destroyed with a hammer. All backup copies will be destroyed with the hammer or if on CD otherwise snapped into small pieces by hand.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

Certificates are archived by the online repository for at least 6 months beyond their expiration.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

USHER CA1 CA root and subordinate certificates are issued with validity periods up to 20 years; however, Cooperating PKI domain CA certificates are issued with validity periods of less than 20 years and never more than the remaining validity period of the USHER signing key. The PA also will consider recommendations in NIST SP800-78 (or successor) for appropriate key usage periods.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation & Installation

USHER CA1 CA private keys are stored on a cryptographic module that requires a passphrase to be entered before the keys can be accessed and used.

6.4.2 Activation Data Protection

The passphrase used to unlock private keys is memorized. As a back up, it also is recorded and stored in a separate, secure location. Only OA-authorized personnel have access to this location.

6.4.3 Other Aspects of Activation Data

N/A

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the CA1 CA operating system or procedures, and physical safeguards:

- Require authenticated logins for USHER OA Administrators' CA access
- Provide Discretionary Access Control
- Provide a security audit capability through log records
- Restrict access control to USHER services by the adherence to distinct trusted roles
- Enforce separation of duties for trusted roles
- Require identification and authentication of trusted officers
- Prohibit object re-use or require separation for USHER CA1 CA random access memory
- Archive USHER Foundation Level CA history and audit data
- Require a trusted path for identification of Subscriber trusted officers and associated identity credentials
- Use of minimum system access controls to ensure integrity of critical CA processes.

While the CA1 platform as such has not been evaluated for computer security assurance compliance, the components are maintained in a highly secure environment with procedural controls and methods ensuring CA1 security requirements.

6.5.2 Computer Security Rating

N/A

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

N/A

6.6.2 Security Management Controls

All configuration, modifications and upgrades of the CA system are documented and controlled. The CA verifies at least annually the integrity of the software by a process such as making a check sum of the application directory after initialization and confirming that it has not been modified at subsequent verifications (e.g., multiple hash functions are used to ensure any tampering attempts are identified). The USHER CA1 CA is operated offline and only used for purposes approved by the USHER PA.

6.6.3 Life Cycle Security Controls

N/A

6.7 NETWORK SECURITY CONTROLS

CA signing equipment is never connected to a live network. Certificates, CRLs, or other PKI-related data from the CA required to be posted to an online repository are transferred using portable media.

The USHER CA1 CA Repository is connected to the Internet and provides continuous service (except, when necessary, for brief periods of maintenance or backup) but protected via the same network security controls imposed on Internet2 public websites.

6.8 TIME-STAMPING

Asserted times will be accurate to within three minutes of standard time. Upon boot of the off-line CA system, the operator will check the clock of the laptop against a device known to have synchronized recently with NIST or other commonly trusted time authority and make adjustments if necessary.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version Numbers

The USHER CA1 CA issues X.509 v3 certificates (the version field contains integer "2").

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of X.509 extensions are defined in the USHER certificate profiles found at:

http://www.usherca.org/profiles/

7.1.3 Algorithm Object Identifiers

Certificates issued under this CPS include the following OID for signatures:

Object Name	Object Identifier
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

Certificates under this CPS include the following OID for identifying the algorithm for which the subject key was generated:

Object Name	Object Identifier
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name Forms

The subject and issuer fields of the base certificate are populated with an X.500 Distinguished Name, with the attribute type further constrained by [RFC3647] as detailed in the profile.

7.1.5 Name Constraints

N/A

7.1.6 Certificate Policy Object Identifier

All certificates issued by the USHER CA1 CA to Subscribing CAs include a Policy OID as described in section 1.2 of the USHER Foundation Level CP. Natural person, component, and subordinate PKI Domain CA certificates will contain the USHER Foundation Level CP OID. USHER CA1 CA certificates issued to Cooperating PKI domains will include the X.509 “anyPolicy” CP OID.

7.1.7 Usage of Policy Constraints extension

N/A

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by USHER CA1 contain a CPS Pointer pointing to an on-line copy of a possibly-redacted public version of this CPS at the following address:

http://www.usherca.org/practices/ca1/cps.pdf

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

N/A

7.1.10 Certificate Serial Numbers

The USHER CA system ensures a serial number is provided for all certificates issued by the CA and increments it after the issuance of each certificate. The CA administrator will ensure that no serial number shall be reused even if an otherwise identical certificate is issued.

7.1.11 Information Access fields

Certificates issued by an USHER CA include one or more URIs in the Authority Information Access (AIA) field as defined in the certificate profile document – see Section 7.1.2. These URI(s) enable a Relying Party to retrieve all authority certificates issued to the USHER CA, whether by another USHER CA or an external CA.

Natural person or component Certificates issued by an USHER CA also may include one or more URIs in the Subject Information Access (SIA) field that enable a Relying Party to retrieve further information about the certificate Subject.

Note: Certificates issued by the USHER CA1 CA also can be found in a public repository, which can be located by visiting: http://www.usherca.org

7.2 CRL PROFILE

7.2.1 Version Number(s)

USHER CA1 issues X.509 version two (2) CRLs.

7.2.2 CRL and CRL Entry Extensions

Field	Name	Value	Notes
1	version	2 (0x1)	We are using the version 2 CRL profile
2	signature	SHA1/RSA	
3	Issuer		The Subject value of the USHER Root
4	thisUpdate	Current DateTime	
5	nextUpdate	thisDate + 30 days	
6	Authority Key Identifier	key identifier	This is in the CRL extensions field
7	List of revoked certificates		
		Serial Number	The certificate's serial number
		revocationDate	The day/time that the certificate was revoked
		revocationReason	We must publish a revocation reason if the site has requested us to do so. We will not accept a Certificate Hold reason but will publish any other reason defined in RFC 3280 Section 5.3.1.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

N/A at this time.

7.3.2 OCSP Extensions

N/A at this time.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The USHER OA will cooperate with the PA when it requests periodic verification that the operations of USHER CA1 are in compliance with its CP, CPS, and the provisions of any Agreements.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

N/A

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The assessor will be familiar with the USHER Operation Document, this CPS, and corresponding CP and will, if requested by the USHER PA, be approved by the USHER PA.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The assessor shall be sufficiently organizationally separated from USHER trusted operators to provide an unbiased, independent evaluation.

8.4 TOPICS COVERED BY ASSESSMENT

The assessor will take advice from the PA or other requesting authority on what elements will be assessed during any audit.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The USHER OA will cease operation of CA1 if directed by the USHER PA when the latter determines that it is not complying with its obligations set forth in the CP, this CPS, or any respective Subscriber Agreement. The USHER OA will also comply with other corrective actions the PA recommends to prevent interoperation as soon as is possible.

8.6 COMMUNICATION OF RESULTS

The USHER OA or independent Assessor will produce an Audit Compliance Report identifying corrective measures taken in the case of any deficiencies identified as a result of an audit. The results of this audit will be communicated to the USHER PA as soon as is practicable.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

Fees for Registration Authority services and for annual subscription to USHER are published on the USHER website: http://www.usherca.org/fees.html.

9.1.1 Certificate Issuance or Renewal Fees

N/A. Issuance is part of the USHER service subscription.

9.1.2 Certificate Access Fees

None.

9.1.3 Revocation or Status Information Access Fees

None.

9.1.4 Fees for Other Services

N/A

9.1.5 Refund Policy

N/A

9.2 FINANCIAL RESPONSIBILITY

USHER does not declare anything in this regard. Responsibilities of subscribers are defined in the Subscriber Agreement.

9.2.1 Insurance Coverage

NA

9.2.2 Other Assets

N/A

9.2.3 Insurance or Warranty Coverage for End-Entities

N/A

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

USHER security principles are founded on open practices and confidentiality protections for individuals and devices. While USHER practices are open to the community, certain records are

maintained as confidential to safeguard specific individuals, devices, passphrases, and their locations, contact information, or methods of access. This data will not be revealed to external parties.

9.3.2 Information not within the scope of Confidential Information

Certificates and CRLs issued by USHER are not subject to confidentiality requirements.

9.3.3 Responsibility to Protect Confidential Information

USHER will make all reasonable efforts to protect confidential information but it can not guarantee confidentiality.

9.4 PRIVACY OF PERSONAL INFORMATION

The USHER Operational Authority collects and manages personally identifiable information which it uses to operate the USHER service but does not share it with external parties without prior authorization.

9.4.1 Privacy Plan

All USHER CA1 activities will comply with Internet2's RA privacy policy, available at: http://www.internet2.edu/policies/RA-Privacy.html.

9.4.2 Information treated as Private

Personally identifiable information gathered for the purpose of operating any USHER service which is specifically requested as private by the person in question shall neither be shared nor used outside of USHER record systems.

9.4.3 Information not deemed Private

Information included in certificates is considered public.

9.4.4 Responsibility to Protect Private Information

The USHER OA will take care to ensure that all personally identifiable information is stored securely, and released only in accordance with other stipulations in Section 9.4.

9.4.5 Notice and Consent to use Private Information

Information designated as private (9.4.2) will not be released to third parties without the consent of the information owner. Other information not so designated may be shared as needed to operate the USHER Operational Authority.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The USHER Operational Authority will cooperate with requests for private information as required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

None.

9.5 INTELLECTUAL PROPERTY RIGHTS

See the copyright notice on the cover page of this CPS document and any relevant provisions in the Agreement.

9.6 REPRESENTATIONS & WARRANTIES

The USHER Operating Authority operates and shall continue to operate the USHER CA1 CA in accordance with this CPS.

9.6.1 CA Representations and Warranties

The Agreement is authoritative for all USHER CA1 CA warranties.

9.6.2 RA Representations and Warranties

USHER RA warranties are subsumed under Section 9.6.1 above.

9.6.3 Subscriber Representations and Warranties

Subscribers must use CA1-issued certificates in accordance with the Agreement signed by the Subscribing organization and the USHER Expected Practices.

9.6.4 Relying Parties Representations and Warranties

Each Relying Party decides, pursuant to its own policies, what reliance to make on USHER services or certificates. The USHER CA1 CA merely provides the ability to perform trust path discovery and validation among its issued certificates.

9.6.5 Representations and Warranties of other Participants

N/A

9.7 DISCLAIMERS OF WARRANTIES

Any USHER warranties and disclaimers are stated in the USHER Subscriber Agreement. With respect to relying parties, USHER makes no warranty about its certificates regarding fitness for any purpose, accuracy, or reliability.

9.8 LIMITATIONS OF LIABILITY

The USHER Subscriber Agreement is authoritative on Liability provisions.

9.9 INDEMNITIES

N/A

9.10 TERM & TERMINATION

9.10.1 Term

This CPS is effective and becomes the official USHER CA1 CPS on the date signed by the Chair of the USHER Policy Authority (see the Signature Page). This CPS has no specified term.

9.10.2 Termination

Termination of this CPS is at the discretion of the USHER Policy Authority.

9.10.3 Effect of Termination and Survival

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

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

No stipulation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The USHER PA may review this CPS periodically. Errors, updates, or changes to this CPS that materially change the assurance that the implementation of this CPS otherwise provides shall be communicated to USHER Subscribers as soon after approval of the amendments as is possible.

9.12.2 Notification Mechanism and Period

This CPS and any subsequent changes shall be made publicly available, possibly in a redacted version of the original, within one week of approval. Any prior public version of this CPS shall remain available for at least 6 months after the expiration date of the last certificate referencing it.

9.12.3 Circumstances under which OID must be changed

Minor changes to this document that materially affect the level of operational assurance will be indicated by a suffix on the original CPS OID. Major changes will require a new CPS OID. The USHER PA will decide which applies in each case.

9.13 DISPUTE RESOLUTION PROVISIONS

N/A

9.14 GOVERNING LAW

The terms and provisions of this CPS shall be interpreted under and governed by applicable laws of the United States or its several states.

9.15 COMPLIANCE WITH APPLICABLE LAW

The USHER OA will comply with applicable law when operating the USHER CA1 CA.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

This CPS does not constitute an Agreement with any Party. The USHER Agreement defines the agreement between USHER and USHER Subscribers.

9.16.2 Assignment

N/A

9.16.3 Severability

Should it be determined that one section of this CPS is incorrect or invalid, the other sections of this CPS shall remain in effect until the CPS is updated. The process for updating this CPS is described in section 9.12. See also the USHER Subscriber Agreement.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

See Section 9.8.

9.16.5 Force Majeure

N/A

9.17 OTHER PROVISIONS

9.17.1 USHER Business Information

9.17.1.1 Postal Address

USHER
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor, MI 48104

9.17.1.2 Email Address

usher-admin@internet2.edu

9.17.1.3 Website Address

http://www.usherca.org

9.17.1.4 Phone Numbers

Office: 734.913.4250
Fax: 734.913.4255

10. BIBLIOGRAPHY

The following documents were used in part to develop this CPS:

ABADSG	Digital Signature Guidelines, 1996-08-01. http://www.abanet.org/scitech/ec/isc/dsgfree.html.
FIPS 112	Password Usage, 1985-05-30 http://csrs.nist.gov/fips/
FIPS 140-1	Security Requirements for Cryptographic Modules, 1994-01 http://csrs.nist.gov/fips/fips1401.htm
FIPS 186	Digital Signature Standard, 1994-05-19 http://csrs.nist.gov/fips/fips186.pdf
FOIACT	5 U.S.C. 552, Freedom of Information Act. Http://www4.law.cornell.edu/uscode/5/552.html
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997. ftp://ftp.bull.com/pub/OSIdirectory/ITU/97x509final.doc
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996. Http://www4.law.cornell.edu/uscode/40/1452.html
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. Http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt (redacted version)
NIST SP 800-78	Special Publication 800-78: Cryptographic Algorithms and Key Sizes for Personal Identity Verification
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.
PKCS#12	Personal Information Exchange Syntax Standard, April 1997. Http://www.rsa.com/rsalabs/pubs/PKCS/html/pkcs-12.html
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 3280 Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Housely, Polk, Ford, and Solo, April 2002

RFC 3647 Certificate Policy and Certificate Practices Framework, Chokhani, Ford, Sabett, Godward, Merrill, and Wu, November 2003.

Security Requirements for Certificate Issuing and Management Components, 3 November 1999, Draft

Digital Signatures, W. Ford

United States Department of Defense X.509 Certificate Policy, Version 5.0, 13 December 1999

11. ACKNOWLEDGEMENTS

This Certification Practice Statement was originally created by Scott Rea (Dartmouth). This CPS was edited to its final form by John Krienke (Internet2), IJ Kim (Internet2), and the founding members of the USHER PA: Jim Jokl, Chair (UVA); Michael Gettes (Internet2); Mark Luker (EDUCAUSE); Barry Ribbeck (Rice); Jeff Schiller (MIT); Renee Shuey (Penn State); and David Wasley (ret., UCOP).