Certification Practices Statement

for

Certificate Authority Service by CREN

Version 3.0

CREN

Corporation for Research and Educational Networking

January 27 2000

Acknowledgements

We wish to acknowledge the following individuals who participated in a series of planning discussions and meetings over a period from June of 1998 to June of 1999 to develop and prescribe the foundations of the Certificate Authority Service for Higher Education offered by CREN and this CREN Certificate Authority Certification Practices Statement.

Here is a list of individuals who supported these early planning and announcement efforts and who supported the concept and value of the CREN Certificate Authority service. On behalf of CREN and CREN member institutions, many thanks are extended to all. Particular thanks and recognition goes to Jeff Schiller of the Massachusetts Institute of Technology and his many hours of phone consultation, and the providing of the actual certificate issuance in the first phase of the CREN Certificate Authority service. Many thanks also go to David Wasley of the University of California System Office for his consultation and participation in phone meetings and CREN TechTalks and to UC System CA project leader Joan Gargano. Thanks also to CREN counsel, Dan Burk, who helped to sort out the many techno-legal issues involved in launching and operating the Certificate Authority service.

Other individuals who gave graciously of their time and expertise in the early phases of the project include:

Ira Fuchs, Princeton University

Michael Gettes, Princeton University

Ken Klingenstein, University of Colorado

Phil Long, Yale University

Andy Newman, Yale University

Vance Vaughan, University of California System Office

Other individuals who assisted in the process by way of an ad hoc advisory board include:

Rebecca Graham, Digital Library Federation

Ron Hutchins, Georgia Tech

David Millman, Columbia University

Pete Siegel, Iowa State University

Spencer Thomas, JSTOR

And a special recognition to all the members of the 1998-1999 CREN Board of Trustees who initiated this service by means of their votes at the February 98 and June 98 Board meetings.

Linda A. Cabot, Georgia Institute of Technology

Anthony D. Conto, University of Maryland

Ira Fuchs, Princeton University

Douglas Gale, George Washington University

Raman Khanna, Stanford University

Kenneth King, Board Member Emeritus

Ken Klingenstein, U Colorado at Boulder

Vijay Kumar, Massachusetts Institute of Technology

Cheryl Munn-Fremon, University of Michigan

Larry Rapagnani, University of Notre Dame

Ann E. Stunden, Cornell University

Russell S. Vaught, Pennsylvania State University

James L. Wolf, Binghamton University

Table of Contents

CREN Certificate Authority

Certification Practices Statement

1.0 Executive Summaries

This section describes the goals, purposes, and practices of the CREN Certificate Authority Service and the structure of the Certificate Authority Practice Statement.

1.1 Executive Summary of the CREN Certificate Authority Service

The Certificate Authority Service that CREN provides is designed to facilitate secure transactions for the education and research community. The CREN Certificate Authority service is a top level Certificate Authority Service. As such, this service issues institutional certificates, not individual certificates. These certificates are used in conjunction with certificates issued to students, faculty and staff by the institution. The CREN certificate serves as a second level of trust to authenticate that the individual's certificate listing the institution as issuer is valid and has been issued by that institution. The CREN certificate is a trust point from one institution to other higher education institutions, and to other relying parties, such as content providers and other service providers.

The management and administrative functions of CREN's Certificate Authority service are designed to support the community of higher education and research institutions with needs to safely and securely identify users — faculty, staff, and students — as they access and use resources and services over the network. It is anticipated that one of the first uses of the certificates will be to support inter-institutional resource sharing. This will be particularly useful for authenticating users for digital library and database resources that institutions want to share given instructional and research projects and programs. Another anticipated first use will be by relying parties, such as JSTOR, LEXIS/NEXIS, and other publishers and service providers that support instruction and research activities. It is anticipated that uses of the certificates will extend to other types of inter-institutional cooperation, such as student information, etc. as the infrastructure and trust chains develop.

An institution obtains an institutional certificate by completing the application and requesting institutional certificates according to the process described in the Operations and Procedures for Institutions Document. Part of that process includes sending a Request for Certificate to CREN. CREN then issues an institutional certificate that is signed with CREN's private key and that contains CREN's public key and the public key of the requesting institution's certificate authority.

It is expected that higher education institutions will establish their own local Certifying Authorities for issuing X.509 digital certificates to their faculty, staff and students. The certificates issued by an institution identify the faculty, staff, and students as being members of that community. The certificates issued by CREN certify that a certificate has been issued from a particular institution, providing a second level of trust that supports inter-institutional trust between institutions external to the campus. The value of the CREN certificate is that it provides a way for institutions to trust each other without establishing separate chains of trust between each individual pair of institutions.

The CREN certificate authority is a root level certificate authority. This means that the initial CREN key is a self-signed key. As the CREN certificate is recognized by other Certificate Authorities, a larger chain of trust is established.

The CREN Certificate Authority Service is built on the Public Key Infrastructure (PKI) technology. In brief, this PKI technology depends on certification authorities that certify a population of public-private key-pair holders. Each certificate contains a public key value plus information that uniquely identifies the certificate's subject, usually either a person or an institution.

1.2 Executive Summary of the CREN Certificate Authority Certification Practices Statement (CPS)

This CREN Certification Practice Statement describes the processes and practices that govern the operation of the CREN Certificate Authority. This CPS details and controls the certification process from the initial verification of the institutional requestor and the request for certificate process, through the issuing, acceptance, using, suspending, revoking, and renewing of CREN certificates. This CPS provides the basis for agreement between all parties that request and use CREN certificates for authentication and authorization. Figure 1 provides an overview of the role of the CREN Certificate Authority within the public key infrastructure as used by the research and education community.

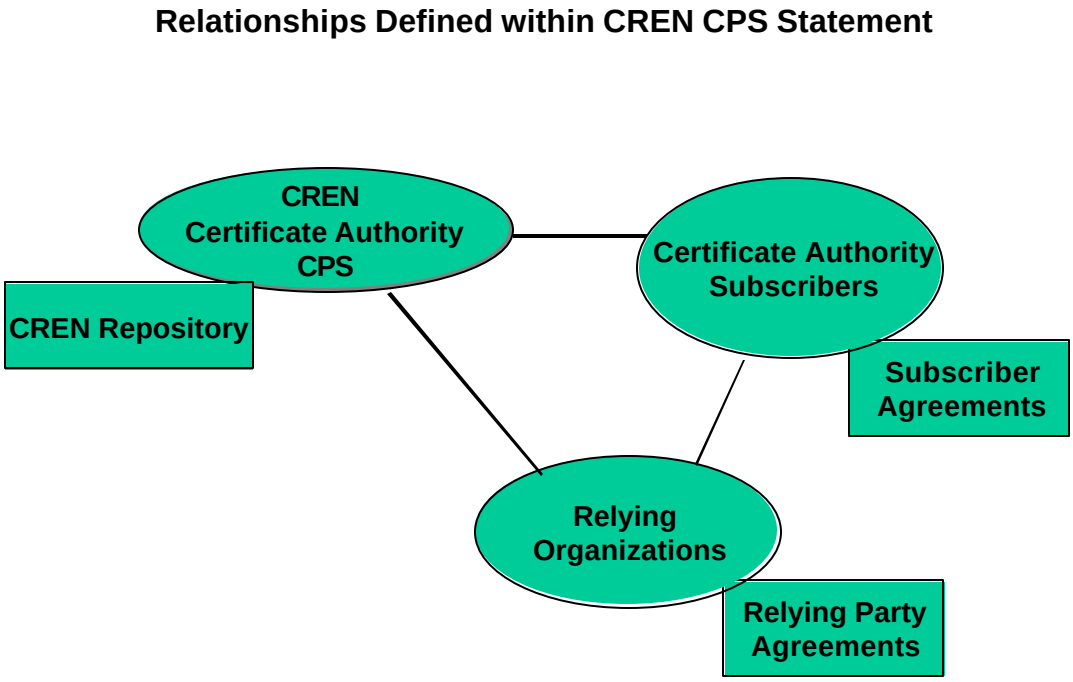

Figure 1 — Overview of the Relationships Defined in the CREN CPS

1.2.1 Structure of the Certification Practice Statement

This Certification Practice Statement describes the processes for the issuing and use of CREN's

certification services. There are five major phases in the issuing and use of CREN Certificates. These phases are as follows:

Phase 1: Initial Application and Subscriber Contact Validation

Phase 2: Validation of the Certificate Authority Institutional Contacts, Certificate Request, Certificate Issuance, and Certificate Acceptance

Phase 3: Procedures for Key Management and Security

Phase 4: Certificate Suspension and Revocation Processes

Phase 5: Certificate Expiration and Renewal

These phases are compatible with other private- and public-sector practice processes and statements. As these practices evolve, the CREN practices will also evolve.

The companion CREN Certificate Authority Operations and Procedures for Institutions Document contains recommended practices and guidelines for Certificate Authority subscribers. It is strongly recommended that subscriber institutions follow these practices in issuing and managing their local institution's certificates and in maintaining their certificate-based public key infrastructure.

1.3 Summary of Certificate Authority Phases and Processes

This section provides a summary of the Certificate Authority phases, processes and obligations that will govern the operation of the CREN CA.

1.3.1 CREN Certificate Request Application Requirement and Processes

An institution that desires to become a subscriber for the CREN Certificate Authority service will complete a Certificate Service Application that includes a statement about the (1) existence and security of an institutional certificate authority or its equivalent on the requesting institution's campus, (2) the designated executive officer who will sign the application for the Certificate Service, (3) and the designated certificate authority technical contact who will request and accept the CREN institutional CA certificate.

Before submitting an application for the CREN Certificate Authority Service, the institution must have a secure certificate authority set up on campus that is issuing certificates for the members of that institution—or its equivalent. This certificate authority service may support only a subset of the population of the community or it may support the entire community. This means that the institution is using a server that generates key pairs, and that the institution has the private key of the institution's key pair secure from compromise in a trustworthy manner.

1.3.4 Acceptance of the CREN Institutional Certificate

Before a certificate is valid, an institution must accept their institutional certificate after it is issued by CREN. The institution accepts the certificate by sending a secure signed message to the Certificate Authority System Administrator (CASA). An institution also accepts a certificate by making use of it. By accepting a certificate an institution also agrees to certain important representations about the use of the certificate.

1.3.5 Relying Institutions or Relying Service Providers

Any institution or service provider that is the recipient of a digital signature or certificate is responsible

for deciding whether to rely on it. Before relying on a certificate, CREN recommends that an organization check the CREN Repository to confirm that the certificate is valid and has not been revoked or suspended. CREN also recommends that an institution use the CREN certificate to verify that the digital signature was created during the operational period of the institutional certificate.

1.3.6 Notification Agreement

The Institution's Certificate Authority Technical Contact agrees to notify the CREN CA Administrative contact upon compromise of the institution's private key. This is done by communicating the compromise via a secure communication channel that is set up and maintained during the course of the use of the certificate. This secure communication channel must be independent of the institution's certificate. PGP is an example of a recommended secure channel for this purpose. When an institution's private key has been compromised, speed is of the essence to post this information on the repository. CREN will only post a revocation if a secure communication channel has been used for this notification.

1.3.7 Warranties

This Certification Practice Statement describes the warranties made by CREN and the institutional issuing authorities. Otherwise, warranties are disclaimed and liability is limited by CREN. More detail on warranties is in Section 11.

1.3.8 Other Provisions

This Certification Practice Statement contains various miscellaneous provisions. More information is available at CREN's website at http://www.cren.net or by contacting CREN at cren@cren.net. The current version of the Operations and Procedures for Institutions document is also at the CREN website.

1.4 Publication of the CPS

This CPS is available at the CREN web site (http://www.cren.net). The CREN CA Repository will hold the CREN CPS, and also a listing of the issued certificates, the CREN public key certificate, and the revocation lists, or links to such.

1.5 Customer Assistance, Education and Training

This CPS assumes that the Institution's Certificate Authority Technical Contact and other operational institutional contacts are familiar with digital signatures and with PKI technology. To help ensure that familiarity, CREN offers training on digital signatures and public key techniques in various formats. It is recommended that this training occur prior to an institution applying for a CREN certificate. Educational and training information will be available at the CREN web site at http://www.cren.net.

1.6 Table of Acronyms and Abbreviations

CA	Certification Authority
CAEO	Certificate Authority Executive Officer
CASA	Certificate Authority System Administrator
CDPE	CREN Distinguished Panel of Experts (CDPE)
CMR	CREN Member Representative
CREN CA	CREN Certificate Authority
CPS	Certification Practice Statement
CR	CREN Root
CRL	Certificate Revocation List
CSA	Certificate Service Application
CSR	Certificate Signing Request
ICATC	Institution's Certificate Authority Technical Contact
IETF	Internet Engineering Task Force
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RDN	Relative Distinguished Name
RSA	a cryptographic system
RSP	Relying Service Providers
X.509	ITU-T standard for certificates and their corresponding authentication framework

2.0 CREN Certificate Authority Infrastructure

This section describes the infrastructure for the CREN Certificate Authority Service, including an overview of the CREN certificate issuance processes, characteristics of the CREN certificates, subscriber eligibility, and certificate management processes.

2.1 Certificates in Higher Education and Research

CREN's Certificate Authority Service is designed to support and facilitate secure network transactions for the education and research community. To accomplish this, CREN serves as a trusted third party, issuing, managing, suspending, and revoking top level institutional certificates for higher education and research in accordance with published practices.

This statement of practices is the vehicle to provide a common understanding among the parties — CREN, Institutional Certificate Subscribers, and the Relying Service Providers — as to the management and administrative practices used to protect the integrity of CREN's root key and the issuance, acceptance and use

of institutional certificates signed with that key. This statement of practices also sets forth the mutual expectations of this service between CREN and the institutions.

2.2 CREN PKI Model

CREN's certificate authority services are implemented within a PKI hierarchy composed of the following entities:

- The CREN root,
- The set of CREN institutional subscribers and relying parties
- Campus-Issued Certificates for Staff, faculty and students

See Figure 2 for a graphic of this model. Note that the CREN certificate supplements the campus level certificate. Also note that a hybrid model can be implemented within this structure with an individual institution signing the CREN certificate of another institution.

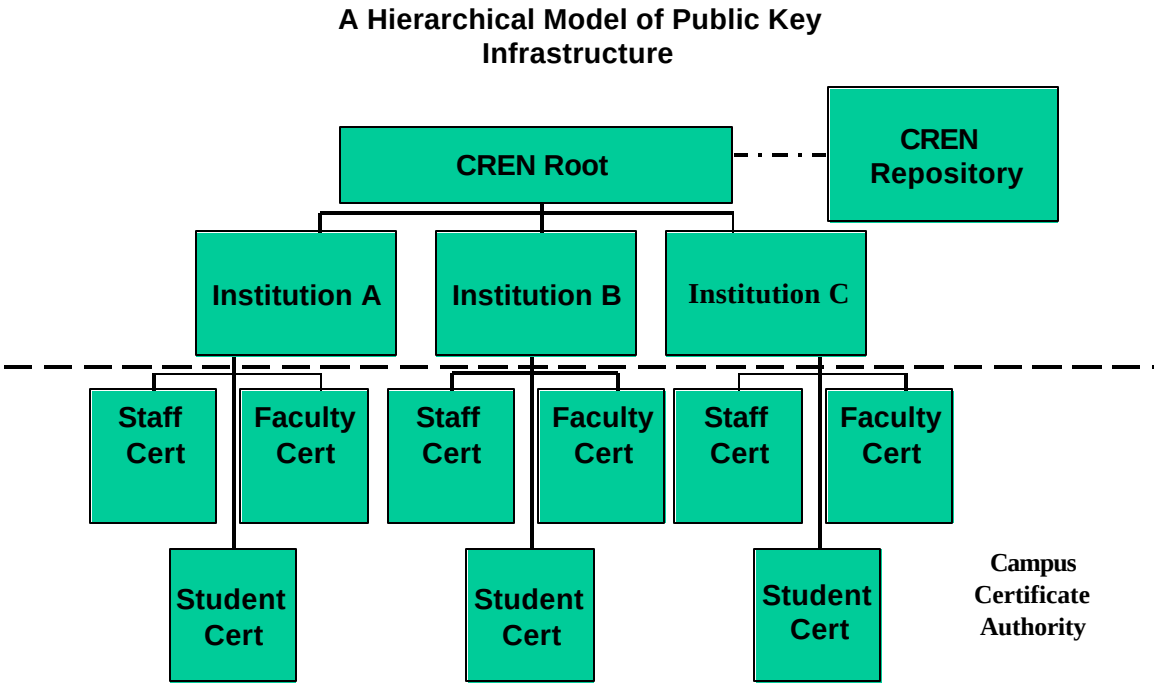

Figure 2 — A Hierarchical Model of Public Key Infrastructure

2.3 General Discussion of CREN Certificate Issuance and Management

CREN acts as a trusted third party to confirm the relationship between a public key and the identity of the entity named in the certificate. This confirmation is expressly represented by a certificate – a digital message — that is is sued and digitally signed by CREN. The management of this certification process includes application and registration, naming conventions, appropriate institutional contact authentication, issuance,

acceptance revocation, suspension, and renewals of institutional certificates.

2.3.1 Characteristics of CREN Certificates

The basic characteristic of a CREN certificate is that it is a top-level certificate that is issued to institutions. CREN currently uses the RSA public key system for the certificate service. CREN provides one level of certificate for institutions with one level of trust associated with that certificate. CREN may also issue server certificates to institutions with one level of trust.

Other issuing authorities often issue certificates with varying level of strengths based on the "method of issuance." Method of issuance refers to the processes used to validate that the representatives of the institution are who they say they are, and that the method of operation of the campus CA is attested to be secure and trustworthy. The following sections describe the content of the CREN certificates.

2.3.2 Naming Policy

The naming policy and validation process that CREN will use to ensure uniqueness and validation of the applicant institution name is detailed in the Operations and Procedures for Institutions Document.

2.3.3 Validation of Identity of Institutional Representatives

Part of the application process for a CREN certificate is validation of the identities of the persons from each institution that will be involved in the application and issuance of a CREN Institutional Certificate. The contacts to be validated are (1) the CREN Member Representative (CMR), (2) the Certificate Authority Executive Officer (CAEO), and (3) the Institution's Certificate Authority Technical Contact (ICATC).

2.3.4 Certificate Request and Issuance

In response to a Certificate Service Application that has been submitted by the CREN Member Representative and signed by the Executive officer or equivalent, and the receipt of a Certificate Service Request from the Institution's Certificate Authority Technical Contact (ICATC), the CREN system administrator issues a CREN institutional certificate to the ICATC. The ICATC reviews the issued CREN certificate to determine its acceptability for the institution's purposes, and, if satisfied, accepts the CREN institutional certificate via an acceptance back to the CREN System Administrator. Once the certificate is accepted, the institutional certificate is posted to the CREN CA repository.

2.4 The CREN Institutional Certificate

The digital certificates issued by CREN will follow the IETF x509.3 standard (RFC 2511). Future standards will be followed as appropriate.

2.4.1 Contents of the CREN Institutional Certificate

The CREN institutional certificates that will be issued will conform to the IETF x.509v3 standard. Here is a listing of the contents of the CREN certificate.

(1) The unique Certificate Serial Number (as per X.509)

(2) The issuer of the Certificate — CREN's X.500 name

(3) The range of dates that the certificate is valid. The initial time period will be for two years.

(4) The Institutions X.500 name as provided in the certificate request message.

(5) The institution’s public key

(6) CREN's digital signature

(7) Other items as specified in the Operations and Procedures for Institutions Document. This may include a limited warranty statement and link to the full CPS.

2.4.2 Warnings, Liability Limitations, and Warranty Disclaimers

Each certificate includes a pointer to the following full text of warnings, limitations, and disclaimers in the CPS. The statement contained on the certificate will be as follows:

> **This certificate incorporates the CREN Certification Practice Statement (CPS) by reference. Use of this certificate is governed by the CPS. The CPS is available on the CREN web site; by email at cren@cren.net; and by mail to the mail address at the www.cren.net site. The CPS disclaims and limits certain liabilities, including consequential and punitive damages. The CPS also includes caps on liability related to this certificate. See the CPS for details.**

2.4.3 Certificate Chain for CREN Certificate

CREN's CA performs the service of a root registration authority. This means that the top-level certificate will be a self-signed certificate. In other words CREN will be listed as both the subject and the issuer. The public key of this self-signed certificate will be the public key of the CREN CA. CREN's self-signed key will conform to the X.509v3 format as profiled by the IETF's X.509 Public Key Infrastructure Working Group. It can be trusted without recourse to additional validation during verification of digital signatures.

2.5 Generation and Protection of CREN Root

The CREN root (CR) is a CREN owned and operated entity that issues certificates for institutions. The CREN's initial self-signed root will be 2048 bits; the minimal length of the institutional certificates will be 1024 bit. A trustworthy hardware device (BBN SafeKeyper Box) is used to create, protect, and destroy CREN's private key. CREN's root key pair may be replaced and the replacement public key published in the CREN repository. The physical keys for the SafeKeyper box are managed to ensure that no one individual can open the box, and that the loss of one key does not disrupt the certificate issuance process.

2.6 CREN Repository

The CREN repository is a publicly available collection of databases for storing and retrieving certificates and other information related to certificates. The CREN repository's content includes, but is not limited to, the following: the public keys of subscriber certificates, Certificate Revocation Lists and other suspension and revocation information, current and prior versions of the CREN CPS, and other information as prescribed by CREN from time to time. The CREN public key will be published on the CREN website and the repository and will be PGP signed.

2.6.1 Publication of Certificates in the CREN Repository

CREN will act promptly to publish certificates, amendments to the CPS, and notices of certificate suspension or revocation in the CREN repository. The CREN repository is accessible at **https://www.cren.net** and by other communications methods as may be appropriate. CREN may publish both within and outside of the CREN repository a subscriber's certificate and CRL-related data.

3.0 Phases One, Two and Three: Certificate Operations:

This section describes the prerequisites for institutions becoming subscribers of the certificate authority service. This section also describes the processes and practices of the Phases One and Two of the Certificate Operations. Phase One is the Application Process, including Validation of Subscriber Institutional Contacts and Approval of the Application; Phase Two includes the Certificate Request, Certificate Issuance, and Acceptance. This section also describes Phase Three, which describes the general procedures for Key Management and Security. Later sections describe the operations of Phase Four, Certificate Suspension and Revocation and Distribution, and Phase Five, Certificate Expiration and Renewal.

3.1 Prerequisites for Subscriber Application and Acceptance

CREN's Certificate Authority Services are designed for use by higher education and research institutions. They are designed primarily for those institutions that are CREN members. To achieve uniform levels of trustworthiness throughout the trust chain, CREN subscribers agree to do their best effort to follow the basic subscriber practices described in the Operations and Procedures for Institutions Document.

3.2 Phase One of Certificate Operations

This section on Phase One of the Certificate Operations describes the processes for the application process. The university and CREN agree to establish a Certificate Authority Service Relationship. The initial point of contact will be the CREN member representative who is duly on record as the CREN Member Representative. The CREN Member Rep contacts the CREN office with a request to establish a Certificate Authority Service Relationship between the institution and CREN. The application form for this service is available on the CREN website at www.cren.net.

Steps Two through Seven of the Application process, including the validation of the institutional contacts are in the Operations and Procedures for Institutions Document.

3.3 Phase Two: Certificate Request, Certificate Issuance, and Acceptance

This section provides a summary of the processes to be used for the request, issuance and acceptance of the institutional CREN certificate. Instructions for sending the Certificate Authority Request will be on the web. The detail on all these steps are in the Operations and Procedures for Institutions Document.

3.4 Phase Three: Key Management and Security of the Certificate Authority Service

This section describes the high level processes for managing the keys and the security of the CREN Certificate Authority Service. The detail on all these processes are in the Operations and Procedures for Institutions Document.

3.5 Records Documenting Compliance

CREN shall maintain records in a trustworthy fashion, including documentation of their own compliance with the CPS, and documentation of actions and information that is material to each certificate application and to the creation, issuance, use, suspension, revocation, expiration, and renewal or re-enrollment of each certificate it issues. These records shall include all relevant evidence in CREN's possession regarding the following:

• The identity of the subscriber institution named in each certificate,

• The identity of persons requesting certificate issuance, suspension or revocation

• Other facts represented in the certificate,

• Time stamps, and

• Other items as may be stated in the Operations and Procedures for Institutions Document

Records may be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate and complete. CREN may require a subscriber or its agent to submit documents to enable CREN to comply with this section.

3.6 Time Stamping

Time stamping is intended to enhance the integrity of CREN's CA service and the trustworthiness of certificates and to contribute to the non-repudiation of digitally signed messages. Time stamping creates a notation that indicates the date and time of an action (expressly or implicitly) and the identity of the person or device that created the notation.

The following data shall be time stamped, either directly on the data or on a correspondingly trustworthy audit trail:

• Certificates,

• CRLs and other suspension and revocation database entries,

• Each version of the CPS,

• Customer service messages, and

• Other information, as may be prescribed in this CPS and the Operations and Procedures for Institutions Document

3.7 Records Retention Schedule

CREN shall retain in a trustworthy fashion records associated with institutional certificates for at least five (5) years after the date a certificate is revoked or expires. Such records may be retained as either retrievable computer-based messages or paper-based documents.

3.8 Audit

CREN shall implement and maintain trustworthy systems to preserve an audit trail for all material events, such as key generation and certificate application, issuance, validation, suspension, and revocation. A certified public accountant or an accredited computer security professional shall audit the CREN operations to evaluate its compliance with this CPS and other applicable agreements, guidelines, procedures, and standards.

CREN will not perform audits of the institutional subscribers. Statements of compliance with appropriate safeguards and certificate processes will be part of the subscriber application form. CREN is not responsible for any damages to anyone resulting from CREN's use of these compliance statements.

3.9 Availability and Publication of Institutional Certificates

Institutions shall make copies of their own certificates (*i.e.*, those in which the Institution is the subject) and any revocation data (where applicable) available to any person who has and desires to duly verify a digital signature that is verifiable by reference to such a certificate. The certificates and associated data will be

published in the CREN Repository.

3.10 Confidential Information

The following information shall be considered received and generated in confidence by CREN and may not be disclosed except as provided below:

- CA application records, whether approved or disapproved,
- Subscriber agreement and certificate application records (except for information placed in a certificate or repository per this CPS),
- Transactional records (both full records and the audit trail of transactions),
- Certificate audit trail records created or retained by CREN,
- Certificate audit reports created by CREN,
- Security measures controlling the operations of the CREN hardware and software and the administration of certificate services.

CREN shall not disclose or sell applicant names or other identifying information, or share such information, except in accordance with this CPS. Note, however, that the CREN Repository shall contain certificates, as well as revocation and other certificate status information.

3.11 Voluntary Release / Disclosure of Confidential Information

CREN shall not release or be required to release any confidential information without an authenticated, reasonably specific request prior to such release from (i) a valid representative of the institution to whom CREN owes a duty to keep such information confidential (ii) or a court order. CREN may require that the requesting person pay a reasonable fee before CREN discloses such information.

3.12 Termination of CA Operations

The following obligations are intended to reduce the impact of a termination of service by providing for timely notice, transfer of responsibilities to succeeding entities, maintenance of records, and certain remedies, CREN reserves the right to terminate the CREN CA operations upon appropriate notice to its subscribers.

Before ceasing to act as a top level Certificate Authority, CREN will do the following:

(a) Notify its subscribers of its intention to cease acting as a top level Certificate Authority. Such notice shall be made at least ninety (90) days before ceasing to act as a CA.

(b) Revoke all certificates that remain unrevoked or unexpired at the end of the ninety (90) day notice period, whether or not the subscribers have requested revocation.

(c) Give notice of revocation to each affected subscriber, as detailed in CPS.

(d) Make a reasonable effort to ensure that discontinuing its certification services will cause minimal disruption to its subscribers and to organizations and people duly needing to verify digital signatures by reference to the public keys contained in outstanding certificates.

(e) Make reasonable arrangements for preserving its records.

4.0 General Requirements for Certificate Authority Subscribers

All institutions applying for certificate authority service shall complete the following general procedures for each certificate application:

(a) Generate a key pair and demonstrate to CREN that it is a functioning key pair,

(b) Protect the private key of this key pair from compromise,

(c) Provide a distinguished name (DN), using the x500 naming protocols, and

(d) Submit an application form for subscriber service, and

(e) Submit a Request for Certificate, including the public key of this key pair, to CREN.

4.1 Key Generation and Protection

The following procedures are applicable to all institutions requesting and using CREN institutional certificates.

4.1.1 Holder Exclusivity; Controlling Access to Private Keys

Each certificate applicant shall securely generate its own private key, using a trustworthy system, and taking necessary precautions to prevent its compromise, loss, disclosure, modification, or unauthorized use. It is understood that CREN subscribers and CREN certificate applicants will use products that provide appropriate protection to keys.

Each certificate subscriber Institution applicant acknowledges that such Institution, and not CREN, is exclusively responsible for protecting its private key(s) from compromise, loss, disclosure, modification, or unauthorized use.

Subscribers and CREN agree not to monitor, interfere with, or reverse engineer the technical implementation of any subscriber's private key.

4.1.2 Delegation of Responsibilities for Private Keys

Delegation of responsibility for any private key, if it occurs, does not relieve the institution of its responsibilities and liabilities concerning the generation, use, retention, or proper destruction of its private key.

4.2 Certificate Authority Service Application Information

The Certificate Authority Service Application form includes the items listed below. Not all information shown below will appear in the Certificate, and the items of such information not included in the certificate will be kept confidential by CREN.

4.2.1 Certificate Application Form Contents

This section provides an example of the type of information that will be on the Certificate Authority Service Application. Detail on the exact information to be required is in the Operations and Procedures for Institutions Document.

(a) Domain name

(b) Organization

(c) Organizational unit (if applicable)

(d) Member Representative Contact Information

(e) City, state, country, postal/zip code,

(f) Contact information of the Certificate Authority Executive Officer (CAEO)

(g) Contact information of the Institution's Certificate Authority Technical Contact (ICATC)

(a) Other items may be specified in the CREN CA Operations and Procedures for Institutions Document

4.3 Method of Communication of Application Form

The completed application and subscriber agreement shall be submitted as specified in the CREN CA Operations and Procedures for Institutions Document

5.0 Validation of Information on Certificate Service Application and Request

This section describes the processes to be used in the validation of the information provided on the (1) Certificate Authority Service Application and (2) Request for Certificate messages. Additional detail is in the Operations and Procedures for Institutions Document.

5.1 Validation Requirements for Certificate Service Applications

Upon receipt of an application for certificate authority service, CREN shall confirm that:

(a) The Member Representative, the Certificate Authority Executive officer (CAEO), and the Institution's Certificate Authority Technical Contact (ICATC) are valid representatives of the institution identified in the certificate service application,

(b) The institution attests to operating a certificate authority service in a trustworthy manner,

(c) The institution agrees to make its best effort to abide by the provisions in this CPS and in the Operations and Procedures for Institutions Document.

5.2 Validation Requirements for Certificate Requests

Upon receipt of a request for certificate message from the Institution's Certificate Authority Technical Contact, CREN shall confirm that:

(a) The certificate message sender is a valid representative of the institution identified in the certificate request.

(b) The certificate institution rightfully holds the private key corresponding to the public key to be listed in the certificate, and

(c) The information to be listed in the certificate is accurate.

(d) Other information as may be specified in the Operations and Procedures for Institutions Document.

(e) Once a certificate is issued, CREN shall have no continuing duty to monitor and investigate the accuracy of the information in a certificate..

5.2.1 Third-Party Confirmation of Institution Information

With respect to certificate service applications for institutions, CREN may use third parties and third party databases to confirm the applicant's name, address, and other registration information through comparison with third-party databases and through inquiry to appropriate government entities. Confirmation of information of an applicant and applicant institution, and other information may require procedures focusing on specific criteria. If CREN and its third party databases do not contain all the information required, CREN or the third party may undertake an investigation or request additional information from the applicant.

5.3 Approval of Certificate Service Applications

Upon successful performance of all required validations in accordance with this CPS, CREN shall approve the service application. Approval is demonstrated by issuing a normal certificate in accordance with this CPS.

5.4 Rejection of Certificate Service Application

If any portion of the validation fails, CREN shall reject the certificate application by promptly notifying the certificate applicant of the validation failure and providing the reason (except where prohibited by law) for such failure. Where such validation failure is caused as a result of third-party database information, CREN shall provide the certificate applicant with the third-party database company's contact information for inquiry and dispute resolution. Such notice shall be communicated to the certificate applicant using the same method as was used to communicate the certificate application to CREN. An institution whose certificate application has been rejected may thereafter reapply.

6.0 Issuance of Certificates

This section provides additional detail on the issuance of the certificate in response to the Request for Certificate message.

6.1 Certificates as a Final Approval of Application for Service

Upon approving a certificate application and a request for certificate message pursuant to this CPS, CREN issues a certificate. The issuance of a certificate indicates a complete and final approval of the certificate application by CREN. The certificate is deemed to be a valid certificate upon the subscriber's acceptance of it as described in this CPS.

6.2 Consent by Subscriber for Issuance of CREN Certificate

CREN shall not issue certificates without the certificate applicant's consent. Consent to issue is presumed from applicant's submission of an application notwithstanding the fact that acceptance of a certificate has not yet occurred.

6.3 Refusal to Issue a Certificate

CREN may refuse to issue a certificate in response to a request for certificate to any organization or person, at its sole discretion, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Upon CREN's refusal to issue a certificate, CREN shall promptly refund to any certificate

applicant any paid fees for the service, unless the certificate applicant submitted fraudulent or falsified information to CREN.

6.4 Representations upon Certificate Issuance

6.4.1 CREN's Representations to Subscriber

Unless otherwise provided in this CPS, CREN promises to the subscriber named in the certificate that:

(a) There are no misrepresentations of fact in the certificate originating from CREN,

(b) There are no data transcription errors as received by CREN from the certificate applicant resulting from a failure of CREN to exercise reasonable care in creating the certificate, and

(c) The certificate meets all material requirements of this CPS.

Unless otherwise provided in this CPS, CREN promises to the subscriber to make reasonable efforts, consistent with the terms of this CPS:

(a) To promptly revoke or suspend certificates in accordance with this CPS, and

(b) To notify the subscriber of any facts known to it that materially affect the validity and reliability of the certificate it issued to such subscriber.

The obligations and representations made in this section of the CPS are made and undertaken solely for the benefit of the subscriber and are not intended to benefit or be enforceable by any other party.

CREN will be deemed to have made reasonable efforts for purposes of this CPS section if its conduct substantially complies with this CPS and applicable law.

6.4.2 CREN's Representations to Relying Parties

By issuing a certificate, CREN represents to all who reasonably rely on a digital signature verifiable by the public key listed in the certificate that CREN has substantially complied with the CPS when issuing the certificate.

6.5 CREN's Representations upon Publication

By publishing a certificate, CREN certifies to all who reasonably rely on the information contained in the certificate that it has issued the certificate to the subscriber and that the subscriber has accepted the certificate.

6.6 Limitations on CREN's Representations

All representations in the above sections related to issuance of certificates are subject to the disclaimers of warranty and limitations of liability found elsewhere in this CPS.

6.7 Time of Certificate Issuance

CREN shall make reasonable efforts to confirm certificate application information and issue subscriber certificates once all relevant information is received by CREN within one to seven business days. This timeframe depends upon a certificate applicant's timely submission of complete and accurate information, and responsiveness to any CREN administrative requests, including the provision of appropriate and accurate payment information and approval.

6.8 Certificate Validity and Operational Periods

After issuance by CREN, all certificates shall be considered valid upon acceptance by the subscriber. The standard operational period for a CREN certificate shall be two years, subject to earlier termination of the operational period due to suspension or revocation. All certificates begin their operational period at the date and time of issuance, unless a later date and time (no later than sixty (60) days after the date of issue) is indicated in the certificate. The operational period begins at this date and time even if the certificate has not yet been accepted and is therefore not yet valid.

7.0 Acceptance of Certificates by Subscribers

This section describes the status and process of an institutional subscriber accepting the CREN issued digital certificate.

7.1 Certificate Acceptance

A subscriber is deemed to have accepted a certificate when, following communication of the certificate request to CREN, and the issuance of a certificate, when the certificate applicant responds explicitly in a signed secure email message to accept the certificate.. The certificate applicant must notify CREN of any inaccuracy or defect in a certificate promptly after receipt of the certificate.

7.2 Representations by Subscriber upon Acceptance of a CREN Certificate

By accepting a certificate issued by CREN, the subscriber certifies to and agrees with CREN and to all whom reasonably rely on the information contained in the certificate that at the time of acceptance and throughout the operational period of the certificate, until notified otherwise by the subscriber:

(a) each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of the subscriber and the certificate has been accepted and is operational (not expired, suspended or revoked) at the time the digital signature is created,

(b) no unauthorized person has ever had access to the subscriber's private key,

(c) all representations made by the subscriber to CREN regarding the information contained in the certificate are true,

(d) all information contained in the certificate is true to the extent that the subscriber had knowledge or notice of such information and will promptly notify CREN of any material inaccuracies in such information as required in this CPS, and

(e) the certificate is being used exclusively for authorized and legal purposes, consistent with this CPS.

By accepting a certificate, the subscriber acknowledges that the institution agrees to the terms and conditions contained in this CPS and the applicable subscriber agreement.

7.3 Subscriber Duty to Prevent Private Key Disclosure

By accepting a certificate, the subscriber assumes a duty to retain control of the institution subscriber's private key, to use a trustworthy system, and to take reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.

7.4 Indemnity by Subscriber

By accepting a certificate the subscriber agrees to indemnify and hold CREN and its agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that CREN and its agents and contractors may incur, that are caused by the use or publication of a certificate, and that arises from (i) falsehood or misrepresentation of fact by the subscriber or a person acting upon instructions from anyone authorized by the subscriber; (ii) failure by the subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive CREN or any person receiving or relying on the certificate; or (iii) failure to protect the

subscriber's private key, to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's private key.

7.5 Publication

Upon the subscriber's acceptance of the certificate, CREN shall publish a copy of the certificate in the CREN Repository. Subscribers may publish their CREN Certificate in other repositories.

8.0 Use of Certificates

This section describes the uses of certificates by subscribers and relying parties.

8.1 Effect on Subscribers and Relying Parties

All subscribers and relying parties are governed by this CPS, and in particular those found in this section of the CPS. Subscribers and relying parties are deemed to have agreed on this CPS effective:

(a) Upon submission of an application for a certificate, in the case of a subscriber; and

(b) Upon reliance of a certificate or a digital signature verifiable with reference to a public key listed in the certificate, in the case of a recipient of a certificate or a relying party.

8.2 Verification of Digital Signatures

Verification of a digital signature is undertaken to determine that (i) the digital signature was created by the private key corresponding to the public key listed in the signer's certificate and that (ii) the associated message has not been altered since the digital signature was created. Such verification shall be undertaken as follows:

(a) **Establishing a certificate chain for the digital signature** – A digital signature shall be verified with regard to a successful confirmation of certificate chain.

(b) **Checking the CREN (or other) repository for revocation or suspension of certificates in the chain** – The recipient must determine if any of the certificates along the chain from the signer to an acceptable root have been revoked or suspended, because a revocation or suspension has the effect of prematurely terminating the operational period during which verifiable digital signatures can be created. This may be ascertained in two different ways. The CREN repository may be queried for the most up-to-date revocation status. Alternatively, Certificate Revocation Lists (CRLs) may have been provided in the certificate chain. These CRLs may be used to determine the revocation status of certificates in the chain.

(c) **Delimiting data to which digital signatures are attached** – In order to verify a digital signature, it is necessary to know precisely what data has been signed. In the case of public key cryptography standards (PKCS), a standard signed message format is specified to accurately denote the signed data.

(d) **Indicating digital signature time and date of creation** – In order for a digital signature to support nonrepudiation, the data to which the corresponding digital signature is attached must include a time stamp. The time stamp shall reflect the date and time the digital signature is affixed.

(e) **Establishing the assurances intended by its signer** – Various technical means may be used to determine the purpose (or meaning) of the digital signature intended by its signer.

(f) **Ensuring that no certificates in the chain limit the use of the subscriber's certificate** – A certificate issuer (including CREN) may limit the purposes for which a private key corresponding to a certificate it issues may be used. Such limitations are indicated or incorporated by reference in the certificate and provide a means to warn recipients of situations for which reliance upon the certificate would not be considered reasonable. Persons validating certificates must inspect certificate contents for such warnings and limitations to ensure that no certificate in the chain denies the use of the certificate as otherwise desired by the recipient.

8.3 Effect of Validating a Subscriber Certificate

A digital signature is binding against its maker if:

(a) It was created during the operational period of a valid certificate,

(b) Such digital signature can be properly verified by confirmation of certificate chain,

(c) The relying party has no knowledge or notice of a breach of the requirements of this CPS by the signer, and

(d) The relying party has complied with all requirements of this CPS.

8.4 Authority Not Implied in Certificate

The use of certificates does not convey evidence of authority on the part of any user to act on behalf of any person or to undertake any particular act. Verifiers of digitally signed messages are solely responsible for exercising due diligence and reasonable judgment before relying on certificates and digital signatures. A certificate is not a grant from CREN of any rights or privileges, except as specifically provided in this CPS.

8.5 Procedures upon Failure of Digital Signature Verification

A person relying on an unverifiable digital signature assumes all risks with regard to it and is not entitled to any presumption that the digital signature is effective as the signature of the institutional subscriber.

8.6 Reliance on Digital Signatures

A recipient of a message signed by a digital signature of an institutional subscriber may rely upon that digital signature as binding against the subscriber if:

(a) The digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate chain, and

(b) Such reliance is reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the relying party must obtain such assurances for such reliance to be reasonable.

8.7 Writings and Signatures

A message bearing a digital signature verified by the public key listed in a valid certificate is as valid,

effective, and enforceable as if the message had been written and signed on paper. Where a rule of law or applicable practice requires a signature or provides for certain consequences in the absence of a signature, that rule is satisfied in relation to a message by a digital signature affixed by a signer with the intention of signing a message and subsequently verified by reference to the public key listed in a valid certificate.

9.0 Phase 4: Certificate Suspension and Revocation

This section describes the processes and reasons for certificate suspension and revocation.

9.1 General Reasons for Suspension or Revocation

A certificate shall be suspended or revoked if:

(a) There has been a loss, theft, modification, unauthorized disclosure, or other compromise of the private key of the certificate's institutional subject,

(b) The certificate's institutional subscriber has breached a material obligation under this CPS,

(c) If CREN discovers and confirms that the certificate was not issued in accordance with the procedures required by this CPS, a certificate may be suspended while CREN investigates to confirm grounds for revocation, or

(d) The performance of a person's obligations under this CPS is delayed or prevented by an act of God; natural disaster; computer or communications failure; change in statute, regulation, or other law; official government action, including but not limited to acts by agencies responsible for export control administration; or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised.

9.2 Termination of a Suspension of a Certificate

CREN shall terminate a certificate suspension (thereby reinstating the certificate), if:

(a) The institutional subscriber requests it and CREN confirms the identity of the institutional representatives according to the procedures in this CPS and the Operations and Procedures Document,

(b) CREN determines that the request for suspension was made without the institutional subscriber's authorization, or

(c) CREN determines that the reasons for the suspension were unfounded.

9.3 Revocation at Institutional Subscriber's Request

CREN must revoke a certificate upon the request of an institutional subscriber once it has confirmed that the person requesting the revocation is in fact the valid representative of the institutional subscriber.

9.4 Effect of Suspension or Revocation

During suspension, or permanently upon revocation of an institutional subscriber's certificate:

(a) That certificate's operational period shall immediately be considered terminated;

(b) The underlying contractual obligations created or communicated under this CPS shall be unaffected by the suspension or revocation;

(c) Private keys corresponding to public keys contained in suspended or revoked certificates shall be safeguarded by the subscriber in a trustworthy manner throughout the period of suspension and, upon revocation for the applicable retention period, unless destroyed.

10.0 Phase 5: Certificate Expiration and Renewal

This section provides additional detail on certificate expiration processes.

10.1 Notice Prior to Expiration

CREN will make a reasonable effort to notify subscribers, via E-mail, of the impending expiration of their certificates. Such notice is intended solely for the convenience of the subscriber in the re-enrollment or renewal process, whichever is applicable.

10.2 Effect of Certificate Expiration on Underlying Obligations

Expiration of a certificate shall not affect the validity of any underlying contractual obligations created or communicated under this CPS.

10.3 Re-enrollment and Subscriber Renewal

Subscriber renewal and re-enrollment shall be initiated by providing only new or changed information from the initial application or any subsequent renewal. Requirements for renewal and re-enrollment are subject to change at CREN's discretion. Up-to-date requirements for re-enrollment and renewal are generally accessible from the CREN repository at **http://www.cren.net** or by contacting the CREN office.

11.0 Obligations of CREN and Limitations on such Obligations

This section provides additional detail on CREN's obligations and the limitations on those obligations.

11.1 Limited Warranties and Other Obligations

CREN warrants and promises:

(a) To provide the infrastructure and certification services, including the establishment and operation of the CREN repository, as described in this CPS,

(b) To perform the application validation procedures for certificates as set forth in this CPS,

(c) To issue certificates in accordance with this CPS and honor the various representations to subscribers and to relying parties presented in this CPS,

(d) To publish accepted certificates in accordance with this CPS,

(e) To suspend and revoke certificates as required by this CPS,

(f) To provide for the expiration, re-enrollment, and renewal of certificates as stated in this CPS,

(g) That its own private key has not been compromised unless CREN provides notice to the contrary via the CREN repository.

(h) CREN makes no other warranties and has no further obligations under this CPS.

11.2 Disclaimers and Limitations on Obligations of CREN

Except as expressly provided in the preceding paragraph, CREN disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided, and further disclaims any and all liability for negligence and lack of reasonable care.

Except as expressly stated in this Section of the CPS, CREN:

(a) Does not warrant the accuracy, authenticity, reliability, completeness, currentness, merchantability, or fitness of any information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of CREN,

(b) Shall not incur liability for representations of information contained in a certificate, provided the certificate content substantially complies with this CPS,

(c) (3)Does not warrant "nonrepudiation" of any certificate or message (because nonrepudiation is determined exclusively by law and the applicable dispute resolution mechanism), and

(d) Does not warrant any software.

11.3 Exclusion of Certain Elements of Damages

In no event shall CREN be liable for any indirect, special, incidental, or consequential damages, or for any loss of profits, loss of data, or other indirect, consequential, or punitive damages, arising from or in connection with the use, delivery, license, performance, or nonperformance of certificates, digital signatures, or any other transactions or services offered or contemplated by this CPS, even if CREN has been advised of the possibility of such damages.

11.4 Damage and Loss Limitations

In no event will the aggregate liability of CREN to all parties (including without limitation a subscriber, an applicant, a recipient, or a relying party) exceed $20,000.

This limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, special, consequential, exemplary, or incidental damages incurred by any person, including without limitation a subscriber, an applicant, a recipient, or a relying party, that are caused by reliance on or use of a certificate CREN issues, manages, uses, suspends or revokes, or a certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim. The liability cap on each certificate shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. In the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall CREN be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.

11.5 Subscriber Liability to Relying Parties

Without limiting other subscriber obligations stated in this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one or more digital signatures

with the certificate, reasonably rely on the representations contained therein.

11.6 No Fiduciary Relationship

CREN is not an agent, fiduciary, trustee, or other representative of subscribers or relying parties. The relationship between CREN and subscribers and that between CREN and relying parties is not that of agent and principal. Neither subscribers nor relying parties have any authority to bind CREN, by contract or otherwise, to any obligation. CREN shall make no representations to the contrary, either expressly, implicitly, by appearance, or otherwise.

12.0 Miscellaneous Provisions of the CPS

This section describes other miscellaneous provisions of this CPS.

12.1 Conflict of Provisions

In the event of a conflict between this CPS and other rules, guidelines, or contracts, this CPS would govern, except where another contract with CREN states that that contract supercedes the terms of this CPS or to the extent of any provisions of this CPS that are prohibited by law.

12.2 Compliance with Export Laws and Regulations

Export of certain software used in conjunction with this CPS may require approval of appropriate government authorities. All parties who may be exporting any software used in conjunction with this CPS shall conform to applicable export laws and regulations.

12.3 Governing Law

The enforceability, construction, interpretation, and validity of this CPS shall be governed by the laws of the Commonwealth of Virginia, USA (without regard to any conflicts of laws which might result in the application of the laws of any other jurisdiction). This choice of law is made to ensure uniform procedures and interpretation for all users, no matter where they reside or use their certificates. See also Section 12.7.

12.4 Dispute Resolution, Choice of Forum, and Presumptions

12.4.1 Notification among Parties to a Dispute

Before invoking any dispute resolution mechanism (including litigation as detailed below) with respect to a dispute involving any aspect of this CPS or a certificate issued by CREN, aggrieved persons shall notify the other party or parties for the purpose of seeking dispute resolution among themselves.

12.4.2 Distinguished Panel of Experts

If the dispute is not resolved within thirty (30) days after initial notice as provided in the previous paragraph, then a party may submit the dispute in written or electronic form to CREN. In response, CREN will convene a CREN Distinguished Panel of Experts (CDPE), composed of three PKI experts, to assemble relevant facts with the goal of facilitating dispute resolution. The submitting party must deliver a copy of the submittal to all other parties. Any party that did not submit the matter may provide appropriate information to the CDPE within one (1) week after the date the dispute was submitted to the CDPE. The CDPE shall complete and communicate its recommendations to the parties within three (3) weeks (unless the parties mutually agree to

extend this period for a specified additional period) after the matter was initially submitted to the CDPE. The CDPE will generally operate via E-mail, teleconferencing, courier and postal mail. The recommendations of the CDPE shall not be binding upon the parties.

12.5 Merger

No term or provision of this CPS directly affecting the respective rights and obligations of CREN may be orally amended, waived, supplemented, modified, or terminated, except by an authenticated message or document of such affected party, except to the extent provided otherwise herein.

12.6 Severability

If any provision of this CPS, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted so as best to reasonably effect the intent of its parties. It is expressly understood and agreed that each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

12.7 No Waiver

Failure by any person to enforce a provision of this CPS will not be deemed a waiver of future enforcement of that or any other provision.

12.8 Notice

Whenever any person hereto desires or is required to give any notice, demand, or request with respect to this CPS, such communication shall be made either using digitally signed messages consistent with the requirements of this CPS, or in writing. Electronic communications shall be effective upon the sender's receiving a valid, digitally signed acknowledgment of receipt from the recipient. Such acknowledgment must be received within five (5) days, or else written notice must then be communicated. Communications in writing must be delivered by a courier service that confirms delivery in writing or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows:

CREN

Current address of CREN, as listed on the CREN web site at http://www.cren.net.)

Attn: Certification Services

12.9 Amendment of CPS

12.9.1 Amendments Generally

CREN shall be entitled to amend this CPS from time to time (prospectively and not retroactively). CREN shall be entitled to make amendments either in the form of an amended version of the CPS or in the Operations and Procedures for Institutions Document at the CREN CA Web Site. A material amendment to the CPS shall become effective fifteen (15) days after CREN publishes the amendment in the CREN repository in accordance with this CPS.

12.9.2 Material Amendments Exception

If, notwithstanding the preceding paragraph, CREN publishes a material amendment to the CPS, it shall become effective immediately upon publication in the CREN repository if failure by CREN to make the amendment may result in a compromise of CREN's Certificate Authority or the Certificate Authority structure.

12.9.3 Non-Material Amendments

An amendment to the CPS that is non-material shall become effective immediately upon publication in the CREN repository. CREN's decision to designate an amendment as non-material shall be within CREN's sole discretion.

12. 9.4 Assent to Amendments

A certificate applicant and subscriber's decision not to request revocation of its certificate within fifteen (15) days following the publication of an amendment shall constitute agreement to the amendment.

12.10 CREN Property

The following shall be the personal property of CREN:

(a) All certificates issued by CREN. Certificates issued by CREN may contain a copyright notice with CREN's name included. Permission is hereby granted to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full.

(b) This CPS.

(c) CREN's public and private keys regardless of the physical medium within which they are stored and protected.

(d) The Operations and Procedures for Institutions Document.

12.11 Subscriber Property

The following shall be the personal property of each individual subscriber:

(a) The private key for such subscriber regardless of the physical medium within which it is stored and protected.

(b) The public key for such subscriber regardless of the physical medium within which it is stored and protected.

12.12 Infringement and Other Damaging Material

Certificate applicants (and, upon acceptance, subscribers) represent and warrant that their submission to CREN and use of a domain and distinguished name (and all other certificate application information) does not interfere with or infringe upon the rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortuous interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated. Certificate applicants (and, upon acceptance, subscribers) shall defend, indemnify, and hold CREN harmless for any loss or damage resulting from any such interference or infringement.

CREN shall not be responsible for non-verified subscriber information submitted to CREN or otherwise submitted for inclusion in a certificate. In particular, subscribers shall be solely responsible for the legality of the information they present for use in certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed. Because laws regarding the transmission and availability of information content are constantly changing and vary widely, certificate applicants' and subscribers' responsibilities are determined not only by laws in existence at the time CREN issues a certificate to a certificate applicant institution, but also by any laws that may be enacted after such date. Certificate applicant institutions and subscribers should be aware that there are many laws regarding the transmission of data, especially data that is encrypted or involves encryption algorithms, and that these laws may vary dramatically from state to state and country to country. Further, it is generally not possible to limit the distribution of content on the Internet or certain other networks based on the locality of the user/viewer, and this may require certificate applicants and subscribers to comply with the laws of each jurisdiction in which the content may be viewed or used.

Certificate applicant institutions and subscribers will not submit to CREN any materials that contain statements that (i) are libelous, defamatory, obscene, pornographic, abusive, bigoted, hateful, or racially offensive, (ii) advocate illegal activity or discuss illegal activities with the intent to commit them, or (iii) otherwise violate any law.

12.13 Fees

CREN may charge subscribers fees for their use of CREN's services. A current schedule of such fees is available from the CREN web site at **http://www.cren.net.** Such fees are subject to reexamination.

12.14 Choice of Cryptographic Methods

All persons acknowledge that they (not CREN) are solely responsible for and have exercised independent judgment in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques.

12.15 Survival

Termination of this CPS shall not terminate any obligations of any party under this CPS as required to give the full term and affect to the obligations. Without limiting the generality of the foregoing, any provisions related to confidential information, audit rights and dispute resolution shall survive the termination of this CPS.

12.16 Force Majeure

CREN shall not be responsible for any breach of warranty, delay, or failure in performance under this CPS that results from events beyond its control, such as acts of God, acts of war, epidemics, power outages, fire, earthquakes, and other disasters.

12.17 Conflicts of Law.

Notwithstanding anything to the contrary in this CPS, if the laws of any state of the United States or the law of the United States governing a Subscriber (including but not limited to any laws related to choice of law) ("Subscriber Governing Laws") forbid the inclusion of specific provisions of this CPS, then with respect to that

Subscriber only, the specific provision of this CPS shall be deemed null and void as if not included at all. However, wherever possible within the letter and spirit of the Subscriber Governing Laws, rather than causing a provision of this CPS to be null and void pursuant to the prior sentence, all Subscriber Governing Laws will be interpreted in such a way as to achieve the letter and spirit of this CPS. Where a conflict cannot be resolved between this CPS and a Subscriber Governing Law, that Subscriber Governing Law shall prevail.