X.509 Certificate Policy

For

U.S. Higher Education Root (USHER)

Foundation Level Class of

Certification Authorities

1 June 2007

Version 1.0.1

Signature Page

A copy of this document shall be available on-line at a location specified in any Certification Practices Statement (CPS) referencing this Certificate Policy. Certificates issued under this policy must include a URI pointing to an on-line repository for the applicable CPS.

This Certificate Policy (CP) has been developed by the U.S. Higher Education Root (USHER) Policy Authority (USHER PA). It becomes the official USHER Foundation Level CP when signed by the Chair of the USHER Policy Authority.

The global Object Identifier (OID) for this document is { 1.3.6.1.4.1.24726.1.1 }. See section 1.2 for this and other OID assignments defined under this Certificate Policy.

James A Jokl

Jim Jokl, Chair of the USHER Policy Authority

JUNE 1, 2007

Date

Revision History

Document Date	Revision Details

Table of Contents

1. INTRODUCTION

This Certificate Policy (CP) defines the procedural and operational requirements for U.S. Higher Education Root (USHER) Foundation level Certification Authorities (CAs) in support of interoperability among cooperating and subordinate Public Key Infrastructure (PKI) domains. USHER Foundation Level CAs are governed by a Policy Authority (USHER PA) that determines how the strictures in this Certificate Policy shall be implemented and under what conditions certificates may be issued to Subscribers (cooperating PKI domains, individual persons, or other end entities). Subordinate PKI domains are defined in this CP as administrative CAs under the purview of the USHER PA and which must abide by this CP. Cooperating PKI domains are defined in this CP as PKI domains which 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. USHER is defined to mean the USHER PA or other delegated authority, such as the USHER Operational Authority (OA), Registration Authority (RA), business office, or other entity representing USHER services. USHER Foundation Level CA authority certificates issued to PKI domains indicate that the named PKI domain is considered to be eligible for inclusion in the USHER Foundation Level (the most fundamental level of assurance) community of members. Cooperating PKI domains at this Foundation level are encouraged to publish their CP and/or Certification Practice Statement (CPS) since USHER provides no oversight to subscribing CAs at this level of assurance, and relying parties must make their own determination of trustworthiness. USHER Foundation Level CAs do not add to and should not subtract from trust relationships established by other means between transacting parties.

USHER Foundation Level CAs are intended to facilitate appropriate interoperability between parties within the USHER community and with parties in other PKI domains recognized by the USHER PA. This CP only describes USHER Foundation Level CAs operated by USHER at the foundation assurance level. The word “assurance” used in this CP refers to how well a Relying Party can be certain of the identity binding between the certificate public key and the individual or entity referenced in a subject name in the certificate. It also reflects the level of security of the system used to produce the key pairs and x.509 certificate and how well the Relying Party can be certain that the subject of the certificate is in sole control of the private key that is associated with the public key in the certificate.

PKI domains cross-certified by USHER but not managed nor audited by the USHER PA are not required to conform to the strictures of this CP. Instead, they are required to execute an USHER Subscriber Agreement and abide by the USHER Expected Practices that define their responsibilities with respect to the use of USHER CA certificates. The CA certificate issued to such a domain will include the ITU-T X.509 standard “anyPolicy” CP OID to indicate this fact. However, such a PKI domain may request mapping of the USHER CP to its CP as described herein in which case an appropriate USHER CP OID will be included in its CA certificate. Any use of or reliance on a reference to this USHER CP, on certificates produced pursuant to this CP, or by CAs associated with USHER but outside the purview of the USHER PA is undertaken completely at the Relying Party’s risk. **THE USHER PA ASSUMES NO LIABILITY FOR ANY CP OR LEVEL OF ASSURANCE ASSERTED BY A CA NOT MANAGED BY USHER.**

This USHER CP 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 Certificate Policy

USHER certificates contain a registered Certificate Policy object identifier (OID), which may be used by a Relying Party to help decide whether the certificate might be trusted for a particular purpose. OIDs other than X.509 standard OIDs are registered by the USHER PA which also publishes the CP for examination by Relying Parties. Any certificate also may include whatever other information is determined by the USHER PA or USHER Operational Authority (OA) (described in section 1.3.1.3) to be necessary for transitive trust determinations or interoperability.

1.1.2 Relationship Between the CP and the CPS

This CP states what assurance can be placed in a certificate issued by USHER Foundation Level CAs. A corresponding USHER Foundation Level CPS states how the USHER PA and OA establish that assurance for a particular CA.

1.1.3 Relationship Between the CP and a Subordinate PKI Domain CP

Subordinate PKI Domains may be established from time to time by the USHER OA by direction of the USHER PA and will conform to this same CP. Subordinate PKI Domain CA certificates will contain the USHER Foundation CP OID.

1.1.4 Relationship Between the CP and a Cooperating PKI domain CP

USHER does not require that there be a relationship between its CP and that of a Cooperating PKI domain. However, if so requested by the Cooperating domain PA, the levels of assurance of the certificates issued under an USHER Foundation Level CP may be mapped by the USHER PA, if possible, to the levels of assurance of the certificates issued by the Cooperating PKI domain CA as defined by their CP and CPS and verified by the USHER PA. If mapping is successful, the appropriate USHER Foundation CP OID and policy mapping(s) information is placed into the CA certificate issued to the Cooperating domain by an USHER Foundation Level CA to facilitate interoperability. When no mapping is requested or determined, the USHER Foundation Level CA certificate issued to the Cooperating PKI domain will include the "anyPolicy" CP OID and no mapping information will be present.

1.1.5 Scope of Services

USHER exists to facilitate electronic transactions among organizations within the Higher Education community. For this purpose, the USHER PA may choose to instantiate one or more CAs providing certification for cooperating CAs operated by other entities. USHER may choose to cross-certify with other Higher Education root and/or bridge CAs.

1.1.6 Definition of Terms used in this CP

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

The generic term “entity” applies equally to Higher Education institutions and other organizations owning or operating PKI domains, as well as individual Subscribers to an USHER Foundation Level CA.

PKI domain refers to the set of PKI CAs that operate under a common PKI CP. PKI domain CA may refer to a Higher Education institution’s or collective’s PKI, a PKI provided by a commercial service, a business partner's or other sponsored partner's PKI, or a bridge CA serving a community of interest to USHER members.

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. All PKI Domain Subscribers to USHER Foundation Level CAs are considered Cooperating PKI domains as defined in this CP.

Other terms are defined in Section 1.6.

1.1.7 Interoperation with CAs External to Higher Education

To facilitate the missions of subscribing institutions of higher education, USHER services also may be offered to non-higher-education entities under terms and conditions determined by the USHER PA.

1.2 IDENTIFICATION

This policy defines one fundamental level of assurance (LOA) that is reserved for use in CA certificates issued under this CP. The USHER Foundation LOA Object Identifier (OID) will be asserted in the certificate policy extension and possibly in policy mapping extensions of certificates issued by USHER Foundation Level CAs to Subordinate CAs. The OIDs are registered under the Internet Assigned Numbers Authority (IANA) arc as follows:

OID Name or Arc	OID Specification
id-usher arc	::= { 1.3.6.1.4.1.24726 }
id-usher-cp arc	::= { id-usher 1 }
id-usher-cp-LOA arc	::= { id-usher 2 }
id-usher-cp-LOA-FoundationAssurance	::= { id-usher-cp-LOA 2 }
-ITU-T X.509 anyPolicy	::= { joint-iso-ccitt(2) ds(5) 29 32 0 }
This USHER Foundation CP document identifier	::= { id-usher-cp 1 }
id-usher-cps arc	::= { id-usher 3 }
id-usher-cps-ca1	::= {id-usher-cps 1}

Subsequent major revisions of this Certificate Policy shall have new OID assignments under the id-usher-cp-LOA arc.

1.3 PKI PARTICIPANTS

The community served by USHER is primarily U.S. Higher Education PKI domains that wish to interoperate with other PKI domains known to USHER. Entities that are not U.S. Higher Education organizations may also participate in USHER if sponsored by a U.S. Higher Education organization and approved by the USHER PA. The applicability of services or certificates offered by USHER is not constrained by this CP. However, Relying Parties are advised to review section 1.3.5 carefully before making a decision to place trust in a certification path containing a certificate issued by USHER Foundation Level CAs.

The following are authorities relevant to the administration and operation of USHER Foundation Level CAs.

1.3.1 PKI Authorities

1.3.1.1 Internet2 and AIRE

Internet2 (http://www.internet2.edu) is a not-for-profit membership organization that initiates and oversees technology-based programs on behalf of Higher Education and other institutional members. The Advanced Infrastructure for Research and Education (AIRE) is a single-member LLC created by Internet2 to support advanced infrastructure services. USHER is an activity initiated under the auspices of the AIRE LLC.

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. Thus, the term “Agreement” as used in this CP shall always refer to the Subscriber Agreement cited in this paragraph.

1.3.1.2 Policy Authority

The USHER Policy Authority (PA) is instantiated under the authority of and with the approval of AIRE and Internet2. The USHER PA is an appointed governing body representing the interests of subscribing PKI domains. The Policy Authority is responsible for:

- This and any USHER CP;
- Any USHER Certification Practice Statements;
- Overseeing the operation of the USHER Operational Authority;
- Defining eligibility criteria for PKI domains desiring to interoperate by means of an USHER CA;
- Certifying policy mapping, path length and/or name constraints, if any (which determination will include objective and subjective evaluation of the facts deemed relevant by the USHER Policy Authority); and
- After a PKI domain is issued a certificate by an USHER Foundation Level CA, requiring continued conformance by that PKI domain to the requirements in the Agreement and the Expected Practices as a condition for allowing continued use of any PKI certificate issued to that entity by USHER.

1.3.1.3 Operational Authority (OA)

The USHER Operational Authority (OA) is the organization that is responsible for the CA infrastructure and issuance of USHER certificates as so directed by the USHER PA, the posting and distribution of those certificates and any Certificate Revocation Lists (CRLs) into a corresponding CA repository, and maintaining the continued availability of the repository to all parties relying on its certificates. Specific responsibilities of the USHER OA include:

- Day to day operation and maintenance of USHER CAs, repositories, and technical components;
- Overseeing the registration process (see also USHER RA below) including applicant identification and authentication;
- Complying with all requirements and representations of this CP; and
- Other activities as assigned by the USHER PA.

1.3.1.4 PKI Domain Principal Certification Authority (Principal CA)

The PKI domain Principal CA is an entity within a PKI domain that has been designated by the PKI domain’s Policy Authority (PA) (or equivalent duly authorized entity) to be certified directly by USHER (e.g., through the issuance of a CA authority certificate), and which in turn may issue end-entity certificates to Subjects, certificates to other PKI domain CAs, cross-certificates to external party CAs, and/or revocation lists pertaining to these types of certificates. It should be noted that a PKI domain PA may request that USHER certify more than one CA within its domain; that is, a PKI domain may have more than one Principal CA. Additionally,

this CP may refer to PKI domain CAs which are “subordinate” to the Principal CA. The use of this term shall encompass any CA operating under the common policy requirements of the PKI domain and which has a certificate issued to it by the Principal CA or any CA that is subordinate to the Principal CA.

1.3.1.5 USHER Certification Authority

USHER Foundation Level CAs managed by the USHER Operational Authority are authorized by the USHER Policy Authority to create, sign, and issue public key certificates to PKI domain Principal CAs or other certificate Subjects and/or revocation lists pertaining to these types of certificates. As directed by the USHER OA, an USHER Foundation Level CA is responsible for all aspects of the issuance and management of its certificates including:

- The certificate manufacturing process;
- Publication of certificates;
- Revocation of certificates; and
- Re-key, renewal, and update.

1.3.1.6 Related Authorities

An USHER Foundation Level CA operating under this CP may require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. An USHER Foundation Level CPS or the USHER OA shall identify the parties responsible for providing such services and the mechanisms used to support these services.

1.3.2 Registration Authorities

The Registration Authority (RA) is the entity that verifies each certificate Subject’s identity and collects information that is to be entered into any resulting public key certificate with respect to that identity. The RA also verifies the identity of any persons who are considered sponsors for certificates that are issued to Subscriber CAs. The USHER OA may act as the RA for USHER Foundation Level CAs or may delegate this responsibility with appropriate oversight. The RA performs its function in accordance with RA documentation approved by the USHER PA.

1.3.3 Subscribers

Subscribers named as Subjects in certificates issued under this CP may be natural persons or other entities that are sponsored by a responsible person or organization as determined by the specific USHER Foundation Level CPS. In all cases the Subscriber or sponsor shall be responsible for protection of the private key corresponding to the public key included in any resulting certificate(s).

1.3.3.1 Certificate Subjects Who are Natural Persons

A Subject who is a natural person will be provided a unique identifier in the subjectName field in an USHER end-entity certificate. The named subject will use his or her private key and certificate in accordance with any certificate policy asserted in the certificate. USHER end-entity

Subjects shall include USHER OA personnel and may include other natural persons as determined by the USHER PA.

1.3.3.2 Certificate Subjects That Are Not Natural Persons

The USHER PA may authorize issuance of an end-entity device certificate if deemed to be in support of the USHER infrastructure, mission, or Subscriber community. The device entity making use of that certificate and private key, e.g., certain network or hardware devices such as servers, firewalls or routers needed for infrastructure protection, must be under the control of the Subscriber or other responsible individual(s) designated by the Subscriber. The PA will determine what additional requirements or constraints may be appropriate.

1.3.3.3 Certificate Subjects That Are Subordinate PKI Domain CAs

Certain Subordinate PKI CAs may be issued certificates as appropriate and as approved by the USHER PA in order to support USHER activities.

1.3.3.4 Certificate Subjects That Are Cooperating PKI Domain CAs

A PKI domain CA that has met USHER eligibility requirements, has signed an Agreement, and has agreed to abide by the USHER Expected Practices shall be considered a Subscriber and will be issued an authority certificate by the USHER OA with contents as defined by the USHER PA, including any agreed upon policy mapping and name, path length, or other constraints.

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's subjectName to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificates in the trust path between the Relying Party's trust anchor and the certificate being evaluated; this decision typically is done by checking the appropriate information in certificates comprising the trust path, and by checking whether any of those certificates have been revoked, then applying whatever business, regulatory, or other rules the Relying Party wishes to employ to decide whether the trust path is acceptable for the specific use. The Relying Party can use the Subscriber's certificate to verify the integrity of a digitally signed message or file, to identify the creator of a message or file, or to establish confidential communications with the holder of the certificate. A Relying Party is entirely responsible for determining the suitability of the certificate for a particular use (see section 1.4).

1.3.5 Other Participants

The USHER PA may allow other participants with the execution of an appropriate Agreement which will set forth the details of that participation.

1.4 CERTIFICATE USAGE

Each Relying Party must evaluate the application environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept in making use of a certificate issued by an USHER Foundation Level CA based on the sensitivity or significance of

the information the Relying Party must protect. The sensitivity of the information processed or protected using certificates issued by USHER or a PKI domain CA may vary significantly. This evaluation must be done within each PKI domain for each application and is not controlled by this CP.

This CP defines an assurance level referred to as Foundation which is intended to be sufficient for a community of Cooperating PKI domains without specific oversight from a community trust anchor PA. A related assurance level referred to as "anyPolicy is defined and is used when the Subject CA or party is not known to conform to a specific CP, or is not verified by the USHER PA to be operating at a specific LOA but is instead guided by the USHER Expected Practices. A Relying Party must decide for itself to what degree to rely upon the certificate contents or to provide services to the certificate holder of a credential issued under this policy.

1.4.1 Appropriate Certificate Uses

The Relying Party must first determine the level of assurance required for an application, and then select the certificate appropriate for meeting the needs of that application. This will be determined by various risk factors including the value of the information, the threat environment, the existing protection of the information environment, and the risk tolerance of the Relying Party (i.e., what business, regulatory, or other rules the Relying Party is required to meet). These determinations are made by the Relying Party and are not controlled by the USHER PA or the USHER OA. For Cooperating PKI Domain CAs issued certificates under this CP, USHER makes no assertion about assurance levels or usage beyond the authority certificate issued to the Cooperating PKI Domain CA.

1.4.2 Prohibited Certificate Uses

Certificates issued by USHER must not be used for purposes that violate U.S. law or the law of the country in which the subject end entity (i.e. application or host, addressee of an e-mail) is located. Neither Internet2, nor AIRE, nor the USHER PA are responsible for Subscribers' or their end entities' actions, or for the decisions or actions of any Relying Party.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The USHER PA is responsible for all aspects of this CP.

1.5.2 Contact Person

Questions regarding this CP shall be directed to the Chair of the USHER PA, whose address can be found at http://www.usherca.org or pages linked under this URL.

1.5.3 Entity Determining CPS Suitability for the Policy

The USHER PA shall approve all USHER Foundation Level CPSs used by the USHER OA. The USHER PA shall exercise its responsibility to oversee activities of the USHER OA and its compliance with this CP and any associated CPS as it sees fit in its best judgment.

Cooperating PKI domains certified under an USHER Foundation Level CA are responsible for determining whether their CA CPSs conform to their CA CPs, and are encouraged to publish these policies and practices to facilitate community trust evaluations of their credentials, but the USHER PA makes no assertion about their trustworthiness.

1.5.4 CPS Approval Procedures

The term certification practice statement (CPS) is defined in the Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates." It is a comprehensive description of such details as the precise implementation of services and detailed procedures of certificate life-cycle management. It details how the strictures in the corresponding certificate policy are implemented. The specific USHER Foundation Level CPS, which is contained in a separate document published by the USHER OA and approved by the USHER PA, specifies how this CP will be implemented. A public version of this CPS shall be made available at the location identified in each certificate's CPSuri.

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
COMSEC	Communications Security
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSOR	Computer Security Object Registry
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard

FIPS PUB	(US) Federal Information Processing Standard Publication
HEBCA	Higher Education Bridge Certification Authority
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
ISSO	Information Systems Security Officer
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
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SPKAC	Signed Public Key And Challenge
SSL	Secure Sockets Layer
UPS	Uninterruptible Power Supply
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]
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [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.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
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	A statement of the practices that a CA employs in issuing,

Statement (CPS)	suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate-Related Information	Information, such as a Subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
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.
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 which 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.

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.
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]
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
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.
Key Escrow	A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, whereby one or more agents hold the Subscriber's private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the 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.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Mission Support Information	Information that is important to the support of deployed and contingency forces.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital

	signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique numeric identifier registered under the ISO registration standard to reference a specific object or object class. In USHER certificates they are used to uniquely identify the policy, each of the four levels of assurance, the Certificate Practice Statement, and the cryptographic algorithms supported.
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 CP 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 Management Authority (PMA)	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 CA, the PMA is the USHER PA.
Principal CA	The Principal CA is a CA designated by a PKI domain to be certified by the USHER Foundation Level CA.
Privacy	Restricting access to Subscriber or Relying Party information in accordance with Federal or State law, PKI domain, and institution 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 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 CP; may also be referred to as a directory.

Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
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 potential 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.
Secret Key	A “shared secret” used in symmetric cryptography, wherein users are authenticated based on a password, Personal Identification Number (PIN), or other information shared between the user and the remote host or server. A single key is shared between two parties: the sender, to encrypt a transmission, and the recipient, to decrypt the transmission, with the shared key being generated with an algorithm agreed to beforehand by the transacting parties.
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 CP.
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.
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 Agent	Entity authorized to act as a representative of a PKI domain in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
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]
UCAID	University Corporation for Advanced Internet Development, d/b/a Internet2. The UCAID Internet2 OID arc is registered under IANA {1.3.6.1.4.1} as organization 5923.
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 to Subordinate and Cooperating PKI domain Principal Certification Authorities.
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 may use a variety of mechanisms for posting information into a repository as required by this CP. These are described in the corresponding CPS.

2.1 REPOSITORIES

Each USHER Foundation Level CA will securely publish its root, CRLs, and valid Subscriber certificates. Access control mechanisms will be used when needed to protect repository information as described in Section 2.4 of this CP.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The USHER OA shall publish information concerning each USHER Foundation Level CA necessary to support its use and operation and the evaluation of its issued certificates by interested Relying Parties. Requirements for the publication by Cooperating PKI domains of information pertaining to their CAs may be set forth in the Agreement. Subscriber certificates and certificate status information shall be made publicly available.

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificate status information is published as specified in section 4.9.7. This CP and any subsequent changes shall be made publicly available within one week of approval. Any prior

major version of this CP shall remain publicly available for at least 6 months after the expiration date of the last certificate referencing it.

2.4 ACCESS CONTROLS ON REPOSITORIES

Security mechanisms will ensure that only authorized information is published by USHER at the specified location(s). Information will be protected similarly to the way most organizations protect critical data.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

USHER Foundation Level CAs shall be able to generate and sign certificates that contain an X.500 Distinguished Name (DN); the X.500 DN also may contain domain component elements. Certificates issued by an USHER Foundation Level CA to PKI domain CAs shall use the DN form.

3.1.2 Need for Names to be Meaningful

Certificates issued pursuant to this CP are only meaningful if the Subject names that appear in the certificates are not intentionally misleading and can be understood and used by Relying Parties. Subject names used in the certificates must refer to the entity to which they are assigned in a meaningful way.

When DNs are used, it is preferable that the common name represent the Subject in a way that is easily understandable by a person. For Subjects who are natural persons, this typically will be a name recognized for legal or business purposes. For other Subject entities, this may be a Certification Authority or other authorized designation. USHER Foundation Level CAs shall use DNs in certificates they issue.

3.1.3 Anonymity or Pseudonymity of Subscribers

No stipulation.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be contained in the applicable certificate profile and are established by the USHER PA.

3.1.5 Uniqueness of Names

The USHER PA is responsible for maintaining name uniqueness in certificates issued by an USHER Foundation Level CA. Name conflicts will be referred to the USHER PA to resolve.

Cooperating PKI Domains will be encouraged first to resolve any name conflicts among themselves.

3.1.6 Recognition, Authentication and Role of Trademarks

No Stipulation.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

USHER Foundation Level CAs accept from Subscribers' authenticated designated officers CSRs, which are reviewed and validated per the requirements in the appropriate Certificate Profile.

3.2.2 Authentication of Organization Identity

The USHER RA shall verify the eligibility of all applicant organizations based on criteria approved by the USHER PA before permitting certificate requests. Requests for USHER Foundation Level CA issued certificates shall include all information as outlined in the appropriate certificate profile. The USHER OA or RA shall verify the information to the best of its ability.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Individual Identities

An USHER Foundation Level CA RA shall verify the identity information of trusted officers of Subscribing Organizations in accordance with this CP and corresponding CPS. Additionally, the USHER RA shall record the process that was followed for each identity proofing. The process documentation and authentication requirements may include:

- 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; and
- The date of the verification;

3.2.3.2 Authentication of Component Identities

Devices or services may be named as certificate Subjects for USHER Foundation Level CA issued certificates. In such cases, the CA must have a natural person sponsor as defined in section 1.3.3. The PKI sponsor is responsible for providing the relevant information as outlined in the appropriate USHER certificate profile.

3.2.4 Non-Verified Subscriber Information

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

3.2.5 Validation of Authority

Before issuing certificates that assert organizational authority, an USHER Foundation Level CA shall validate the sponsor's authority to act in the name of the organization.

3.2.6 Criteria for Interoperation

The USHER PA shall determine the interoperability criteria for CAs operating under this policy. No warrantee of interoperation or suitability for any purpose is made with respect to end-entity certificates.

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

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes its identity. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key); a different serial number; and may be assigned a different validity period.

New certificates will need to be issued to Subscribers by an USHER Foundation Level CA when the USHER Foundation Level CA re-keys and when the Subscriber CA re-keys. Upon re-key of either of these components, the USHER OA shall identify and authenticate PKI domain Principal CAs 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 was identified as described in Section 3.2, using the currently valid credentials issued by the USHER RA to the Subscriber's trusted Administrator.

3.3.1.2 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the original certificate, but with a new, extended validity period and a new serial number. Authority certificates may be renewed pursuant the practices outlined in section 3.3.1.1.

3.3.1.3 Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old certificate. The old certificate may or may not be revoked pursuant the practices outlined in section 3.3.1.1.

3.3.2 Identification and Authentication for Re-Key After Revocation

After a certificate 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

Revocation requests must either be received from a trusted officer who has been authenticated or must be signed by that certificate's associated private key, regardless of whether or not the private key has been compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

Requests by a PKI domain for an USHER Cooperating Level authority certificate shall be submitted to USHER using a procedure approved by the USHER PA. The USHER PA shall establish the eligibility criteria which the USHER OA shall use to determine whether to approve an applicant's request to join USHER. After eligibility criteria have been satisfied (which may include USHER PA's separate approval of certain applicant organizations), a Subscriber Agreement will be negotiated with the applicant organization and its trusted officers will be identity-proofed by the USHER OA. The Agreement shall set forth responsibilities of the PKI domain and USHER and must be executed before USHER authorizes issuance of an USHER certificate to the PKI domain Principal CA. The PKI domain Principal CA shall have a distinguished name as defined in X.509, and that shall be placed in the certificate subject name field per the requirements of the corresponding Subscriber certificate profile.

4.1.1 Who Can Submit a Certificate Application

USHER accepts applications from U.S. higher education institutions or any entity or consortia that may have a need to interact with that community as determined by the USHER PA. Any resulting Agreement must be executed by an individual who has been designated by the organization as authorized to act on behalf of the organization.

4.1.2 Enrollment Process and Responsibilities

The USHER OA will evaluate the application in accordance with criteria approved by the USHER PA and will make a determination whether to issue the requested certificate(s), and what policy mappings (if any) to express in the certificate(s) if the USHER PA desires any policy mappings. Prior to issuance, the applicant PKI domain will enter into an Agreement with AIRE setting forth their respective responsibilities. After execution of the Agreement and after the applicant's trusted officers have been identity proofed, the USHER OA will issue the certificate(s). Before issuance, each CSR submitted to the USHER Foundation Level CA shall be checked to verify that each field and extension is properly populated with the correct information, before the certificate is delivered to the Subscriber.

4.2 CERTIFICATE APPLICATION PROCESSING

USHER will receive a certificate application (aka certificate signing request) from an approved and authenticated sponsor and will carry out issuance procedures. Information in certificate applications must be verified as accurate before certificates are issued.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the applicant PKI domain must meet the requirements specified for authentication as specified in Section 3. of this CP.

4.2.2 Approval or Rejection of Certificate Applications

USHER may approve or reject a certificate application based on applicability to the community or some other criteria that will be explained to the applicant at the decision point.

4.2.3 Time to Process Certificate Applications

No stipulation.

Practice Note: Certificate applications will be processed as soon as practicable.

4.3 CERTIFICATE ISSUANCE

This certificate issuance section relates to Subscribers of USHER Foundation Level CAs operated or managed by the USHER OA.

4.3.1 CA Actions during Certificate Issuance

Upon receiving a request for a certificate from a Subscriber, the USHER RA shall respond in accordance with the requirements set forth in this CP and corresponding CPS. For USHER Foundation Level CAs these requirements include (but are not limited to):

- Verify the information in the certificate request
- Build and sign a certificate if all certificate requirements have been met
- Make the certificate available to the Subscriber
- Request Subscriber confirmation that the certificate is correct. If the Subscriber does not confirm the accuracy of the certificate after a specified period, the certificate will be revoked.
- Once confirmed, publish the certificate.

This certificate will not be signed and issued until the processes set forth in the CP and CPS have been met.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

USHER Foundation Level CAs operating under this policy shall inform Subscriber of the issuance of its requested certificate(s) via email which shall describe how such certificate(s) will be made available to that entity.

4.4 CERTIFICATE ACCEPTANCE

Once an USHER Foundation Level certificate has been issued, its acceptance by the Subscriber completes the OA's issuance responsibility. For a Cooperating PKI domain, acceptance also commences interoperability with the USHER Foundation Level CA.

4.4.1 Conduct constituting certificate acceptance

Subscriber must confirm that the content of the certificate is valid.

4.4.2 Publication of the Certificate by the CA

USHER Foundation level certificates shall be published to an on-line accessible repository in accordance with the requirements of section 2. as soon as the certificate has been accepted.

4.4.3 Notification of Certificate Issuance by the CA to other entities

The USHER Policy Authority and all Subscribers must be notified when an USHER Foundation Level CA issues a CA authority certificate to a Subscriber.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Cooperating PKI domains that receive certificates from an USHER Foundation Level CA must use them only for the purposes for which they were issued. The intended scope of usage for a private key is specified in the associated certificate. Subscribers shall also be required to comply with any requirements set forth in the Agreement.

4.5.2 Relying Party Public key and Certificate Usage

Certificates issued under this policy specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. USHER Foundation Level CAs will issue CRLs specifying the current status of all unexpired certificates. Recommended guidelines for usage by relying parties are found in Section 1.4 of this CP. It is recommended that relying parties process and comply with this information whenever using certificates issued under this policy in a transaction, however, this CP does not specify what exact steps a Relying Party should take to determine whether to rely upon a certificate. The Relying Party decides, pursuant to its own policies, what steps to take. USHER Foundation Level CAs merely provide the tools needed to perform the trust path discovery and validation, and other considerations which the Relying Party may wish to employ in its determination.

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. Certificate renewal is permitted under this policy.

4.6.1 Circumstance for Certificate Renewal

If an end entity has a currently valid certificate, the end entity certificate may be renewed pursuant the practices outlined in section 3.3.1.1.

4.6.2 Who may request Renewal

See section 3.3.1.1.

4.6.3 Processing Certificate Renewal Requests

See section 3.3.1.1.

4.6.4 Notification of new certificate issuance to Subscriber upon Renewal

Same policy as detailed under Section 4.3.2

4.6.5 Conduct constituting acceptance of a Renewal certificate

No stipulation.

4.6.6 Publication of the Renewal certificate by the CA

Same policy as detailed under Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to other entities

Same policy as detailed under Section 4.4.3.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

An USHER Foundation Level CA may choose to re-key as approved by the USHER PA. Subscriber CAs may re-key as their policies require. Further, when an USHER Foundation Level CA updates its private signature key and thus generates a new root certificate, the OA shall notify all Subscribers that it has been changed. The new Foundation Level CA root certificate shall be conveyed to Subscribers as described in Section 2.1.

Subscribers shall identify themselves for the purpose of re-keying as required in Section 3.

4.7.1 Circumstance for Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for private keys for CAs and Subscribers.)

4.7.2 Who may request certification of a new public key

A Subscriber or human sponsor may request certification of a new public key.

4.7.3 Processing certificate Re-keying requests

Subscriber re-key requests will be processed per section 3.3.1.1.

4.7.4 Notification of new certificate issuance to Subscriber

Same policy as detailed under Section 4.3.2.

4.7.5 Conduct constituting acceptance of a Re-keyed certificate

Same policy as detailed under Section 4.4.1.

4.7.6 Publication of the Re-keyed certificate by the CA

Same policy as detailed under Section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other Entities

Same policy 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 must not be further re-keyed, renewed, or updated.

4.8.1 Circumstance for Certificate Modification

The new certificate may have the same or different subject public key. After certificate modification, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.8.2 Who may request Certificate Modification

Subscribers with a currently valid certificate may make a request for certificate modification. A Subscriber or human sponsor may request certificate modification**.**

4.8.3 Processing Certificate Modification Requests

Subscriber modification requests will be processed using the same process used for initial certificate issuance.

4.8.4 Notification of new certificate issuance to Subscriber

Same policy as detailed under Section 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

Same policy as detailed under Section 4.4.1.

4.8.6 Publication of the modified certificate by the CA

Same policy as detailed under Section 4.4.2

4.8.7 Notification of certificate issuance by the CA to other Entities

Same policy as detailed under Section 4.4.3.

4.9 CERTIFICATE REVOCATION & SUSPENSION

USHER Foundation Level CAs shall issue CRLs covering all unexpired certificates revoked under this policy. USHER shall make public a description of how to obtain revocation information for the certificates it publishes. Revocation requests must be authenticated.

4.9.1 Circumstances for Revocation

Circumstances under which certificates issued by an USHER Foundation Level CA to Cooperating PKI domains will be revoked include:

- At the request of The USHER Policy Authority as outlined in the Subscriber Agreement.
- The USHER PA receives sufficient evidence of compromise or loss of, or loss of control over, the private key corresponding to a certificate issued by an USHER Foundation Level CA.
- The USHER Operational Authority receives an authenticated request for certificate revocation from a Subscriber's previously designated trusted officer.

In addition, with regard to Subordinate PKI domains, USHER OA personnel might determine that an emergency has occurred that could impact the integrity of an USHER Foundation Level CA. Under such circumstances, the Chair of the USHER PA may authorize immediate certificate revocation. The full USHER Policy Authority shall meet as soon as practical to review such emergency revocation.

4.9.2 Who Can Request Revocation

An USHER certificate may be revoked upon direction of the USHER PA or upon an authenticated request by an end entity, or any of the Subscriber's designated trusted officers.

4.9.3 Procedure for Revocation Request

The process for requesting revocation of a Subscriber certificate shall be set forth in the corresponding CPS. When revocation of a certificate issued by an USHER Foundation Level CA is required, the revocation process shall be completed within the shortest practical time period.

A request to revoke a certificate from a Cooperating PKI Domain CA shall identify the certificate to be revoked and allow the request to be authenticated (e.g., digitally or manually). Only the USHER PA may direct the USHER OA to revoke USHER Foundation Level CA root certificates and Subordinate CA authority certificates. If a reason is provided and Subscriber requests that the reason be published in the CRL, the USHER Foundation Level CA will publish the reason upon revocation. USHER Foundation Level CAs will not accept the revocation "Hold" value.

Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber must so indicate to the USHER OA. All requests shall be authenticated.

If the revocation request appears to be valid, the USHER OA will revoke the certificate by placing its serial number and other identifying information on a published CRL.

Revocation of an USHER certificate shall be accomplished in accordance with Section 4.9.7 *CRL Issuance Frequency* of this CP. A certificate that is revoked shall remain in the published status information until the certificate expires and for one additional CRL beyond that point. A certificate may be removed from the second CRL issued after the revoked certificate expires. Further, and separate from the publication of the status information, prompt electronic notification shall be given by the USHER OA to all other USHER Foundation Level Subscribers.

4.9.4 Revocation Request Grace Period

No stipulation.

4.9.5 Time within which CA must Process the Revocation Request

USHER Foundation Level CAs will revoke certificates as quickly as practical upon receipt of a proper, authenticated revocation request. Authenticated revocation requests shall be processed before the next CRL is published, excepting those authenticated requests received within two hours of CRL issuance. Revocation requests received and authenticated within two hours of CRL issuance shall be processed before the following CRL is published.-

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

CRLs shall be issued periodically, even if there are no changes to be made. The frequency of issuance provides advice to Relying Parties about how often they may wish to re-check the CRL. Certificate status information (CRL) may be issued more frequently than the issuance frequency described below when circumstances warrant, for example after loss or compromise of a Private Key. The USHER OA shall remove superseded certificate status information from the repository upon posting of the latest certificate status information.

Certificate status information shall be published not later than the next scheduled update as indicated in each CRL.

USHER Foundation Level CAs shall issue CRLs at least once per month.

Circumstances related to emergency CRL issuance are specified in Section 4.9.12.

4.9.8 Maximum Latency for CRLs

For USHER Foundation Level CAs, CRLs shall be published at least once per month. There is no stipulation for cooperating PKI domain CAs.

4.9.9 On-line Revocation/Status Checking Availability

No stipulation.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related To Key Compromise

In the event of a PKI domain Principal CA private key compromise or loss, an updated CRL shall be published at the earliest feasible time by the USHER OA per the procedure outlined in Section 4.9.3.

4.9.13 Circumstances for Suspension

Suspension shall not be used by USHER Foundation Level CAs.

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 stipulation.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

The Subscriber Agreement is authoritative regarding this section:

Upon withdrawal by Subscriber from all USHER services, any certificates issued to Subscriber by AIRE through USHER that have not expired will be revoked. This Agreement may be terminated for cause by either party for failure of the other party to comply with or to perform any term, condition, representation or covenant contained in this Agreement if such failure continues for fifteen (15) days after written notice from the affected party to the offending party. If termination is by Subscriber for failure of USHER to perform, Subscriber shall be entitled to a refund of the prepaid portion of its current year's Annual Subscription Fees and shall be entitled to continue use of its USHER Authority Certificate until (1) it acquires and deploys an alternate Authority Certificate or (2) sixty (60) days, whichever occurs first. Subscriber’s USHER subscription may also be terminated by AIRE upon the majority vote of a quorum of the USHER PA that Subscriber is no longer qualified or has failed to observe its commitments under this Agreement. If Subscriber is terminated by vote of the USHER PA, Subscriber shall not be entitled to a refund of its Registration Fee or Annual Subscription Fees. Upon termination of this Agreement by either Party under this Section, any certificates issued to Subscriber by AIRE through USHER that have not expired will be revoked, except as provided for in this Section.

4.12 KEY ESCROW & RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

Under no circumstances shall USHER Foundation Level CA's or Subordinate CA's signature keys used to support non-repudiation services be permitted to be escrowed by a third party. For information regarding back up of private keys, see section 5.1.8.

Subscriber key management keys may be escrowed to provide key recovery and if this option is implemented, the USHER PA recommends that the document describing the practices be

identified in the applicable CPS and further recommends that under no circumstances should a Subscriber signature key be held in trust by a third party.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

USHER Foundation Level CAs do not issue encryption keys to PKI domain CAs. However, if encryption key pairs need to be issued by an USHER Foundation Level CA covering repository system access or for other purposes, the USHER PA shall set applicable requirements for that purpose.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

USHER Foundation Level CAs shall impose physical security requirements that provide similar levels of protection as those specified below.

The RA shall implement physical access controls to reduce the risk of unauthorized access and equipment tampering. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

5.1.1 Site Location and Construction

The location and construction of any facility housing USHER Foundation Level CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as intrusion sensors and keyed access, shall provide robust protection against unauthorized access to USHER Foundation Level CA equipment.

5.1.2 Physical Access

USHER Foundation Level CA equipment shall always be protected from unauthorized access, especially while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

These security mechanisms shall be commensurate with the level of threat in the equipment environment. The physical security requirements pertaining to CAs that issue Foundation-level certificates must be designed to provide that no unauthorized access to the hardware is permitted.

Physical security requirements pertaining to cooperating PKI domain CAs at the Foundation Assurance level shall be as set forth in the Agreement and Expected Practices.

Removable cryptographic modules shall be inactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and other USHER Foundation Level CA equipment shall be placed in secure containers. Activation data shall either be memorized or recorded and stored in a manner

commensurate with the security afforded the cryptographic module and shall not be stored with the cryptographic module. Access logs will be printed and archived.

5.1.3 Power and Air Conditioning

No Stipulation.

5.1.4 Water Exposures

USHER Foundation Level CA equipment shall be located in a facility outside of any known flood zone with sufficient floor drainage to remove the full flow of water that might occur if a supply line breaks without affecting the equipment.

5.1.5 Fire Prevention and Protection

Fire prevention or suppression shall be installed to protect USHER Foundation Level CA equipment.

5.1.6 Media Storage

USHER Foundation Level CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the USHER Foundation Level CA.

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

Back ups of signing keys may be kept in a secure offsite location.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of an USHER Foundation Level CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first requires that the person filling a role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

Each Cooperating PKI domain shall identify at least one individual responsible and accountable for the operation of each CA in that PKI domain to aid in problem resolution and other issues.

An USHER Foundation Level CA may encompass a variety of CA products. Different products support somewhat different roles, and use different mechanisms for registering or enrolling Subscribers and issuing certificates. The requirements of this policy are therefore drawn in terms of two abstract roles:

5.2.1.1 Administrator

The 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, and;
- generating and backing up CA keys.
- executing issuance of CRLs and certificates to Subscribers when authorized by an officer
- generating audit logs;
- routine operation of the CA equipment and operations such as system backups and recovery or changing recording media

5.2.1.2 Officer

The officer role is responsible for the issuance of certificates, that is:

- registering new Subscribers and requesting the issuance of certificates;
- verifying the identity of Subscribers and accuracy of information included in certification requests;
- approving the issuance of certificates;
- requesting or approving the revocation of certificates.
- performing or overseeing internal compliance audits to determine whether the USHER CA is operating in accordance with its CPS;
- generating, reviewing, and archiving audit logs

5.2.2 Number of Persons Required Per Task

The separation of roles among individuals provides a set of checks and balances over USHER Foundation Level CA operation. Distribution of roles among individuals may be enforced either by the CA equipment, or procedurally, or by both means.

5.2.3 Identification and Authentication for Each Role

An individual shall log his or her critical actions while performing the assigned role.

5.2.4 Roles Requiring Separation of Duties

For USHER Foundation Level CAs, individual CA personnel shall be specifically designated to the two roles defined in Section 5.2.1 above. No one individual shall assume both the Officer and Administrator roles.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit an USHER Foundation Level CA shall be set forth in the corresponding CPS.

For USHER Foundation Level CAs, personnel holding any of the Trusted Roles shall undergo background checks.

5.3.2 Background Check Procedures

Background check procedures shall be described in the CPS.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the USHER Foundation Level CA shall receive training in his/her respective role.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for PKI roles shall be aware of changes in their USHER Foundation Level CA operation. Any significant change to the operations shall have a training (awareness) plan. Examples of such changes are software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

AIRE, upon advisement from the USHER PA, shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving any USHER Foundation Level CA that violate the stipulations of this CP, the USHER associated Foundation Level CPS, or other procedures published by the USHER OA.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to any USHER Foundation Level CA shall meet applicable requirements set forth in this CP as determined by the USHER OA.

5.3.8 Documentation Supplied to Personnel

The USHER OA shall make available to the CA personnel the certificate policies it supports, relevant parts of the CPS, and any relevant statutes, policies or contracts.

5.4 AUDIT LOGGING PROCEDURES

Where possible, security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used as appropriate. The security audit logs for each auditable event defined in this section shall be maintained in accordance with *Retention period for archive*, Section 5.5.2.

Automated audit processes shall be invoked at system startup, and cease only at system shutdown. Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the USHER OA shall determine whether to suspend USHER Foundation Level CA operation until the problem is remedied.

5.4.1 Types of Events Recorded

At a minimum, system logs will be kept for USHER Foundation Level CA operating systems. Specific auditable events that must be recorded are defined in the CPS accompanying this CP.

- Access to the CA;
- Certificate life cycle events;
- Changes of configuration;
- Unexpected events; and
- Events that affect the security of the system

5.4.2 Frequency of Processing Log

Logs for the USHER Foundation Level CA shall be reviewed only when required for cause. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below. The individual who removes audit logs from an USHER Foundation Level CA system shall be an official different from the individuals who perform the Administrator role.

5.4.4 Protection of Audit Log

USHER Foundation Level CAs system configuration and operational procedures must be implemented together to provide that:

- only authorized people have read access to the logs;
- only authorized people may archive audit logs; and,
- audit logs are not modified.

Audit logs shall be moved to a safe, secure storage location separate from the USHER Foundation Level CA equipment with sufficient frequency to ensure availability. If a system is designed to over-write audit log file space after a specified time interval, the audit logs formerly contained therein are not considered deleted or destroyed if those audit logs have been backed up and successfully archived.

5.4.5 Audit Log Backup Procedures

A copy of the audit log shall be sent off-site in accordance with the CPS.

5.4.6 Audit Collection System (Internal vs. External)

USHER Foundation Level CA 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 an USHER Foundation Level CA.

The audit log collection system may include an automated logging system external to an USHER Foundation Level CA system if deemed appropriate by the USHER PA.

5.4.7 Notification to Event-Causing Subject

This CP imposes no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

The Operational Authority shall perform routine self assessments of security controls.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

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

5.5.2 Retention Period for Archive

The minimum retention period is subject to change depending on future administrative requirements or legal guidance. All entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities.

5.5.3 Protection of Archive

For an USHER Foundation Level CA, archived records may be moved to another medium when authorized by the USHER OA. The contents of the archive shall not be released to any third party except as determined by the USHER PA or as required by law. Archive media shall be stored in a safe, secure storage facility separate from the USHER Foundation Level CA.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 KEY CHANGEOVER

To minimize risk from compromise of an USHER Foundation Level CA’s private signing key, that key may be changed periodically. From that time on, only the new key should be used for certificate signing purposes. The older, but still valid, certificate should be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If a CA implements Certificate Revocation then the old key should be retained and protected until all potentially revocable certificates have expired.

This CP recommends that any USHER Foundation Level CA's signing key have an operational life of one half the validity period of its corresponding certificate. An USHER Foundation Level CA’s authority certificate shall have a validity period of not more than twenty years.

5.7 COMPROMISE & DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The USHER Policy Authority shall be notified if any Foundation Level or Subordinate CAs operating under this policy experience the following:

- suspected or detected compromise of the CA systems;
- physical or electronic penetration of CA systems;
- successful denial of service attacks on CA components;
- any incident preventing the CA from issuing a scheduled CRL.

The USHER Policy Authority will take appropriate steps to protect the integrity of the USHER PKI.

The CA's Operational Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CPS.

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

If USHER Foundation Level CA equipment is damaged or rendered inoperative, but the USHER Foundation Level CA signature keys are not destroyed, USHER Foundation Level CA operation shall 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 Foundation Level CA or Subordinate CA signature keys are compromised or lost (such that compromise is possible even though not certain):

- The USHER PA and all of its member PKI domains shall be notified securely and at the earliest feasible time (so that PKI domains may issue CRLs revoking any authority certificates issued to subordinate CAs);
- A new USHER Foundation Level CA key pair shall be generated in accordance with procedures set forth in the USHER Foundation Level CPS; and
- New USHER Foundation Level CA certificates shall be issued to Subscribers also in accordance with the USHER Foundation Level CPS.

The USHER OA shall also investigate and report to the USHER PA what caused the compromise or loss, and what measures have been taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby an USHER Foundation Level CA installation is physically damaged and all copies of the USHER Foundation Level CA signature key are destroyed as a result, the USHER PA and all of its member PKI domains shall be notified in a manner at the earliest feasible time, and the USHER PA shall take whatever action it deems appropriate, including but not limited to reestablishing the USHER Foundation Level CA equipment,

generating new private and public keys, being re-certified, and re-issuing all Subscriber certificates. Relying Parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of USHER Foundation Level CA operation with new certificates.

The USHER Foundation Level CA certificate status repository and on-line status servers, if any, shall be deployed so as to remain operational in the event of a physical disaster at any single USHER CA site. Typically this will be accomplished by means of mirrored servers located at another secure facility.

5.8 CA OR RA TERMINATION

In the event of termination of USHER Foundation Level CA operation, certificates signed by the USHER Foundation Level CA shall be revoked and USHER shall advise USHER Subscribers and any other certified PKI domains such as Bridge CAs, who have entered into Agreements that USHER Foundation Level CA operation has terminated so they may revoke certificates they have issued to any USHER Foundation Level CA. Prior to USHER Foundation Level CA termination, the USHER Foundation Level CA shall provide archived data to an approved archival facility.

PKI domains will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought in the event that the USHER Foundation Level CA is terminated.

In the event that an USHER Cooperating PKI domain CA terminates operation, the PKI domain PA shall notify the USHER PA as far in advance of the termination date as is feasible.

Practice Note: This section does not apply to CAs that have ceased issuing new certificates but are continuing to issue CRLs until all certificates have expired. Such CAs are required to continue to conform with all relevant aspects of this policy (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 CA Key Pair Generation

Cryptographic keying material for USHER Foundation Level CAs shall be generated in a secure manner, such as using FIPS 140 validated cryptographic modules or similar hardware/software as determined by the USHER PA.

An USHER Foundation Level CA must document its key generation procedure, and generate auditable evidence that the documented procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used.

6.1.1.2 Subscriber Key Pair Generation

Organizations are required to use a 2048 bit RSA key pair. USHER Foundation Level CAs will sign certificate requests that contain a 1024 bit RSA key only upon special approval from the USHER Policy Authority but for a shorter, 10-year validity period.

6.1.2 Private Key Delivery to Subscriber

Cooperating or subscribing PKI domain CAs generate their own key pair and therefore do not need private key delivery.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys shall be delivered to the certificate issuer in an authenticated manner.

6.1.4 CA Public Key Delivery to Relying Parties

Copies of USHER Foundation Level CA public keys shall be published in corresponding certificates in order to facilitate trust path validation. Each Subscriber's signed authority certificate will be sent via email to the Subscriber.

6.1.5 Key Sizes

FIPS-approved signature algorithms as detailed in the corresponding certificate profile shall be considered acceptable. If the USHER PA determines that the security of a particular algorithm may be compromised, it will recommend that applicable USHER PKI domain CAs revoke the affected certificates.

Authority certificates issued by an USHER Foundation Level CA to Cooperating PKI Domains shall use at least 1024 bit RSA or DSA (or better) with SHA-1 (or better) in accordance with FIPS 186.

If an USHER Foundation Level CA issues server certificates, similar security shall require at a minimum triple-DES or equivalent for the symmetric key, and 1024 bit RSA (or better) or equivalent for the asymmetric keys as determined by the USHER PA.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186. Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186 or a more stringent test if specified by the USHER PA.

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

Subscriber public keys that are bound into USHER Foundation Level CA Subscriber authority certificates shall be certified for the following uses: Certificate Signing, CRL Signing(06). The use of a specific key is determined by the key usage extension in the X.509 certificate. In particular, certificates to be used for digital signatures (including authentication) shall set the *digitalsignature* bit. Certificates to be used for data encryption shall set the *dataencryption* bit.

For Subordinate CAs and any administrative persons, certificates may include a single key for use with encryption and signature in support of legacy Secure Multipurpose Internet Mail Extensions (S/MIME) and other applications.

6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards & Controls

The relevant standard for cryptographic modules is FIPS PUB 140 *Security Requirements for Cryptographic Module*. The USHER PA may determine that other comparable validation, certification, or verification standards are sufficient. Cryptographic modules shall be validated to the FIPS 140 level identified in this section, or validated, certified, or verified to requirements published by the USHER PA.

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

Use of an USHER Foundation Level CA private signing key shall require action by multiple persons as set forth in Section 5.2 of this CP.

6.2.3 Private Key Escrow

Under no circumstances shall USHER Foundation Level CA signature keys used to support non-repudiation services be permitted to be escrowed by a third party.

6.2.3.1 Escrow of PKI Domain CA Encryption Keys

An USHER Foundation Level CA shall 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

If backed up, USHER Foundation Level CA private signature keys shall be backed-up under the same multi-person control as the original signature key. A single copy of the signature key may be stored at the USHER Foundation Level CA location; additional copies may be kept at USHER Foundation Level CA backup locations. Procedures for USHER Foundation Level CA private signature key backup shall be included in the USHER CPS.

6.2.4.2 Backup of Subject Private Signature Key

No stipulation.

6.2.5 Private Key Archival

USHER Foundation Level CA private signature keys shall not be escrowed or archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

USHER Foundation Level CA private keys shall be generated by and remain in a cryptographic module (or an equivalent process approved by the USHER PA). The CA private keys may be backed up in accordance with Section 6.2.4.1.

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 officer must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs, or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Method of Deactivating Private Key

If cryptographic modules are used to store USHER Foundation Level CA private keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

6.2.10 Method of Destroying Private Key

Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a “zeroize” command. Physical destruction of hardware should not be required.

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 at least 6 months beyond their expiration.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

USHER Foundation Level CA and Subordinate CA certificates will be issued with validity periods up to 20 years; however, Cooperating PKI domain CAs will be issued validity periods of less than 20 years and never more than the remaining validity period of the USHER signing key.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation & Installation

The activation data used to unlock USHER Foundation Level CA private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and may be user selected.

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should either be biometric in nature or memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module. The protection mechanism shall include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the respective CP or CPS.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. An USHER Foundation Level CA and its ancillary parts shall include the following functionality:

- Require authenticated logins
- Provide Discretionary Access Control
- Provide a security audit capability
- Restrict access control to USHER services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Prohibit object re-use or require separation for USHER Foundation Level CA random access memory
- Archive USHER Foundation Level CA history and audit data
- Require a trusted path for identification of PKI roles and associated identities
- Enforce domain integrity boundaries for security critical processes

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version

of the computer operating system as that which received the evaluation rating, or a later version if the platform in use has been re-evaluated with that newer version.

6.5.2 Computer Security Rating

No Stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

No stipulation

6.6.2 Security Management Controls

The configuration of the CA system, in addition to any modifications and upgrades, shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the software or configuration. The CA software, when first loaded, shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use. The CA shall periodically verify the integrity of the software as specified in the CPS. USHER Foundation Level CAs are operated offline and only used for purposes approved by the USHER PA.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

USHER Foundation Level CAs and their internal directories shall be connected within a secure system environment. They will not be connected to any network external to the secure environment. The USHER Foundation CA Repository shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup). Information will be transported using manual or equivalent off-line mechanisms, and all such information will be digitally signed (certificates and CRLs). The USHER Foundation Level CA Repository shall also be securely protected.

6.8 TIME-STAMPING

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version Numbers

USHER Foundation Level CAs and certified Cooperating PKI domain CAs shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of X.509 extensions are defined in certificate profiles. Certificate extensions used by an USHER Foundation Level CA shall conform to the certificate profile established by the USHER PA, compatible with appropriate standards bodies such as the IETF and the ISO, and published as part of the public USHER related Foundation Level CPS. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. Private extensions shall not be used in USHER Foundation Level CA authority certificates.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

Object Name	**Object Identifier**
id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

Certificates under this CP will use the following OIDs for identifying the algorithm for which the subject key was generated:

Object Name	**Object Identifier**
id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

7.1.4 Name Forms

Where required as set forth above, the subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by [RFC3647].

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

All certificates issued under this CP shall include a Certificate Policy OID. Certificates issued to USHER Foundation CAs or end-entities shall include the appropriate USHER OID. Certificates issued to Cooperating PKI domain CAs shall include an USHER OID or the X.509 anyPolicy OID as described in section 1 of this CP.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP shall contain a CPS Pointer pointing to an on-line copy of the public version of the CPS under which the USHER Foundation Level CA operates. That CPS must include a URL pointing to an on-line copy of this CP.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.1.10 Certificate Serial Numbers

Each certificate signed by an USHER Foundation Level CA in conformance with this CP shall include an integer serial number unique among all certificates issued by that CA. 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 Foundation Level CA shall include one or more URIs in the Authority Information Access (AIA) field that will enable a Relying Party to retrieve a copy of all certificates issued to the corresponding USHER Foundation Level CA, naming that CA as the subject and including that CA's public key. These will include self-signed CA certificates, CA authority certificates issued to it by another CA, and cross-certificates issued to it as part of cross certification with another CA.

Certificates issued by an USHER Foundation Level CA also may include one or more URIs in the Subject Information Access (SIA) field that might enable a Relying Party to retrieve

additional information about the Subject of the certificate. The corresponding CPS will provide details about these URIs, if any.

Note: Certificates issued by an USHER Foundation Level CA will be found in a public repository.

7.2 CRL PROFILE

7.2.1 Version Number(s)

USHER Foundation Level CAs shall issue X.509 version two (2) CRLs.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles addressing the use of each extension shall be issued by the USHER PA and published in the public version of the USHER Foundation Level CPS.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

The USHER PA will specify OCSP version compatibility at the time this service is introduced.

7.3.2 OCSP Extensions

No Stipulation at this time.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The USHER PA will periodically verify that the operations of USHER Foundation Level CAs are in compliance with its CP, CPS, and the provisions of any Agreements.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

No stipulation.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

At the time of any audit, the compliance auditor must be thoroughly familiar with requirements which the USHER PA imposes on the issuance and management of USHER Foundation Level CA certificates.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor either shall be a private firm or other private or public entity which is independent from the entity being audited, or it shall be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. The USHER PA shall determine the suitability of the compliance auditor recommended by the OA.

8.4 TOPICS COVERED BY ASSESSMENT

Any compliance audit of an USHER Foundation Level CA will verify that the CA is implementing all provisions of a CPS approved by the USHER Policy Authority on the basis of meeting the requirements of this Certificate Policy.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The USHER PA may determine that an USHER Foundation Level CA or PKI domain CA is not complying with its obligations set forth in this CP or the respective Agreement. If such a determination is made with respect to an USHER Foundation Level CA, the USHER PA may direct the USHER OA to cease operation of that CA until the deficiency is corrected. If such a determination is made with respect to a Cooperating PKI domain, the USHER PA may direct the USHER OA to suspend interoperating with it (e.g., by revoking its certificate(s)), or may direct that other corrective actions be taken which prevent interoperation.

8.6 COMMUNICATION OF RESULTS

Any Audit Compliance Report identifying corrective measures taken by the USHER Foundation Level OA shall be provided to the USHER PA and, where necessary, shall be communicated as set forth in 8.5 above.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

The USHER PA will approve and publish the fees, if any, for USHER services.

9.1.1 Certificate Issuance or Renewal Fees

No Stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

There will be no fee for access to certificate revocation information.

9.1.4 Fees for Other Services

There will be no fee for access to on-line certificate policy information. There may be fees for other forms of access at the sole discretion of the USHER PA.

9.1.5 Refund Policy

Refunds will not be given except as may be authorized under an Agreement.

9.2 FINANCIAL RESPONSIBILITY

Relying Parties, shall determine what financial limits, if any, they wish to impose for certificates used in any way to consummate a transaction. Liabilities are outlined in the Agreement.

9.2.1 Insurance Coverage

No stipulation except as outlined in the Agreement.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

USHER information not requiring protection shall be made publicly available. USHER access to PKI domain information will be addressed in the Agreement with that PKI domain.

9.3.2 Information not within the scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

Certain parts of USHER Foundation Level CPSs could contain information which, if disclosed, might compromise the integrity, security, or reliability of the USHER Foundation Level CA. Therefore, any USHER Foundation Level CPS that shall be made available publicly may be redacted.

9.4 PRIVACY OF PERSONAL INFORMATION

In order to operate the USHER Service, the USHER Operational Authority collects and manages personally identifiable information. This information includes contact information for individuals and other related information.

9.4.1 Privacy Plan

All other personal information gathered by USHER will be protected by AIRE's general privacy policy.

9.4.2 Information treated as Private

Personal 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.

9.4.3 Information not deemed Private

Information included in certificates is considered public.

9.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely, and may be 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 can be shared as needed to operate the USHER Operational Authority.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

None.

9.5 INTELLECTUAL PROPERTY RIGHTS

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

9.6 REPRESENTATIONS & WARRANTIES

The USHER Policy Authority shall—

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

9.6.1 CA Representations and Warranties

The Agreement is authoritative for all USHER Foundation Level CA warranties.

9.6.2 RA Representations and Warranties

USHER Warranties are outlined in Section 9.6.1 above. Any USHER Foundation Level CA's RA or Trusted Agent shall be expected to operate in accordance with the applicable sections of this CP.

9.6.3 Subscriber Representations and Warranties

PKI domains that receive certificates from an USHER Foundation Level CA must use them in accordance with the Agreement signed by the Subscribing organization and the USHER Expected Practices.

9.6.4 Relying Parties Representations and Warranties

This CP does not specify what steps a Relying Party should take to determine whether to rely upon a certificate. The Relying Party decides, pursuant to its own policies, what steps to take. An USHER Foundation Level CA merely provides the tools needed to perform the trust path discovery and validation, and other considerations which the Relying Party may wish to employ in its determination.

9.6.5 Representations and Warranties of other Participants

None.

9.7 DISCLAIMERS OF WARRANTIES

Any USHER warranties are outlined in the Agreement as in Section 9.6.1.

9.8 LIMITATIONS OF LIABILITY

The USHER Agreement is authoritative on Liability provisions.

9.9 INDEMNITIES

No stipulation.

9.10 TERM & TERMINATION

9.10.1 Term

This CP becomes effective when approved by the USHER Policy Authority. This CP has no specified term.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS

The USHER PA shall establish appropriate procedures for communications with PKI domain CAs operating under this policy as applicable.

For all other communications, no stipulation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The USHER PA shall review this CP periodically. Errors, updates, or suggested changes to this CP shall be communicated to every PKI domain Principal CA and Subscriber. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

In evaluating the need for changes to this CP and the Object Identifiers it contains, the USHER Policy Authority will be guided by the language of RFC 3647 which states (in section 4.9.12):

> *It will occasionally be necessary to amend a CP or CPS. Some of these changes will not materially reduce the assurance that a CP or its implementation provides, and will be judged by the policy administrator to have an insignificant effect on the acceptability of certificates. Such changes to a CP or CPS need not require a change in the CP OID or the CPS pointer (URL). On the other hand, some changes to a specification will materially change the acceptability of certificates for specific purposes, and these changes may require corresponding changes to the CP OID or CPS pointer qualifier (URL).*

9.12.2 Notification Mechanism and Period

All policy changes under consideration by the USHER PA shall be disseminated to interested parties. All interested parties shall provide their comments to the USHER PA in a fashion to be prescribed by the USHER PA.

The ratified version of this policy shall be signed as described in on the Signature page of this CP.

This CP and any subsequent changes shall be made publicly available within one week of approval. Any prior version of this CP shall remain publicly 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

No stipulation.

9.13 DISPUTE RESOLUTION PROVISIONS

The USHER PA shall resolve disputes associated with the use of an USHER Foundation Level CA or certificates issued by an USHER Foundation Level CA. This CP anticipates that a PKI domain PA may, for its own reasons, decline to accept the USHER Policy Authority's evaluation or mapping of its CP. In that case, the PKI domain PA may seek a dispute resolution hearing before the USHER PA, or may pursue directly an agreement with another PKI domain concerning reliance on a particular PKI domain CP and the certificates it issues.

9.14 GOVERNING LAW

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

9.15 COMPLIANCE WITH APPLICABLE LAW

All CAs operating under this policy are required to comply with applicable law.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

See the USHER Agreement.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

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

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.

10. BIBLIOGRAPHY

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

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)

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 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 Certificate Policy was originally based upon the Higher Education PKI Bridge (HEBCA) Certification Policy. That Certificate Policy was constructed initially by the EDUCAUSE/Internet2 HEPKI CP working group, chaired by Ken Klingenstein with David Wasley as editor. It was further refined by the EDUCAUSE Board of Instantiation and Development for the HEBCA by the HEBCA PA. That CP was adapted specifically for USHER Foundation Level CAs and reconfigured in accordance with the RFC 3647 format by Scott Rea (Dartmouth). Finally, this CP was edited to its final form by Scott Rea, John Krienke (Internet2), and the founding members of the USHER PA: Jim Jokl (Chair), Michael Gettes (Duke), Mark Luker (EDUCAUSE), Barry Ribbeck (Rice), Jeff Schiller (MIT), Renee Shuey (Penn State), and David Wasley (ret. UCOP).