



INFORMATION SECURITY

HIGH PERFORMANCE COMPUTING VIRTUAL
LABORATORY
ENTRUST CA
Certificate Policy Version 1.0

Date: **October 8, 2004**

DOCUMENT VERSION CONTROL

VERSION	DATE	AUTHOR(S)	DESCRIPTION	REASON FOR CHANGE
0.1	12 September 2003	T. Sexsmith, Entrust	Initial draft	
0.2	21 April 2004	M. Staveley HPCVL	HPCVL details / customization	Update
0.3	27 September 2004	C. Dafnas HPCVL	HPCVL details / customization	Update
1.0	8 October 2004	C. Dafnas HPCVL	HPCVL details / customization	Update

TABLE OF CONTENTS

1. INTRODUCTION.....	1
1.1 OVERVIEW.....	1
1.2 IDENTIFICATION.....	2
1.3 COMMUNITY AND APPLICABILITY	2
1.3.1 PKI Authorities.....	3
1.3.2 Registration Authorities	5
1.3.3 End Entities	5
1.3.4 Applicability	6
1.4 CONTACT DETAILS.....	6
1.4.1 Specification Administration Organization	6
1.4.2 Contact Person.....	6
1.4.3 Person Determining CPS Suitability for the Policy	7
2. GENERAL PROVISIONS	8
2.1 OBLIGATIONS.....	8
2.1.1 Certification Authority Obligations	8
2.1.2 Registration Authority Obligations	8
2.1.3 Subscriber Obligations	9
2.1.4 Relying Party Obligations	11
2.1.5 Repository Obligations	12
2.2 LIABILITY.....	12
2.2.1 Certification Authority and Registration Authority Liability	13
2.3 FINANCIAL RESPONSIBILITY	14
2.3.1 Indemnification by Relying Parties	15
2.3.2 Fiduciary Relationships	15
2.3.3 Administrative Processes	15
2.4 INTERPRETATION AND ENFORCEMENT.....	15
2.4.1 Governing Law	15
2.4.2 Severability, Survival, Merger, Notice	15

2.4.3	Dispute Resolution Procedures.....	15
2.5	FEES.....	15
2.5.1	Certificate Issuance or Renewal Fees.....	16
2.5.2	Certificate Access Fees.....	16
2.5.3	Revocation or Status Information Access Fees.....	16
2.5.4	Fees for Other Services such as Policy Information.....	16
2.5.5	Refund Policy	16
2.6	PUBLICATION AND REPOSITORY	16
2.6.1	Publication of Certification Authority Information.....	16
2.6.2	Frequency of Publication	16
2.6.3	Access Controls	16
2.6.4	Repositories	17
2.7	COMPLIANCE AUDIT.....	17
2.7.1	Frequency of Entity Compliance Audit	17
2.7.2	Identity/Qualifications of Auditor	17
2.7.3	Auditor's Relationship to Audited Party	17
2.7.4	Topics Covered by Audit	17
2.7.5	Actions Taken as a Result of Deficiency	17
2.7.6	Communication of Results	18
2.8	CONFIDENTIALITY	18
2.8.1	Types of Information to be Kept Confidential	18
2.8.2	Types of Information not Considered Confidential	18
2.8.3	Disclosure of Certificate Revocation/Suspension Information.....	19
2.8.4	Release to Law Enforcement Officials.....	19
2.8.5	Release as Part of Civil Discovery	19
2.8.6	Disclosure upon Owner's Request	19
2.8.7	Other Information Release Circumstances.....	19
2.9	INTELLECTUAL PROPERTY RIGHTS.....	19
3.	IDENTIFICATION AND AUTHENTICATION.....	21
3.1	INITIAL REGISTRATION	21

3.1.1	Types of Names	21
3.1.2	Need for Names to be Meaningful.....	21
3.1.3	Rules for Interpreting Various Name Forms	21
3.1.4	Uniqueness of Names	21
3.1.5	Name Claim Dispute Resolution Procedure	21
3.1.6	Recognition, Authentication and Role of Trademarks	22
3.1.7	Method to Prove Possession of Private Key	22
3.1.8	Authentication of Organization Identity.....	22
3.1.9	Authentication of Individual Identity	22
3.2	ROUTINE REKEY	23
3.3	REKEY AFTER REVOCATION	23
3.4	REVOCATION REQUEST	23
4.	OPERATIONAL REQUIREMENTS	25
4.1	CERTIFICATE APPLICATION	25
4.2	CERTIFICATE ISSUANCE	25
4.3	CERTIFICATE ACCEPTANCE	26
4.4	CERTIFICATE SUSPENSION AND REVOCATION.....	26
4.4.1	Circumstances for Revocation.....	26
4.4.2	Who can Request Revocation.....	26
4.4.3	Procedure for Revocation Request	26
4.4.4	Revocation Request Grace Period.....	26
4.4.5	Circumstances for Suspension.....	27
4.4.6	Who can Request Suspension	27
4.4.7	Procedure for Suspension Request	27
4.4.8	Limits on Suspension Period.....	27
4.4.9	Certificate Revocation List Issuance Frequency	27
4.4.10	Certificate Revocation List Checking Requirements	27
4.4.11	On-line Revocation/Status Checking Availability.....	27
4.4.12	On-line Revocation Checking Requirements.....	27
4.4.13	Other Forms of Revocation Advertisements Available	28

4.4.14	Checking Requirements for Other Forms of Revocation Advertisements	28
4.4.15	Special Requirements re Key Compromise.....	28
4.5	SECURITY AUDIT PROCEDURES	28
4.5.1	Types of Event Recorded	28
4.5.2	Frequency of Processing Log.....	29
4.5.3	Retention Period for Audit Log	29
4.5.4	Protection of Audit Log	29
4.5.5	Audit Log Backup Procedures.....	29
4.5.6	Audit Collection System	29
4.5.7	Notification to Event-Causing Subject	29
4.5.8	Vulnerability Assessments	29
4.6	RECORDS ARCHIVAL	30
4.6.1	Types of Event Recorded.....	30
4.6.2	Retention Period for Archive.....	30
4.6.3	Protection of Archive	30
4.6.4	Archive Backup Procedures	30
4.6.5	Requirements for Time-Stamping of Records	30
4.6.6	Archive Collection System.....	30
4.6.7	Procedures to Obtain and Verify Archive Information	31
4.7	KEY CHANGEOVER	31
4.8	COMPROMISE AND DISASTER RECOVERY.....	31
4.8.1	Computing Resources, Software, and/or Data are Corrupted.....	31
4.8.2	Entity Public Key is Revoked.....	31
4.8.3	Entity Key is Compromised	31
4.8.4	Secure Facility after a Natural or Other Type of Disaster.....	31
4.9	CERTIFICATION AUTHORITY TERMINATION	31
5.	PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS.....	32
5.1	PHYSICAL CONTROLS	32
5.1.1	Site Location and Construction	32
5.1.2	Physical Access	32

5.1.3	Power and Air Conditioning.....	33
5.1.4	Water Exposures.....	33
5.1.5	Fire Prevention and Protection.....	33
5.1.6	Media Storage.....	33
5.1.7	Waste Disposal.....	33
5.1.8	Off-site Backup.....	33
5.2	PROCEDURAL CONTROLS.....	34
5.2.1	Trusted Roles.....	34
5.2.2	Number of Persons Required per Task.....	35
5.2.3	Identification and Authentication for Each Role.....	35
5.3	PERSONNEL CONTROLS.....	35
5.3.1	Background, Qualifications, Experience, and Clearance Requirements.....	35
5.3.2	Background Check Procedures.....	36
5.3.3	Training Requirements.....	36
5.3.4	Retraining Frequency and Requirements.....	36
5.3.5	Job Rotation Frequency and Sequence.....	36
5.3.6	Sanctions for Unauthorized Actions.....	36
5.3.7	Contracting Personnel Requirements.....	36
5.3.8	Documentation Supplied to Personnel.....	37
6.	TECHNICAL SECURITY CONTROLS.....	38
6.1	KEY PAIR GENERATION AND INSTALLATION.....	38
6.1.1	Key Pair Generation.....	38
6.1.2	Private Key Delivery to Entity.....	38
6.1.3	Public Key Delivery to Certificate Issuer.....	38
6.1.4	Certification Authority Public Key Delivery to Users.....	38
6.1.5	Key Sizes.....	38
6.1.6	Public Key Parameters Generation.....	39
6.1.7	Parameter Quality Checking.....	39
6.1.8	Hardware/Software Key Generation.....	39
6.1.9	Key Usage Purposes.....	39

6.2 PRIVATE KEY PROTECTION	39
6.2.1 Standards for Cryptographic Module.....	39
6.2.2 Private Key Multi-Person Control	39
6.2.3 Private Key Escrow	39
6.2.4 Private Key Backup	40
6.2.5 Private Key Archival	40
6.2.6 Private Key Entry into Cryptographic Module.....	40
6.2.7 Method of Activating Private Key	40
6.2.8 Method of Deactivating Private Key	40
6.2.9 Method of Destroying Private Key	40
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	41
6.3.1 Public Key Archival.....	41
6.3.2 Usage Periods for the Public and Private Keys.....	41
6.4 ACTIVATION DATA	41
6.4.1 Activation Data Generation and Installation	41
6.4.2 Activation Data Protection	41
6.4.3 Other Aspects of Activation Data.....	42
6.5 COMPUTER SECURITY CONTROLS	42
6.5.1 Specific Computer Security Technical Requirements	42
6.5.2 Computer Security Rating	42
6.6 LIFE CYCLE TECHNICAL CONTROLS	42
6.6.1 System Development Controls.....	42
6.6.2 Security Management Controls	43
6.6.3 Life Cycle Security Ratings	43
6.7 NETWORK SECURITY CONTROLS.....	43
6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS	43
7. CERTIFICATE AND CERTIFICATE REVOCATION LIST PROFILES	44
7.1 CERTIFICATE PROFILE	44
7.1.1 Version Number	44
7.1.2 Certificate Extensions.....	44

7.1.3	Algorithm Object Identifiers	44
7.1.4	Name Forms.....	45
7.1.5	Name Constraints.....	45
7.1.6	Certificate Policy Object Identifier.....	45
7.1.7	Usage of Policy Constraints Extension.....	45
7.1.8	Policy Qualifiers Syntax and Semantics.....	45
7.1.9	Processing Semantics for the Critical Policy Extension	45
7.2	CERTIFICATE REVOCATION LIST PROFILE	45
7.2.1	Version Number	45
7.2.2	CRL and CRL Entry Extensions	45
8.	SPECIFICATION ADMINISTRATION	46
8.1	SPECIFICATION CHANGE PROCEDURES.....	46
8.2	PUBLICATION AND NOTIFICATION POLICIES.....	46
8.3	CERTIFICATION PRACTICE STATEMENT APPROVAL PROCEDURES	46

LIST OF TABLES

Table 1.1 PKI and Entrust Roles.....	2
Table 6.1 Key Lifetimes	41
Table 7.1 Signature OIDs	44
Table 7.2 Algorithm OIDs	44

1. INTRODUCTION

1.1 OVERVIEW

The High Performance Computing Virtual Laboratory has implemented a Public Key Infrastructure (PKI), based on Entrust Authority™ Security Manager®, to increase the security posture of the organization and to support secure communications. The PKI consists of products and services that provide and manage X.509 public key certificates. The PKI binds its Subscribers (Subscriber is defined in §1.3.3.1) to public/private key pairs through the use of these X.509 certificates. Public key certificates identify the Subscriber named in the certificate and bind that identity to a public key embedded in the certificate. Every public key certificate issued by the High Performance Computing Virtual Laboratory Certification Authority (CA) and asserting one of the policies listed in §1.2 shall be issued under the applicable requirements of this Certificate Policy (CP).

The PKI consists of a self-signed CA, a repository, and the Registration Authorities (RAs), Local Registration Authorities (LRAs) and Subscribers associated with the CA. The CA will act as the Principal CA for cross certification with other CAs to achieve interoperability with other entity PKIs.

The PKI has a Board of Trustees herein referred to as the Policy Management Authority (PMA) who is responsible for the selection/definition of certificate policies for the organization, approval of any cross-certification agreements with external CAs and review of the High Performance Computing Virtual Laboratory Certification Practice Statement (CPS) to ensure consistency with the certificate policies.

The PKI has an Operations Authority (OA) that is overseen by the Executive Director. The OA is responsible for interpretation of the certificate policies as stated by the PMA, creation and management of the CPS, and the correct operation of the CA. The OA manages the overall operations of the CA and is responsible for the day-to-day operation of the CA.

This CP is managed by the Policy Authority (PA) and adheres to the High Performance Computing Virtual Laboratory Security Policy. Overall responsibility for the PKI is assigned to the High Performance Computing Virtual Laboratory PKI Management Authority (PMA).

Throughout this document, references to:

- “the PKI” mean the High Performance Computing Virtual Laboratory Public Key Infrastructure;
- “the CA” mean the High Performance Computing Virtual Laboratory Certification Authority;
- “the Repository” mean the High Performance Computing Virtual Laboratory Repository;
- “the RA” mean the High Performance Computing Virtual Laboratory Registration Authority;
- “the LRA” mean a authorized Local Registration Authority of the High Performance Computing Virtual Laboratory CA;
- “the PMA” mean the High Performance Computing Virtual Laboratory PKI Management Authority;
- “the PA” mean the High Performance Computing Virtual Laboratory Policy Authority;
- “the OA” mean the High Performance Computing Virtual Laboratory Operations Authority;

- “the CP” mean the High Performance Computing Virtual Laboratory Certificate Policy;
- “the CPS” mean the High Performance Computing Virtual Laboratory Certification Practice Statement;
- “certificate” mean a certificate issued by the High Performance Computing Virtual Laboratory CA; and
- “Subscriber” mean the holder of a certificate issued by the High Performance Computing Virtual Laboratory CA.

This CP is for use by all entities with relationships with the CA, including End-Entities and Registration Authorities undertaking to adhere to this CP.

This CP is binding on the CA, and governs its performance with respect to all Certificates it issues. Specific practices and procedures by which the CA implements the requirements of this CP are maintained in a Certification Practice Statement (CPS), which is approved by the PA and made available to Subscribers and Relying Parties.

This CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527 “Certificate Policy and Certification Practice Statement Framework”.

1.2 IDENTIFICATION

This document is called the “High Performance Computing Virtual Laboratory Entrust CA Certificate Policy Version 1.0”

1.3 COMMUNITY AND APPLICABILITY

This CP describes the terms and conditions under which High Performance Computing Virtual Laboratory makes CA and RA services available in respect to certificates; it is applicable to all persons, entities, and organizations that have a relationship with

- High Performance Computing Virtual Laboratory in respect to certificates and/or any services provided by High Performance Computing Virtual Laboratory in respect to certificates; and
- RAs operating under the High Performance Computing Virtual Laboratory CA.

This CP provides a statement of the rights and obligations of High Performance Computing Virtual Laboratory, any third parties that are operating RAs under the CA, and any other persons, entities, or organizations that may use or rely on certificates or have a relationship with the CA or a RA operating under the CA in respect to certificates and/or any services in respect to certificates.

The following table illustrates the relationships of the High Performance Computing Virtual Laboratory individuals to PKI and Entrust roles:

Table 1.1 PKI and Entrust Roles

Individual	PKI Role	Entrust Role
<i>Chair, Board of Trustees</i>	PMA	N/A

Individual	PKI Role	Entrust Role
<i>Security Policy Advisory Committee</i>	PA	First Security Officer
<i>Executive Director</i>	OA	Master User
<i>Security Manager</i>	Entrust CA Administrator	Security Officer
<i>Security Specialist / Systems Administrator</i>	RA	Entrust Administrator
<i>Help Desk / Customer Service Representative</i>	LRA	Subset of Entrust Administrator
<i>HPCVL User / Certificate Subscriber</i>	Subscriber/Relying party	Subscriber

1.3.1 PKI Authorities

1.3.1.1 PKI Management Authority

The PKI Management Authority (PMA) is the *Board of Trustees*. The PMA is responsible for:

- Approval and sign-off of all CPs and CPSs pertaining to the CA;
- Approval and sign-off of all cross certifications by the CA with external entity CAs; and
- Execution of a Memorandum of Agreement (MOA) between the CA and an external entity CA. The MOA will set forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in this CP and those in the entity CA CP. Thus, the term “MOA” as used in this CP shall always refer to the Memorandum of Agreement cited in this paragraph.

1.3.1.2 Policy Authority

The Policy Authority (PA) is the *Security Policy Advisory Committee*. The PA is responsible for:

- Creation, maintenance, submission to the PMA, and publication of all CPs pertaining to the CA;
- Review for CP compliance and submission to the PMA of all CPSs pertaining to the CA;
- Review of the CA operations and assurance of continued conformance with the CPs and CPSs pertaining to the CA.
- Review and submission to the PMA of all recommended cross certifications by the CA with external entity CAs;
- Negotiation of a Memorandum of Agreement (MOA) between the CA and an external entity CA. The MOA will set forth the respective responsibilities and obligations of both parties,

and the mappings between the certificate levels of assurance contained in this CP and those in the entity CA CP. Thus, the term “MOA” as used in this CP shall always refer to the Memorandum of Agreement cited in this paragraph; and

- Review and assurance of continued conformance of all cross-certified entities with applicable requirements as set forth in the MOA as a condition for allowing continued cross certification with the CA.

1.3.1.3 Operations Authority

The Operations Authority (OA) is the organization that operates the CA and reports to the *Executive Director*. The OA is responsible for:

- Creation, submission to the PA, and maintenance of all CPSs pertaining to the CA;
- Creation and management of CA Operating Procedures ensuring that the practices that the CA employs in issuing certificates, as described in the CPS, are consistent with this CP; and
- Management of CA Operations, including all aspects of the issuance and management of a certificate, such as:
 - Control over the registration process;
 - The certificate manufacturing process;
 - Publication of certificates;
 - Revocation of certificates;
 - Generation and destruction of CA signing keys;
 - Rekey of CA; and
 - Ensuring that all aspects of CA services, operations and infrastructure related to certificates issued under this CP are in accordance with the requirements, representations, and warranties of this CP.

1.3.1.4 Certification Authority

The Certification Authority (CA) is responsible for:

- Creation, signing, distribution, and revocation of certificates binding the X.500 Distinguished Name of Subscribers and Registration Authorities with their respective signature verification key and their public encryption key;
- Delegation of limited authority to one or more Registration Authorities;
- Promulgation of certificate status through Certificate Revocation Lists (CRLs) and Authority Revocation Lists (ARLs); and
- Implementation and operation of its certification practices to achieve the requirements of this CP.

Only CAs approved by the PMA shall issue certificates under this CP. In the event that more than one CA is authorized to issue certificates, High Performance Computing Virtual Laboratory shall post a list of authorized CAs in the Repository.

Where necessary, this CP distinguishes the different users and roles accessing the CA functions. Where this distinction is not required, the term Certification Authority is used to refer to the total CA entity, including the hardware, software, personnel, processes, and its operations.

1.3.2 Registration Authorities

Registration Authorities (RAs) are appointed by the OA and are responsible for the verification and processing of subscriber applications received from the LRAs in accordance with this CP.

Only RAs authorized by the OA shall submit requests to the CA for the issuance of certificates. In the event that more than one RA is authorized to perform this function, High Performance Computing Virtual Laboratory shall post a list of authorized RAs in the Repository.

1.3.2.1 Local Registration Authorities

Local RA (LRAs) are appointed by the RA and are responsible for the identification and authentication of End Entities in accordance with this CP.

1.3.3 End Entities

End Entities in the PKI consist of Subscribers, Relying Parties, hardware devices and/or specific applications. All End Entities are Subscribers. End Entities use certificates issued by the CA to encrypt information for and verify the digital signatures of other End Entities within the PKI for legitimate High Performance Computing Virtual Laboratory business use. As such, End Entities are also Relying Parties.

This CP is binding on each End Entity that applies for and obtains or relies certificates by virtue of a Subscriber Agreement or equivalent conditions in a contract. The CP governs each applicant's performance with respect to their application for, use of, and reliance on certificates.

1.3.3.1 Subscribers

To become a Subscriber of the CA a person, entity, or organization must apply for a certificate, during which time they are referred to as an Applicant. Subscribers to the CA include:

- High Performance Computing Virtual Laboratory full-time employees, part-time employees, contractors and temporaries;
- High Performance Computing Virtual Laboratory Customer full-time employees, part-time employees, contractors and temporaries;
- Other individuals with whom High Performance Computing Virtual Laboratory has a business relationship; and
- External cross-certified Certificate Authorities.

1.3.3.2 Relying Parties

The right to reasonably rely on certificates is limited to the following persons:

- Subscribers that are using approved applications, as defined in §1.3.4;
- Devices or applications utilizing certificates for authentication or to protect sensitive information; and

- External cross-certified CAs that have been approved by the PMA.

1.3.4 Applicability

Certificates issued under this CP are intended to support low to medium value data/transactions in high-risk network environments or data/transactions of moderate to high organizational or financial value in secure low risk network environments.

Certificates issued under this CP are appropriate for transactions that are official in nature, and for which there is a need for high confidence in the asserted electronic identity of the transacting party. In particular, an authentication error of a user's identity might result in:

- Significant inconvenience to any party; or
- Significant financial loss to any party; or
- Significant damage to any party's standing or reputation; or
- Significant distress being caused to any party; or
- Release of some personal information, High Performance Computing Virtual Laboratory sensitive information, or information commercially sensitive to third parties; and
- Significant risk that an egregious criminal act will occur in the transaction or that the transaction will assist materially in the commission or concealment of an egregious criminal act.

1.3.4.1 Authorized Applications

The certificates issued by the CA under this CP are to be used exclusively for applications authorized by the PMA.

1.3.4.2 Prohibited Applications

All applications not explicitly authorized for use with certificates by the PMA are prohibited.

1.4 CONTACT DETAILS

1.4.1 Specification Administration Organization

This CP is administered by the PA and is approved by the PMA.

1.4.2 Contact Person

The contact information for the PA is:

Costa Dafnas, CISSP

Research Computing Security Officer

High Performance Computing Virtual Laboratory

Queen's University HPCVL
993 Princess Street, Suite 115
PO Box 5
Kingston, Ontario
Canada K7L 1H3
Tel: (613) 533-2561
Fax: (613) 533-2015
Email: dafnasc@post.queensu.ca
Web: <http://www.hpcvl.org/>

1.4.3 Person Determining CPS Suitability for the Policy

The CPS is administered by the OA and is approved by the PMA. Suitability is determined by the PA prior to presentation to the PMA for approval

2. GENERAL PROVISIONS

2.1 OBLIGATIONS

2.1.1 Certification Authority Obligations

The CA shall conform to the stipulations of this CP, including:

- Providing to the PMA a CPS, as well as any subsequent changes, for conformance assessment;
- Conforming to the stipulations of the approved CPS;
- Make best effort to provide CA services on a 7 day per week, 24 hour per day basis in accordance with this CP and the CPS;
- Ensuring that registration information is accepted only from properly authenticated RAs and or LRAs who understand and are obligated to comply with this CP;
- Issue certificates to Subscribers in accordance with this CP as well as the procedures and practices described in the CPS;
- Including only valid and appropriate information in certificates and maintaining evidence that due diligence was exercised in validating the information contained in the certificates;
- Revoke certificates that are issued by this CA in accordance with the stipulations of this CP as well as those in the CPS;
- Issue and publish CRLs on a regular schedule as per the CPS;
- Notify Subscribers that certificates have been issued to them or that their digital signature verification certificate has been revoked via secure exchanges between the CA and the client application representing that Subscriber;
- Notify others (e.g. Relying Parties) of certificate issuance/revocation by provision of access to certificates and CRLs in the Repository;
- Provide renewal, suspension, and replacement of certificates; and
- Operating or providing for the services of an on-line Repository.

Some obligations that are defined as the CA's may actually be carried out by an RA, on behalf of the CA, but the CA remains ultimately responsible for such obligations.

2.1.2 Registration Authority Obligations

An RA or LRA who performs registration functions as described in this CP shall comply with the stipulations of this CP and comply with the CPS. An RA or LRA who is found to have acted in a manner inconsistent with these obligations shall be subject to revocation of RA responsibilities and possible disciplinary action.

The RA and LRA is obliged to verify the accuracy and authenticity of the information provided by LRAs for the acceptance of Subscriber certificate applications. The RA may make use of existing High Performance Computing Virtual Laboratory databases as an agent to verify the application data by comparing it with information in the databases. The RA provides this verification on behalf of the CA.

A RA and LRA represents and warrants to the CA that it shall:

- receive certificate applications in accordance with the terms and conditions of the CPS;
- perform limited verification of information submitted by Applicants when applying for certificates, and if such verification is successful, submit a request to the CA for the issuance of an certificate, all in accordance with the terms and conditions of the CPS;
- receive and verify requests from Subscribers for the revocation of certificates, and if the verification of a revocation request is successful, submit a request to the CA for the revocation of such certificate, all in accordance with the terms and conditions of the CPS;
- notify Subscribers, in accordance with the terms and conditions of the CPS, that a certificate has been issued to them; and
- notify Subscribers, in accordance with the terms and conditions of the CPS, that a certificate issued to them has been revoked or will soon expire.

2.1.3 Subscriber Obligations

A Subscriber shall:

- Provide correct information to the LRA/RA without errors, omissions, or misrepresentations;
- Generate a new and secure key pair to be used in association with the Subscriber's certificate;
- Refrain from modifying the certificate contents;
- Request revocation of a certificate if a key is no longer needed;
- Memorize and not record any passwords or PINs associated with accessing or using private keys or cryptographic tokens;
- Exercise diligence in protecting their private keys and cryptographic tokens at all times against loss, theft or tampering;
- Inform the LRA/RA *within 48 hours* of a change to any information included in it's certificate or certificate application request;
- Inform the High Performance Computing Virtual Laboratory *Customer Service Center / Help Desk within 24 hours* of a suspected or actual compromise of one or all of it's private keys, activation data, or security module;
- Immediately cease to use the Subscriber's certificate upon expiration or revocation of such HPCVL Certificate, or any suspected or actual compromise of the private key corresponding to the public key in such certificate, and remove such certificate from the devices and/or software in which it has been installed;

- Understand the basic principles of Public Key certificates and their use within the business / application;
- Use certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of this CP and applicable laws;
- Only use certificates on behalf of the person, entity, or organization listed as the subject of the certificate; and
- Read, understand and abide by all the terms, conditions, and restrictions in the Subscriber Agreement or contract.

Certificates and related information may be subject to export, import, and/or use restrictions. Subscribers shall comply with all laws and regulations applicable to a Subscriber's right to export, import, and/or use certificates or related information. Subscribers shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of certificates or related information. Certain cryptographic techniques, software, hardware, and firmware ("Technology") that may be used in processing or in conjunction with certificates may be subject to export, import, and/or use restrictions. Subscribers shall comply with all laws and regulations applicable to a Subscriber's right to export, import, and/or use such Technology or related information. Subscribers shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of such Technology or related information.

2.1.3.1 Subscriber and Applicant Representations and Warranties

Subscribers and Applicants represent and warrant to High Performance Computing Virtual Laboratory that:

- all information provided by the Subscriber or Applicant to High Performance Computing Virtual Laboratory or to any independent third-party RA is correct and does not contain any errors, omissions, or misrepresentations;
- the private key corresponding to the public key submitted by the Subscriber and/or Applicant in connection with a certificate application was created using sound cryptographic techniques and has not been compromised;
- any information provided to High Performance Computing Virtual Laboratory or to any independent third-party RAs by the Subscriber and/or Applicant in connection with an certificate application does not infringe, misappropriate, dilute, unfairly compete with, or otherwise violate the intellectual property, or other rights of any person, entity, or organization in any jurisdiction;
- the Applicant shall notify High Performance Computing Virtual Laboratory or, if the Applicant submitted its certificate application to an independent third-party RA, such independent third-party RA, as soon as practicable if any information included in the Applicant's certificate application changes or if any change in any circumstances would make the information in the Applicant's certificate application misleading or inaccurate;
- the Subscriber shall immediately cease to use the Subscriber's certificate if any information included in the Subscriber's certificate changes or if any change in any circumstances would make the information in the Subscriber's certificate misleading or inaccurate;
- the Subscriber shall immediately cease to use the Subscriber's certificate upon

- expiration or revocation of such certificate, or
- any suspected or actual compromise of the private key corresponding to the public key in such certificate, and shall remove such certificate from the devices and/or software in which it has been installed; and
- the Subscriber and/or Applicant will not use certificates for any hazardous or unlawful (including tortuous) activities.

2.1.4 Relying Party Obligations

Each Relying Party shall:

- Use certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of this CP and applicable laws;
- Perform cryptographic operations properly;
- Verify certificates, including the use of CRLs, in accordance with the certification path validation procedure specified in ITU-T Rec. X.509, taking into consideration any critical extensions;
- Trust and make use of a certificate issued under this CP only if the certificate has not expired nor been revoked and only if a proper chain of trust can be established to an acceptable root CA;
- Make their own judgment and rely on a certificate only if such reliance is reasonable in the circumstances, including determining whether such reliance is reasonable given the nature of the security and trust provided by a certificate and the value of any transaction that may involve the use of a certificate;
- Preserve the original signed data, the applications necessary to read and process the data, and the cryptographic applications needed to verify the digital signatures on that data as long as it may be necessary to verify the signature on the data; and
- Understand the basic principles of Public key certificates and their use within the business / application.

Certificates and related information may be subject to export, import, and/or use restrictions. Relying Parties shall comply with all laws and regulations applicable to a Relying Party's right to use certificates and/or related information. Relying Parties shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of certificates and/or related information. Certain cryptographic techniques, software, hardware, and firmware ("Technology") that may be used in processing or in conjunction with certificates may be subject to export, import, and/or use restrictions. Relying Parties shall comply with all laws and regulations applicable to a Relying Party's right to export, import, and/or use such Technology or related information. Relying Parties shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of such Technology or related information.

2.1.4.1 Relying Party Representations and Warranties

Relying Parties represent and warrant to High Performance Computing Virtual Laboratory that:

- the Relying Party shall properly validate a certificate before making a determination about whether to rely on such certificate, including confirmation that the certificate has not expired or been revoked and that a proper chain of trust can be established to a trustworthy root CA;
- the Relying Party shall not rely on a revoked or expired certificate;
- the Relying Party shall not rely on a certificate that cannot be validated back to a trustworthy root CA;
- the Relying Party shall exercise its own judgment in determining whether it is reasonable under the circumstances to rely on a certificate, including determining whether such reliance is reasonable given the nature of the security and trust provided by a certificate and the value of any transaction that may involve the use of a certificate; and
- the Relying Party shall not use a certificate for any hazardous or unlawful (including tortuous) activities.

2.1.5 Repository Obligations

The Repository is obligated to:

- Post to an X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol;
- Publish and archive certificates;
- Publish and archive CRLs/ARLs;
- Publish and archive the CP;
- Post all CA provided information in a timely manner;
- Maintain security to prevent unauthorized access and tampering.
- Maintain the availability of the information as required by the certificate information posting and retrieval stipulations of this CP; and
- Provide access control mechanisms when needed to protect Repository information as described in this CP.

2.2 LIABILITY

As the CA and RA functions are provided by the High Performance Computing Virtual Laboratory, the liability issues related to both functions are combined in this CP.

Nothing in this CP shall create, alter, or eliminate any other obligation, responsibility, or liability that may be imposed on the High Performance Computing Virtual Laboratory by virtue of any contract or obligation that is otherwise determined by applicable law.

The maximum cumulative liability of the High Performance Computing Virtual Laboratory to all Subscribers, Relying Parties and any other entities for losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to use of an certificate or any services provided by the

High Performance Computing Virtual Laboratory in respect to any certificate is limited by this CP. This CP also contains limited warranties and disclaimers of representations, warranties and conditions.

Each Relying Party acknowledges that to the extent that its reliance on any certificate causes itself or its customer damages, of any type, in excess of the liability limits described in this CP and the Subscriber Agreement, such reliance is unreasonable.

2.2.1 Certification Authority and Registration Authority Liability

2.2.1.1 Warranties and Limitations on Warranties

The High Performance Computing Virtual Laboratory warrants and promises to:

- Provide certification and repository services consistent with this CP;
- Perform the identification and authentication procedures set forth in §3 of this CP and the procedures defined in §3 of the CPS;
- Provide key management services including certificate issuance, publication, revocation and update in accordance with this CP and with the CPS; and
- Comply with all legal provisions in this CP.

The High Performance Computing Virtual Laboratory makes no representations or warranties with respect to:

- The techniques used in the generation and storage of the Private Key corresponding to the Public Key in certificate, including, whether such Private Key has been compromised or was generated using sound cryptographic techniques;
- The reliability of any cryptographic techniques or methods used in conducting any act, transaction, or process involving or utilizing a certificate;
- Any software whatsoever; or
- Non-repudiation of any certificate or digital signature verified using a certificate, since determination of non-repudiation is a matter of applicable law.

2.2.1.2 NOTICE OF LIMITED LIABILITY

No stipulation.

2.2.1.3 Disclaimers

The High Performance Computing Virtual Laboratory is not liable for loss due to any of the following:

- Loss of CA or RA service due to war, natural disasters or other uncontrollable forces.
- Incurred between the time that a certificate is revoked and the next scheduled issuance of a Certificate Revocation List.
- Due to unauthorized use of certificates issued by the CA.

- Use of certificates beyond the prescribed use defined by the CP under which the certificate is issued and the related CPS. Caused by fraudulent or negligent use of certificates and/or CRLs and/or ARLs issued by the CA.
- Due to disclosure of information contained within certificates and CRLs; and
- Due to losses incurred if not notified of revoked certificates.

The High Performance Computing Virtual Laboratory disclaims all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided.

Under this CP, the High Performance Computing Virtual Laboratory provides for total cumulative damages resulting from loss as a result of using a certificate issued by the CA. Any compensation claim deemed to be valid by the PMA is limited to a maximum of ***\$0.00(zero dollars)*** per instance.

2.3 FINANCIAL RESPONSIBILITY

In no event shall the total cumulative liability of the High Performance Computing Virtual Laboratory and any of the High Performance Computing Virtual Laboratory's employees, or directors to any Subscribers, Relying Party or any other person, entity, or organization arising out of or relating to any certificate or any services provided by the High Performance Computing Virtual Laboratory in respect to certificates, including any use or reliance on any certificate, exceed the net amounts received by the High Performance Computing Virtual Laboratory from the Subscribers, Relying Party, or other person, entity or organization for the certificate giving rise to the liability ("cumulative damage cap"). This limitation shall apply on a per certificate basis regardless of the number of transactions, digital signatures, or causes of action arising out of or related to such certificate or any services provided in respect of such certificate. The foregoing limitations shall apply to any liability whether based in contract (including fundamental breach), tort (including negligence) or any other theory of liability, including any direct, indirect, special, punitive, exemplary, consequential, reliance, or incidental damages.

In the event that liability arising out of or relating to a certificate or any services provided by the High Performance Computing Virtual Laboratory in respect to certificates exceeds the cumulative damage cap set forth in this section above, the amounts available under the cumulative damage 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 High Performance Computing Virtual Laboratory be obligated to pay more than the cumulative damage cap for each certificate regardless of apportionment among claimants.

In no event shall the High Performance Computing Virtual Laboratory or any of the High Performance Computing Virtual Laboratory's subcontractors, agents, suppliers, employees, or directors be liable for any incidental, special, punitive, exemplary, indirect, reliance, or consequential damages (including, without limitation, damages for loss of business, loss of business opportunities, loss of goodwill, loss of profits, business interruption, loss of data, lost savings or other similar pecuniary loss) whether arising from contract (including fundamental breach), tort (including negligence) or any other theory of liability.

The foregoing limitations shall apply notwithstanding the failure of essential purpose of any limited remedy stated herein and even if the High Performance Computing Virtual Laboratory has been advised of the possibility of those damages.

Subscribers, Relying Parties, Registration Authorities and cross-certified Certification Authorities are not eligible for compensation claims for losses resulting from inappropriate or fraudulent use of this Public

Key Infrastructure. The High Performance Computing Virtual Laboratory is responsible only for direct, compensatory damages in any action to recover a loss due to reliance on a certificate, which damages do not include punitive or exemplary damages, damages for lost profits, savings, or opportunity, damages for pain and suffering, losses or damages suffered by anyone who is not a Subscriber.

2.3.1 Indemnification by Relying Parties

No stipulation.

2.3.2 Fiduciary Relationships

No stipulation.

2.3.3 Administrative Processes

No stipulation.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing Law

This Certificate Practice Statement and all associated agreements shall be construed in accordance with the laws of the Province of Ontario, Canada.

2.4.1.1 Interpretation

All references in this CP to “§” refer to the sections of this CP. As used in this CP, neutral pronouns and any variations thereof shall be deemed to include the feminine and masculine and all terms used in the singular shall be deemed to include the plural, and vice versa, as the context may require. The words “hereof,” “herein”, “hereunder”, and other words of similar import refer to this CP as a whole, as the same may from time to time be amended or supplemented, and not to any subdivision contained in this CP. The words "include" and “including” when used herein is not intended to be exclusive and mean, respectively, "include, without limitation," and “including, without limitation.”

2.4.2 Severability, Survival, Merger, Notice

No stipulation.

2.4.3 Dispute Resolution Procedures

No stipulation.

2.5 FEES

There is no fee as certificates will be issued without charge to all users in good standing as per the High Performance Computing Virtual Laboratory Membership/Access Policy. Notwithstanding, we reserve the right to charge fees. The High Performance Computing Virtual Laboratory may also issue certificates to members of participating organizations for a fee.

2.5.1 Certificate Issuance or Renewal Fees

No stipulation.

2.5.2 Certificate Access Fees

No stipulation.

2.5.3 Revocation or Status Information Access Fees

No stipulation.

2.5.4 Fees for Other Services such as Policy Information

No stipulation.

2.5.5 Refund Policy

No stipulation.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of Certification Authority Information

For the use of its Subscribers and Relying Parties, the CA shall publish the following information to the Repository:

- Issued certificates;
- CRLs/ARLs;
- The CA's certificate associated with its signing key;
- This CP; and
- Any relevant information that is necessary for reliance on certificates issued under this CP.

The CA shall not publish the CPS to the Repository.

2.6.2 Frequency of Publication

All information to be published in the Repository shall be published as soon as such information is available to the CA. Certificates shall be published immediately following user acceptance as specified in §4.3 and proof of possession of private key as specified in §3.1.7. Information regarding frequency of CRL/ARL publication is found in §4.4.9.

2.6.3 Access Controls

The CA shall protect any Repository information not intended for public dissemination or modification. Public Key certificates and certificate status information in the Repository shall be

publicly available. Where applicable, access privileges to information stored or controlled by the CA shall be determined by the PA.

2.6.4 Repositories

The CA shall operate a Repository in which digital signature verification and encryption certificates issued to End Entities as well as CRLs and ARLs are stored. The CA shall ensure unrestricted End Entity access to CRLs and ARLs.

2.7 COMPLIANCE AUDIT

The CA shall have a compliance audit mechanism in place to ensure that the requirements of this CP and the CPS are being implemented and enforced. The PA shall determine adequacy of the compliance audit reporting, and shall be responsible for ensuring all CAs and RAs are audited for compliance on a periodic basis as set forth in §2.7.1.

2.7.1 Frequency of Entity Compliance Audit

A compliance audit shall be performed within *6 months* after the establishment of the CA and *once every 12 months* thereafter.

The PA reserves the right to require an inspection or audit of any CA or RA asserting this CP at any time; the PA shall state the reason for any inspection or audit.

2.7.2 Identity/Qualifications of Auditor

The compliance auditor must perform information system security or CA compliance audits as its primary responsibility. The compliance auditor must be proficient in PKI technology and security auditing and thoroughly familiar with this CP and the CPS.

2.7.3 Auditor's Relationship to Audited Party

The compliance auditor either shall be independent from the PKI, or it shall be sufficiently organizationally separated from the PKI to provide an unbiased, independent evaluation.

2.7.4 Topics Covered by Audit

The purpose of a compliance audit of the PKI shall be to verify that all CAs and RAs are complying with the requirements of this CP, the CPS and any MOAs. All aspects of the CA and RA operations shall be subject to any compliance audit inspection, including, but not limited to: the I&A policies, key management policies, system security controls, operations policy, and certificate profiles.

2.7.5 Actions Taken as a Result of Deficiency

The PA may determine that the CA or RA is not complying with its obligations, as set forth in this CP, or the CPS, or MOA. Any discrepancies between a CA or RA operation and the stipulations of the CPS, MOA and this CP shall be noted in an Audit Compliance Report. The PA shall determine an appropriate remedy that includes a time for completion.

Remedies may include permanent or temporary CA or RA cessation, but several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes, and the disruption to the certificate using community. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

2.7.6 Communication of Results

An Audit Compliance Report, including identification of corrective measures taken or being taken by the OA, shall be provided to the PA and PMA.

2.8 CONFIDENTIALITY

Neither High Performance Computing Virtual Laboratory nor any independent third-party RAs operating under the CA shall disclose or sell Applicant or Subscriber names (or other information submitted by an Applicant or Subscriber when applying for a certificate), except in accordance with this CP, a Subscription Agreement, or a Relying Party Agreement. High Performance Computing Virtual Laboratory shall use a reasonable degree of care to prevent such information from being used or disclosed for purposes other than those set forth in the CP, a Subscription Agreement, or a Relying Party Agreement. Notwithstanding the foregoing, Applicants and Subscribers acknowledge that some of the information supplied with a certificate application is incorporated into certificates and that High Performance Computing Virtual Laboratory and all independent third-party RAs operating under the CA shall be entitled to make such information publicly available.

2.8.1 Types of Information to be Kept Confidential

A certificate shall only contain information that is relevant and necessary to effect secure transactions using the certificate. For the purpose of proper administration of the certificates, non-certificate information may be requested to manage the certificates (e.g. identifying numbers, business or home addresses, and telephone numbers). Any such information shall be explicitly identified in the CPS. All personally identifiable information obtained from Subscribers in connection with the administration of the certificates will be handled in accordance with the collection, maintenance, retention, and protection requirements of the *relevant privacy laws*.

Special procedures may be necessary to deal with aggregation of sensitive information within components of the infrastructure. Particular attention shall be paid to protect private information.

The following information shall also be considered confidential and may not be disclosed except as detailed in §2.8.3 through §2.8.7:

- Audit trail records created and retained by the CA,
- Security measures of the CA and its operation, and
- Disaster recovery plans.

2.8.2 Types of Information not Considered Confidential

Certificates that are published to the Repository are not considered confidential. To promote the interoperation and widespread utility of PKI resources, information included in certificates or the Repository (or any aggregation of that information) should be limited to information that is not overtly confidential.

This CP is not considered confidential.

Without limiting the foregoing, information that

- was or becomes known through no fault of High Performance Computing Virtual Laboratory or an independent third-party RA under a CA,
- was rightfully known or becomes rightfully known to High Performance Computing Virtual Laboratory or an independent third-party RA under the CA without confidential or proprietary restriction from a source other than the Subscriber,
- is independently developed by High Performance Computing Virtual Laboratory or an independent third-party RA under a CA, or
- is approved by a Subscriber for disclosure,

shall not be considered confidential.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

Information concerning the events leading up to and the investigation of a revocation shall be limited to those individuals with a need to know.

2.8.4 Release to Law Enforcement Officials

The CA may release sensitive information, including the private decryption key, in the course of a criminal investigation as required by law. The CA is not obligated to inform the Subscriber of such release.

2.8.5 Release as Part of Civil Discovery

The CA shall release personally identifiable or other information submitted to the CA by a Subscriber, if authorized by the Subscriber. Non-disclosure of information shall remain an obligation notwithstanding the status of a certificate (current or revoked) or the status of the CA.

2.8.6 Disclosure upon Owner's Request

Any personally identifiable information submitted to the CA by a Subscriber shall be made available to the Subscriber for individual review following an authenticated request from the Subscriber. This information shall be subject to correction and/or update at the Subscriber's request.

2.8.7 Other Information Release Circumstances

Audit trail information may only be released to the authorized auditing party, as determined by the PA.

2.9 INTELLECTUAL PROPERTY RIGHTS

High Performance Computing Virtual Laboratory retains all right, title, and interest (including all intellectual property rights), in, to and under all public key certificates and private key that it issues, and

any products or information developed under or pursuant to this CP, except for any information that is supplied by an Applicant or a Subscriber and that is included in a certificate, which information shall remain the property of the Applicant or Subscriber. Because a Subscriber's private signature keys are created by the Subscriber and not issued by the CA, the Subscriber maintains ownership of the private signature keys.

3. IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Types of Names

The CA shall generate, sign, and process certificates that contain a X.500 Distinguished Name (DN) in the certificate *subject name* field. Certificates issued to CAs and RAs shall also use the X.500 DN form.

Certificates may additionally assert an alternate subject name, using the *subjectAltName* extension as defined in X.509; when asserted it must be marked as non-critical.

3.1.2 Need for Names to be Meaningful

All certificates shall include an identifier that represents the individual, entity, or object to which the certificate was issued. This identifier shall be in such a form as not to hide or conceal the true identity of the End Entity.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be in accordance with the Certificate Profile, defined in §7.

Standards may include:

- X.500 for DN;
- RFC 822 for email address; and
- Appropriate IETF RFCs for URL and IP address.

3.1.4 Uniqueness of Names

All certificates issued by the CA shall include an identifier that represents the individual, entity, or object to which the certificate was issued. This identifier shall be unique such that no two certificates have the same identifier.

The CA shall enforce name uniqueness.

3.1.5 Name Claim Dispute Resolution Procedure

The CA shall investigate and correct any name duplication brought to its attention. The PA is the final arbiter in name dispute resolution (when the CA is unable to resolve a dispute) and reserves the right to reject any name at its sole and absolute discretion.

3.1.6 Recognition, Authentication and Role of Trademarks

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

3.1.7 Method to Prove Possession of Private Key

Prior to the issuance of a certificate, the CA shall require proof of possession of the Subscriber's private key before creating and signing a certificate containing the associated public key.

Where the Applicant directly generates keys, in either software or hardware, the Applicant shall be required to prove possession of the private key, which corresponds to the public key in the certificate issuance request.

Where the RA generates keys on behalf of the Applicant, and delivers them to the certificate subject, the delivery shall be accomplished in a way that ensures that the correct keys and activation data are provided to the correct subject. The CA shall maintain a record of validation for receipt of the keys by the Applicant. When any mechanism that includes a shared secret (e.g. a password or PIN) is used, the mechanism shall ensure that the Applicant and the RA are the only recipients of this shared secret.

The CA shall generate its own key management keys.

3.1.8 Authentication of Organization Identity

Requests for certificates in the name of an organization, whereby the Applicant is acting on behalf of that organization, shall require authentication of that organization's identity. Organization identification information shall include the organization name, address, and documentation of the existence of the organization. Acceptable forms of identification are a Dun & Bradstreet number, or a letter signed by an executive of the organization. A D&B D-U-N-S® Number is a unique nine-digit sequence recognized as the universal standard for identifying and keeping track of over 84 million businesses worldwide.

The RA or LRA shall verify the organization identity information. In addition, the RA or LRA shall verify the identity information of the requesting representative of the organization in accordance with authentication of individual identity as in §3.1.9 and verify the authenticity of the representative's authorization to act in the name of the organization.

The PA shall perform authentication of organization identity for the purpose of issuing a cross-certificate. Organization identification information shall include the organization name, address, and documentation of the existence of the organization.

3.1.9 Authentication of Individual Identity

For individuals requesting a certificate, the CA shall ensure that the applicant's identity information is verified and checked in accordance with this CP and the CPS. The CA shall ensure that the applicant's identity and public key are properly bound. The authentication process shall involve an applicant presenting acceptable identification credentials to the RA or LRA personnel.

The RA or LRA shall record the process that was followed for each identity authentication and each certificate issuance. The information to record includes:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the applicant;
- An employee number or a unique identifying number from the ID of both participants (the verifier and the applicant);
- The date and time of the verification; and
- A declaration of identity signed by the applicant.

The following guidelines are provided to establish the identification requirements for the registration process:

The applicant Subscriber must appear personally before a RA or LRA as being authorized to confirm identities on behalf of an authenticated organization; the information provided must be verified to ensure legitimacy. The credentials required are either:

- One government-issued picture I.D. (e.g. a driver's license or passport); or
- One employer-issued picture I.D. (for employees of an authenticated organization); or
- The employee is personally known to the LRA (for employees of an authenticated organization).

The applicant Subscriber must identify a need for the certificate consistent with §1.3.4.

3.1.9.1 Identification and Authentication of a Device Identity

An application for a device, application, or server to be a certificate subject may be made by an individual authorized to act on behalf of the prospective certificate subject.

The RA shall verify the identity of the individual acting on behalf of the device, application, or server as stipulated in §3.1.9. The RA shall also verify the authority of the individual to receive the keys on behalf of that certificate subject.

3.2 ROUTINE REKEY

Identity for routine rekey shall be established either through the use of the current signature key, provided that it has not been revoked or through the initial registration process as described in §3.1.9.

3.3 REKEY AFTER REVOCATION

After a certificate has been revoked, the Subscriber must go through the initial registration process described in §3.1 to obtain a new certificate.

For revoked cross-certificates, no re-key shall be done until negotiation of a new MOA. The initial registration process described in §3.1 shall then be repeated.

3.4 REVOCATION REQUEST

The RA shall permit Subscribers or another person authorized to act on behalf of the Subscribers (e.g. LRA) to request revocation of a certificate in which the Subscriber is identified as the certificate subject.

The identity associated with the revocation request may be established through the use of the current signature key, provided that it has not been revoked. The identity associated with the revocation request may also be established through the initial registration process as described in §3.1.9.

A revocation request for a cross-certified CA must be received from an authorized official of that organization. The PA shall authenticate the request.

4. OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The Applicant and the RA or LRA shall perform the following steps when a Subscriber applies for a certificate:

- Determine that the Applicant is authorized to be issued certificates (per this CP and the CPS);
- Perform identity proofing and record the identity of the Subscriber (per §3.1); and
- Provide a point of contact for verification of any roles or authorizations requested.

These steps may be performed in any order that is convenient for the CA and applicants, as long as this does not defeat security. However, all of these steps must be completed prior to certificate issuance.

While the Applicant may do most of the certificate application data entry, it is still the responsibility of the RA or LRA to verify that the information is correct and accurate. This may be accomplished through a system approach linking trusted databases containing personnel information, other equivalent authenticated mechanisms, or through personal contact with the Subscriber. If databases are used to confirm Applicant information, then these databases must be protected from unauthorized modification to a level commensurate with the level of assurance of the certificate being requested.

Any electronic transmission of shared secrets communicated during the certificate application process shall be protected (e.g. encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

4.2 CERTIFICATE ISSUANCE

Certificates will be generated based on the RA or LRA review and acceptance of the certificate application and submission of a certificate request to the CA, which is ultimately responsible for approving the certificate request. Upon approval, the CA shall sign and issue the certificate. The certificate request may be submitted and processed electronically.

Upon receiving the certificate request, the CA shall:

- Verify the authority of the requestor and the integrity of the information in the certificate request;
- Obtain a functioning public/private key pair for each certificate required and prove that the private key is held by the Subscriber (per §3.1.7);
- Build and sign a certificate, if all certificate requirements have been met (or sign the certificate that is built by an RA, LRAs or Subscriber); and
- Make the certificate available to the Subscriber and post it to the Repository.

To the extent practical, certificates once created shall be checked to ensure that all fields and extensions are properly populated. This may be done through software which scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

The issuance and publication of a certificate in the Repository by the CA indicates a complete and final approval of the certificate application by the CA.

4.3 CERTIFICATE ACCEPTANCE

Acceptance is the action taken by a Subscriber that triggers the Subscriber's duties and potential liability following the issuance of a certificate. It is the responsibility of the RA or LRA through the delivery process to:

- Explain to the Subscriber their responsibilities;
- Inform the Subscriber of the creation of a certificate and to the contents and purpose of the certificate; and
- Require the Subscriber to indicate acceptance of their responsibilities.

All Applicants shall expressly acknowledge to the RA or LRA, through signing the Subscriber Agreement, that they will adhere to this CP as both a Subscriber and as a Relying Party. This requirement may be waived where a contract exists between High Performance Computing Virtual Laboratory and the organization that the Subscriber represents.

The certificate acceptance process is complete when the Subscriber accomplishes a technical or procedural mechanism, specified in the CPS, to indicate acceptance of their certificate.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Circumstances for Revocation

Each certificate shall be revoked when the Subscriber no longer wants or requires a certificate, when the public key password, token or profile associated with the certificate is compromised, or is suspected of being compromised.

Certificates may also be revoked by the CA upon failure of the Subscriber to meet its obligations under this CP or any other agreement, regulation, or law that may be in force.

The RA or LRA may request a certificate revocation if they have knowledge or suspicion of a compromise.

4.4.2 Who can Request Revocation

A Subscriber, another person authorized to act on behalf of the Subscriber (e.g. LRA), or the RA or CA may request the revocation of certificates. A Subscriber may only request revocation of a certificate in which they are listed as the certificate subject

4.4.3 Procedure for Revocation Request

The OA shall document procedures for revocation requests in the CPS covering the origination, receipt, approval, and processing of the request. These procedures must comply with this CP.

4.4.4 Revocation Request Grace Period

This CP does not explicitly define a revocation grace period; revocation requests shall be processed in a timely manner as documented in the CPS.

4.4.5 Circumstances for Suspension

The RA may suspend a certificate for reasons other than those stipulated in §4.4.1. The RA must document the reason for suspension.

Certificates for Trusted Roles and cross-certified CAs shall not be suspended.

4.4.6 Who can Request Suspension

Only individuals authorized to request revocation, as stipulated in §4.4.2, shall be allowed to request certificate suspension.

4.4.7 Procedure for Suspension Request

The OA shall document procedures for suspension requests in the CPS covering the origination, receipt, approval, and processing of the request. These procedures must comply with this CP.

4.4.8 Limits on Suspension Period

Suspension of a certificate shall not exceed *120 days*. Certificates suspended for more than this period days must be revoked.

4.4.9 Certificate Revocation List Issuance Frequency

CRLs shall be published upon revocation of a certificate or *at least every 12 hours*.

4.4.10 Certificate Revocation List Checking Requirements

Relying Parties shall perform certificate status checking to obtain assurance with a certificate. The Relying Party shall determine how often to obtain new revocation data. If it is infeasible to obtain current revocation information, then the Relying Party should reject use of the certificate, because the certificate's status cannot be guaranteed.

When a Relying Party downloads a Certificate Revocation List from the Repository, the Relying Party shall verify the CRL by validating its digital signature.

In no event shall High Performance Computing Virtual Laboratory or any independent third-party RAs operating under the CA, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing be liable for any damages whatsoever due to

- the failure of a Relying Party to check for revocation or expiration of a certificate, or
- any reliance by a Relying Party on a certificate that has been revoked or that has expired.

4.4.11 On-line Revocation/Status Checking Availability

The CA does not support on-line revocation/status checking (e.g. OCSP).

4.4.12 On-line Revocation Checking Requirements

No stipulation.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements re Key Compromise

If a Subscriber suspects or knows that the private key corresponding to the public key contained in the Subscriber's certificate has been compromised, the Subscriber shall immediately notify the RA that processed the Subscriber's certificate application, using the procedures set forth in §4.4.3, of such suspected or actual compromise. The Subscriber shall immediately stop using such certificate and shall remove such certificate from any devices and/or software in which such certificate has been installed. The Subscriber shall be responsible for investigating the circumstances of such a compromise or suspected compromise and for notifying any Relying Parties that may have been affected by such a compromise or suspected compromise.

4.5 SECURITY AUDIT PROCEDURES

Audit log files shall be generated for all events relating to the security of the CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with the retention period for archive as specified in §4.6.2.

4.5.1 Types of Event Recorded

The auditing capabilities of the underlying PKI equipment operating system shall be enabled during installation. A record shall be kept of file manipulation and account management. These events shall also be recorded during normal operation of the PKI equipment.

The PKI equipment shall be able to record events related to the server (e.g. installation, modification, and accesses), and the CA application (e.g. requests, responses, actions, publications, and error conditions). Events may be attributable to human action or automatically invoked by the equipment.

A message from any source requesting an action by the CA is an auditable event (e.g. certificate requests, revocation requests, creation of certificates, generation and posting of CRLs). At a minimum, the following information related to an event shall be recorded:

- The type of event;
- The entities involved;
- The date and time the event occurred; and
- The success or failure of the event/attempt.

In addition, for some events the following information may be recorded:

- The source and destination of a message; and
- The disposition of a created object (e.g. a filename).

The CPS shall identify each of the audit events for the CA.

4.5.2 Frequency of Processing Log

Audit logs shall be reviewed regularly *on at least a monthly basis* in accordance with the procedures specified in the CPS.

4.5.3 Retention Period for Audit Log

Audit logs shall be retained on the CA equipment for a minimum period of *2 months* and archived in accordance with the procedures specified in the CPS.

4.5.4 Protection of Audit Log

Access to audit logs shall be restricted on a need-to-know basis and shall be protected by a combination of physical and logical security controls in accordance with the procedures specified in the CPS.

4.5.5 Audit Log Backup Procedures

Audit log files shall be backed-up and the backup media shall be stored locally. A consolidated copy of the audit log files shall be sent to a secure off-site storage facility in accordance with procedures specified in the CPS.

4.5.6 Audit Collection System

No stipulation.

4.5.7 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. Real-time alerts are neither required nor prohibited by this CP.

4.5.8 Vulnerability Assessments

The OA shall perform routine self-assessments of security controls.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Event Recorded

PKI archive records shall be detailed enough that they can be used to establish the validity of a signature. At a minimum, the following data shall be archived:

- PKI system equipment configuration files;
- CA and Repository application configuration files, logs, and databases;
- PKI Accreditation;
- Completed CP and CPS; and
- Contractual Obligations.

4.6.2 Retention Period for Archive

Archive records shall be retained for a period of 10.5 *years* in accordance with the procedures specified in the CPS.

4.6.3 Protection of Archive

Access to archive records shall be restricted on a need-to-know basis and shall be protected by a combination of physical and logical security controls in accordance with the procedures specified in the CPS. Additionally, all archive media shall be provided adequate protection from environmental threats such as temperature, humidity, and magnetism.

4.6.4 Archive Backup Procedures

Certificates, CRLs, and keys shall be backed-up and stored locally. A copy of these items shall be made and sent to a secure archive facility in accordance with the procedures specified in the CPS. The backup procedure shall be tested quarterly and the backed-up information shall enable a complete restore of the system in case of a disaster.

For manual (i.e. paper) records, a copy of the document shall be made as it is received and sent to a secure archive facility. Original copies shall be kept locally.

4.6.5 Requirements for Time-Stamping of Records

Backup records shall be time stamped.

4.6.6 Archive Collection System

No stipulation.

4.6.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to obtain and verify the archive information shall be documented in the CPS.

4.7 KEY CHANGEOVER

The CA shall publish a new certificate after key changeover and make it available to Subscribers as stipulated in §6.1.4.

Subscriber certificates shall be configured for either automated renewal or manual renewal. In the case of manual renewal, the RA shall provide the Subscriber *3 months* notice prior to certificate expiry.

4.8 COMPROMISE AND DISASTER RECOVERY

4.8.1 Computing Resources, Software, and/or Data are Corrupted

In the case of an event whereby the CA system is physically damaged or corrupted and becomes inoperative, but the CA signing key is available, the CA system shall be rebuilt and restored to the most recent known good condition.

4.8.2 Entity Public Key is Revoked

No stipulation.

4.8.3 Entity Key is Compromised

In the event of a CA key compromise, the PMA shall conduct an investigation and make a determination of the severity of the compromise and appropriate response. The response may include any reasonable course of action up to and including CA termination, followed by establishment of a new CA.

4.8.4 Secure Facility after a Natural or Other Type of Disaster

In the case of an event whereby the CA facility is physically damaged to such an extent that normal operation cannot be restored, but the CA signing key is available, the CA system shall be rebuilt and restored to the most recent known good condition at a Disaster Recovery facility.

A Business Continuity Plan for the RA shall be established in accordance with the procedures specified in the CPS and the High Performance Computing Virtual Laboratory Security Policy.

4.9 CERTIFICATION AUTHORITY TERMINATION

The PMA shall decide whether to terminate the CA. In the event of CA termination, the OA shall notify the Subscribers and Relying Parties and any cross-certified CAs through any reasonable means (e.g. mail, email). Arrangements to preserve the archive records of the terminated CA shall be made.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

The location and construction of the facility housing the 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 guards and intrusion sensors shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical Access

The 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. Access to the CA equipment and cryptographic tokens shall be limited to specific trusted personnel.

At a minimum, the physical access controls of the CA shall:

- Ensure no unauthorized access to the hardware is permitted;
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers;
- Be manually or electronically (e.g., camera) monitored for unauthorized intrusion at all times;
- Ensure an access log is maintained and inspected periodically;
- Require two-person (or more) integrity physical access control to the CA equipment; and
- Require two-person (or more) integrity access control to the cryptographic module that holds the CA's private keys.

Removable cryptographic modules shall be inactivated before storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and it shall not be stored with the cryptographic module.

A security check of the facility housing the CA equipment shall occur prior to leaving the facility unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "in-use," and secured when "not in use");

- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

Additionally, a periodic security check shall be made if the facility is continuously left unattended, to ensure that no attempts to defeat the physical security mechanisms have been made. A person or group of persons shall be made explicitly responsible for making such checks.

A log shall be maintained, identifying the date and time and person performing each check. Each person performing a check shall sign off on the log, asserting that all necessary physical protection mechanisms are in place and activated.

5.1.3 Power and Air Conditioning

The facility that houses the CA equipment shall be supplied with power and air conditioning sufficient to create a reliable operating environment. The CA equipment shall have backup capability to automatically lock out input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

No stipulation.

5.1.5 Fire Prevention and Protection

An automatic fire extinguishing system shall be installed in accordance with local policy and code.

5.1.6 Media Storage

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

5.1.7 Waste Disposal

Waste shall be removed or destroyed in accordance with industry best practice. Media used to store sensitive data shall be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-site Backup

System backups, sufficient to recover from system failure, shall be made on a periodic schedule, as described in the CPS. A current backup shall be created and stored at an offsite location (separate from the CA equipment) *no less than once per week*. The backup shall be stored at a facility with physical and procedural controls commensurate to that of the CA system.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

All personnel that have access to or control over cryptographic operations that may affect the CA's issuance, use, suspensions, or revocation of certificates, including access to restricted operations of the CA's repository, shall, for purposes of this CP, be considered as serving in a trusted role. A trusted role has special responsibilities, but does not necessarily correspond to special types of Subscribers or certificates.

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 highly trustworthy or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for the entire PKI. Two approaches shall be taken to increase the likelihood that these roles can be successfully carried out: the first shall ensure that the person filling the role is trustworthy and properly trained, and the second shall distribute the functions among more than one person, so that any malicious activity would require collusion.

The trusted roles defined in this CP include:

- Administrator: authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys.
Officer: authorized to request or approve certificates or certificate revocations.
Auditor: authorized to view and maintain audit logs.
Operator: authorized to perform operating system and networking operations.

The CPS may define additional trusted roles to provide further role separation, or to include repository responsibilities

5.2.1.1 Administrator

The Administrator role shall be responsible for:

- Starting and stopping CA services;
- Setting up Security Officers for key recovery;
- Backing up and restoring the CA database;
- Generation and revocation of certificates for personnel in PKI Trusted Roles;
- Posting certificates and CRLs;
- Performing the incremental database backups;
- Administrative functions such as compromise reporting and maintaining the database; and
- Hardware cryptographic module programming and management.

Administrators shall not issue certificates to Subscribers.

5.2.1.2 Officer

The Officer role shall be responsible for issuing certificates and:

- Verifying a Subscriber's identity, either through personal contact, or via agents or employees, as permitted by this CP;
- Entering user information, and verifying correctness;

- Securely communicating requests to and receiving responses from the CA;
- Receiving and distributing Subscriber certificate data; and
- Requesting, approving and executing the revocation of Subscriber certificates.

5.2.1.3 Auditor

PKI Auditors shall have a view only role; they shall be able to view but not modify audit logs, reports, the Security Policy, and user properties. The PKI Auditors shall be responsible for maintaining and archiving audit logs and for performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with the CPS.

The External Compliance Auditors, addressed in §2.7, are different from the PKI Auditor role.

5.2.1.4 Operator

The Operator shall be responsible for the operation and maintenance of operating system and networking elements of the PKI.

5.2.2 Number of Persons Required per Task

No individual shall be assigned to more than one trusted role; this separation provides a set of checks and balances over the CA operation.

No single individual shall directly perform operations with the CA private keys. At a minimum, *two individuals*, using a split knowledge technique, shall be required to perform any CA key issuance, activation, deactivation, recovery, or revocation operation. Two persons shall be required to perform creation and recovery of Officer accounts.

Responsibilities at the CA host computer may be shared by multiple individuals assigned to multiple roles. Each account on the CA host computer and/or within the CA application shall have limited capabilities commensurate with the role of the account holder.

5.2.3 Identification and Authentication for Each Role

The identity of all individuals serving in trusted roles must be verified and authenticated before they are issued an account or certificate to carry out their duties. The account or certificate used for a trusted role shall only be issued to an individual and must not be shared with other individuals. An individual shall authenticate to the CA system through the use of their account and/or certificate to perform actions authorized for a trusted role.

5.3 PERSONNEL CONTROLS

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be a permanent employee not subject to frequent re-assignment or extended periods of absence. The requirements governing the qualifications, selection, and oversight of individuals who operate, manage, oversee and audit the CA shall be set forth in the CPS.

Personnel assigned to operate CA equipment must:

- Complete a background check;
- Have no other duties that would interfere with those assigned in support of the PKI;
- Have not knowingly been previously relieved of CA or High Performance Computing Virtual Laboratory security duties for reasons of negligence or non-performance of duties; and
- Be appointed in writing by the OA.

5.3.2 Background Check Procedures

High Performance Computing Virtual Laboratory Human Resources policy shall be followed to perform background checks for personnel identified to serve in trusted roles. Such checks are to be performed solely to determine the suitability of a person to fill a PKI trusted role, and shall not be released except as required by law.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA/RA security principles and mechanisms;
- All PKI software versions in use on the CA system; and
- All PKI duties they are expected to perform.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles shall be aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan and the execution of such plan shall be documented. Examples of such changes are CA 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

The PMA shall take appropriate administrative and disciplinary actions, consistent with the High Performance Computing Virtual Laboratory Human Resources policy, against personnel who have performed actions involving the CA not authorized in this CP, the CPS, or other procedures published by the OA.

5.3.7 Contracting Personnel Requirements

Contract personnel employed to perform functions pertaining to the PKI shall meet applicable requirements set forth in this CP and as determined by the PMA or OA.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

A key pair is considered to be generated by the end entity that first comes into possession of it: a Subscriber, an RA, or a CA. Each end entity shall have control over the generation of its own signing key pair.

The CA shall document the CA key generation procedure and generate auditable evidence that the documented procedures were followed; these procedures shall be detailed enough to show that appropriate role separation was used. The CA key generation process shall be observed and validated by an independent third party.

6.1.2 Private Key Delivery to Entity

A private key shall not appear outside of the module it was generated in, unless it is encrypted. The encrypted private key may be output for local transmission or for storage by a key recovery mechanism.

Private signature keys shall be generated and remain within the cryptographic boundary of the cryptographic module.

In those cases where Subscriber key pairs (other than signature keys) are generated by the CA on behalf of the Subscriber, the private key shall be delivered to the Subscriber using a delivery mechanism that provides authentication and confidentiality commensurate with the strength of the cryptography offered by the key.

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber public signature keys shall be delivered to the CA in an authenticated manner as part of a certificate request. The delivery mechanism shall provide authentication commensurate with the strength of the cryptography offered by the key.

In those cases where key pairs (other than signature keys) are generated by the CA on behalf of the Subscriber, delivery of the public key to the CA is not necessary.

6.1.4 Certification Authority Public Key Delivery to Users

The public key of the CA must be available to Subscribers, in the form of a certificate, for certificate trust paths to be created and verified. The CA certificate must be delivered in a reliable manner.

6.1.5 Key Sizes

The CA signature key pair shall be at least *2048 bit RSA*; all other signature key pairs shall be at least *1024 bit RSA*.

All encryption key pairs shall be at least *1024 bit RSA*.

6.1.6 Public Key Parameters Generation

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186.

6.1.7 Parameter Quality Checking

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186.

6.1.8 Hardware/Software Key Generation

The CA shall generate and store cryptographic keys in a *hardware* cryptographic module; all other end entities shall use a hardware or software cryptographic module. Cryptographic modules must comply with the stipulations of §6.8.

6.1.9 Key Usage Purposes

The use of a specific key shall be determined by the *keyUsage* extension in the X.509v3 compliant certificate and as specified in IETF RFC 3280 “Internet PKI Certificate and CRL Profile”.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

Cryptographic modules must comply with the stipulations of §6.8.

6.2.2 Private Key Multi-Person Control

Multi-person control requires that more than one individual independently authenticate themselves to the system that will perform CA operations. This mechanism prevents any single party from gaining access to the CA signing key. The private signing key for the CA, including any backup copies, shall only be accessed under *two-person* control. The CA private signing key may only be backed up under *two-person* control. The personnel authorized to perform multi-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

There is no requirement for private key escrow; therefore, it shall not be supported.

6.2.4 Private Key Backup

Backup copies of the CA private keys shall be made to handle primary module failure and disaster recovery. CA private key copies shall be protected from unauthorized access and use. Each occurrence of access shall be recorded.

The CA shall store a backup copy, in encrypted form, of end entity keys generated by the CA.

End entities are permitted to make operational copies of private keys residing in software cryptographic modules for each of the applications or locations that require the key in a different location or format. All key transfers shall be done from and to an approved cryptographic module and the key shall be encrypted during the transfer. The Subscriber is responsible for ensuring that all copies of private keys are protected, including protecting any workstation on which any of its private keys reside.

6.2.5 Private Key Archival

The CA shall retain archives of key backups created under the stipulations of §6.2.4 and §4.6.

6.2.6 Private Key Entry into Cryptographic Module

Private signature keys shall be generated by and stored in a cryptographic module. In the event that a private key (other than a signature key) is to be transported from one cryptographic module to another, the private key must be encrypted during transport. Private keys must never exist in plaintext form outside the cryptographic module boundary.

6.2.7 Method of Activating Private Key

The Subscriber 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).

6.2.8 Method of Deactivating Private Key

After use, the cryptographic module shall be deactivated either via a manual logout procedure or automatically after a period of inactivity as defined in the CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use. Deactivated keys must be cleared from memory before the memory is de-allocated.

6.2.9 Method of Destroying Private Key

Private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

Any disk space where keys were stored must be overwritten before the space is released to the operating system. For hardware cryptographic modules, private keys may be destroyed by executing a “zeroize” command; physical destruction of hardware is not required.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The CA shall retain archives of key backups created under the stipulations of §4.6.

6.3.2 Usage Periods for the Public and Private Keys

The following table identifies the maximum permissible key and certificate lifetimes:

Table 6.1 Key Lifetimes

Encryption	CA	Other End Entities
Certificate Validity Period	<i>20 years</i>	<i>2 years</i>
Key Lifetime	<i>10 years</i>	<i>17 months</i>
Signature	CA	Other End Entities
Certificate Validity Period	<i>20 years</i>	<i>2 years</i>
Key Lifetime	<i>10 years</i>	<i>17 months</i>

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock CA or Subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. A password, PIN or biometric shall be used as activation data to protect access to private keys, as enforced by the cryptographic module. Activation data shall meet the “strength of authentication mechanism” requirements in §6.8. Subscribers must have the ability to change their password or PIN.

If the activation data must be transmitted, it shall be via a secure channel and separate from the associated cryptographic module. If this is not done by hand, the user shall be advised of the delivery date, method of delivery, and expected arrival date of any activation data. Users shall sign and return a delivery receipt as part of the delivery method.

6.4.2 Activation Data Protection

Activation data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data shall either be biometric in nature, stored in encrypted form, or memorized. Activation data must not be written down, except for backup purposes where it shall be secured at the level of the data that the associated cryptographic module is used to protect.

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 shall be provided by the operating system, or through a combination of operating system, CA software, and physical safeguards. The PKI computing environment shall include the following functionality:

- Require authenticated logins;
- Provide Discretionary Access Control;
- Provide a security audit capability;
- Restrict access control to CA services and trusted roles;
- Enforce separation of duties for trusted roles;
- Require identification and authentication of trusted roles and associated identities;
- Residual information protection;
- Require use of cryptography for session communication and database security;
- Archive CA history and audit data;
- Require self-test security related services;
- Require a trusted path for identification and authentication of trusted roles and associated identities;
- Require recovery mechanisms for keys and the CA system; and
- Enforce domain integrity boundaries for security critical processes.

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

Hardware and software implemented for the PKI shall be developed in a controlled environment, and the development process shall be defined and documented.

6.6.2 Security Management Controls

The configuration of the CA system as well as any modifications and upgrades shall be documented and controlled. Methods of detecting unauthorized modifications to the CA equipment and configuration shall be in place to ensure the integrity of the security software, firmware, and hardware for correct operation.

A formal configuration management methodology shall be used for installation and ongoing maintenance of the CA system.

When first loaded, the CA software shall be verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

The integrity of the CA software shall be verified by the CA Operator *at least weekly*.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

PKI equipment shall be connected to at most one network classification at a time. PKI equipment intended to connect to more than one network classification domain shall have procedures that prevent information from one domain from reaching another (e.g. equipment shutdown, removable hard drives, switching the network connection, etc.).

The PKI equipment shall be protected against network attacks. Use of appropriate boundary controls, such as application level firewalls, shall be employed to protect CA equipment. Only those network ports associated with protocols and commands required for PKI services shall be allowed. Any network software present on the PKI equipment shall be necessary to the functioning of PKI applications.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Only cryptographic modules certified by an accredited laboratory to the most recent, or most recent less one, version of the FIPS PUB 140 "Security Requirements for Cryptographic Modules" shall be used.

The CA shall use a cryptographic module certified at *Level 3 or higher*.

All other end entities shall use a cryptographic module certified at *Level 1 or higher*.

7. CERTIFICATE AND CERTIFICATE REVOCATION LIST PROFILES

The CA shall follow the IETF RFC 3280 “Internet PKI Certificate and CRL Profile”, except as modified by the CPS.

7.1 CERTIFICATE PROFILE

7.1.1 Version Number

The CA shall issue certificates in the X.509 v3 format (populate version field with integer "2").

7.1.2 Certificate Extensions

Whenever private extensions are used, they shall be identified in the CPS. Critical private extensions shall be interoperable in their intended community of use.

7.1.3 Algorithm Object Identifiers

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

Table 7.1 Signature OIDs

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 }
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }
sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 }
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1 }

Certificates issued under this CP shall use the following Object Identifiers for identifying the algorithm for which the subject key was generated:

Table 7.2 Algorithm OIDs

id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-x9-62(10045) public-key-type (2) 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

Certificate subject name forms shall be X.500 Distinguished Names as described in §3.1.1.

7.1.5 Name Constraints

The CA may assert name constraints as required.

7.1.6 Certificate Policy Object Identifier

The HPCVL CA uses certificates in a closed environment, and therefore does not make use of policy object identifiers in the certificate.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Policy Extension

This CP does not require the certificate policy extension to be critical. Relying parties that do not process this extension do so at their own risk.

7.2 CERTIFICATE REVOCATION LIST PROFILE

7.2.1 Version Number

The CA shall issue CRLs in the X.509 v2 format (populate version field with integer "1"). .

7.2.2 CRL and CRL Entry Extensions

All end-entity PKI software must correctly process all CRL extensions identified in the CRL profile.

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

Changes to items within this CP that in the judgment of the PA will have no or minimal impact on the users using certificates and CRLs issued by the CA may be made with no change to the CP version number and no notification to the users.

Changes to the CP that in the judgment of the PA may have significant impact on the users using certificates and CRLs issued by this CA shall undergo a review and comment period of **60 days**. The PA will review all comments and respond individually or with further changes as appropriate. If the PA decides not to make any further changes after the review period, the initially-proposed modified document will be published in the Repository.

8.2 PUBLICATION AND NOTIFICATION POLICIES

A copy of this CP is available in electronic format from High Performance Computing Virtual Laboratory.

Authorized Subscribers and Relying Parties shall periodically check the Repository for notice of intended modifications to this CP document.

In order to allow entities to modify their procedures as needed, all changes to this CP shall become effective **15 days after final publication** on the Repository. It shall be the responsibility of Subscribers and Relying Parties to periodically check the Repository for notice of final publication of this CP.

Use of or reliance on a certificate after the above period (regardless of when the certificate was issued) shall be deemed as acceptance of the modified terms.

8.3 CERTIFICATION PRACTICE STATEMENT APPROVAL PROCEDURES

The PMA shall be responsible for determining if the CPS complies with this CP.