

**X.509 Certification Practice Statement**

**for the**

**VT Root**

**Certification Authority**

**March 28, 2006**

**OBJECT IDENTIFIER 1.3.6.1.4.1.6760.5.2.3.1. 1**

**Release 1.0, Version 0.0**

## **Identification and Validation of this Policy**

This Certification Practice Statement (CPS) has been assigned the global Object Identifier (OID) 1.3.6.1.4.1.6760.5.2.3.1.1. A Virginia Tech Certificate Authority (VTCA) MAY NOT SIGN ANY PUBLIC KEY CERTIFICATE (PKC) OR OTHER DOCUMENT THAT ASSERTS BY REFERENCE TO THIS OID ITS CONFORMANCE TO THIS CERTIFICATION PRACTICE STATEMENT UNLESS ALL ASPECTS OF ITS MANAGEMENT AND OPERATION CONFORM COMPLETELY WITH THE REQUIREMENTS CONTAINED HEREIN.

Minor modifications will be indicated by a suffix to this OID. Any significant changes to this policy, as determined by the Policy Management Authority (PMA), will result in a document with a different OID assignment.

A copy of this document is digitally signed using SHA-1 with RSA encryption and the private key associated with the authority certificate of the Virginia Tech Root CA, operating under this policy.

Identification: Virginia Polytechnic Institute and State University; VPI&SU; Virginia Tech

Data Universal Number System: 003137015

**Table of Contents**

- 1. INTRODUCTION ..... 1**
  - 1.1 OVERVIEW ..... 3
    - 1.1.1 Certificate Policy (CP) ..... 3
    - 1.1.2 Relationship between the CP and the CPS ..... 3
    - 1.1.3 Interoperation with CAs External to this Policy Domain..... 3
  - 1.2 IDENTIFICATION ..... 3
  - 1.3 COMMUNITY AND APPLICABILITY ..... 3
    - 1.3.1 PKI Authorities ..... 4
    - 1.3.2 Registration Authorities ..... 4
    - 1.3.3 End Entities ..... 4
    - 1.3.4 Applicability..... 4
  - 1.4 CONTACT DETAILS ..... 5
- 2. GENERAL PROVISIONS ..... 5**
  - 2.1 OBLIGATIONS ..... 5
    - 2.1.1 CA Obligations..... 5
    - 2.1.2 RA Obligations..... 5
    - 2.1.3 Subscriber Obligations ..... 6
    - 2.1.4 Relying Party Obligations ..... 6
    - 2.1.5 Repository Obligations..... 6
  - 2.2 LIABILITY ..... 6
    - 2.2.1 CA Liability ..... 6
    - 2.2.2 RA Liability ..... 6
  - 2.3 FINANCIAL CONSIDERATIONS ..... 6
    - 2.3.1 Fiduciary Relationships..... 6
    - 2.3.2 Administrative Processes ..... 6
  - 2.4 INTERPRETATION AND ENFORCEMENT..... 6
    - 2.4.1 Governing Law..... 6
    - 2.4.2 Severability, Survival, Merger, Notice..... 7
    - 2.4.3 Dispute Resolution Procedures ..... 7
    - 2.4.4 Section Headings..... 7
  - 2.5 FEES ..... 7
    - 2.5.1 Certificate Issuance or Renewal Fees..... 7
    - 2.5.2 Certificate Access Fees ..... 7
    - 2.5.3 Revocation or Status Information Access Fees ..... 7
    - 2.5.4 Fees for Other Services such as Policy Information ..... 7
    - 2.5.5 Refund Policy..... 7
  - 2.6 PUBLICATION AND REPOSITORY ..... 7
    - 2.6.1 Publication of CA Information..... 7
    - 2.6.2 Frequency of Publication ..... 7
    - 2.6.3 Access Controls..... 8
    - 2.6.4 Repositories..... 8

2.7	COMPLIANCE AUDIT .....	8
2.7.1	Frequency of Entity Compliance Audit .....	8
2.7.2	Identity/Qualifications of Auditor .....	8
2.7.3	Auditor's Relationship to Audited Party .....	8
2.7.4	Topics Covered by Audit .....	8
2.7.5	Actions taken as a result of deficiency .....	8
2.7.6	Communication of Results .....	8
2.8	CONFIDENTIALITY .....	8
2.8.1	Types of Information to be Kept Confidential .....	8
2.8.2	Types of Information Not Considered Confidential.....	9
2.8.3	Disclosure of Certificate Revocation Information .....	9
2.8.4	Release to Law Enforcement Officials.....	9
2.8.5	Release as Part of Civil Discovery .....	9
2.8.6	Disclosure upon Subscriber's Request.....	9
2.8.7	Other Information Release Circumstances .....	9
2.9	INTELLECTUAL PROPERTY RIGHTS .....	9
<b>3.</b>	<b>IDENTIFICATION AND AUTHENTICATION .....</b>	<b>9</b>
3.1	INITIAL REGISTRATION.....	9
3.1.1	Types of Names.....	9
3.1.2	Need for Names to be Meaningful .....	9
3.1.3	Rules for Interpreting Various Name Forms .....	9
3.1.4	Uniqueness of Names.....	10
3.1.5	Name Claim Dispute Resolution Procedure.....	10
3.1.6	Recognition, Authentication and Role of Trademarks .....	10
3.1.7	Method to Prove Possession of Private Key .....	10
3.1.8	Authentication of Organization Identity .....	10
3.1.9	Authentication of Individual Identity .....	10
3.1.10	Authentication of Component Identities .....	10
3.2	CERTIFICATE RENEWAL, UPDATE, AND ROUTINE REKEY .....	10
3.2.1	Certificate Rekey .....	10
3.2.2	Certificate Renewal .....	10
3.2.3	Certificate Update .....	10
3.3	OBTAINING A NEW CERTIFICATE AFTER REVOCATION .....	11
3.4	REVOCATION REQUEST .....	11
<b>4.</b>	<b>OPERATIONAL REQUIREMENTS .....</b>	<b>11</b>
4.1	APPLICATION FOR A CERTIFICATE .....	11
4.1.1	Delivery of Public Key for Certificate Issuance .....	11
4.2	CERTIFICATE ISSUANCE .....	11
4.2.1	Delivery of Subscriber's Private Key to Subscriber .....	11
4.3	CERTIFICATE ACCEPTANCE.....	11
4.4	CERTIFICATE SUSPENSION AND REVOCATION.....	11
4.4.1	Circumstances for Revocation of a Certificate.....	11
4.4.2	Who Can Request Revocation of a Certificate.....	11
4.4.3	Procedure for Revocation Request.....	11

4.4.4	Revocation Request Grace Period.....	11
4.4.5	Suspension.....	12
4.4.6	Who Can Request Suspension.....	<b>Error! Bookmark not defined.</b>
4.4.7	Procedure for Suspension Request.....	<b>Error! Bookmark not defined.</b>
4.4.8	Limits on Suspension Period.....	<b>Error! Bookmark not defined.</b>
4.4.9	Certificate Authority Revocation Lists / Certificate Revocation Lists.....	12
4.4.9.1	CARL/CRL Issuance Frequency .....	12
4.4.10	CARL/CRL Checking Requirements.....	12
4.4.11	Online Revocation / Status Checking Availability .....	12
4.4.12	Online Revocation Checking Requirements .....	12
4.4.13	Other Forms of Revocation Advertisements Available .....	12
4.4.14	Checking Requirements for Other Forms of Revocation Advertisements.....	12
4.4.15	Special Requirements Related to Key Compromise .....	12
4.5	SECURITY AUDIT PROCEDURE.....	13
4.5.1	Types of Events Recorded .....	13
4.5.2	Frequency of Processing Data.....	13
4.5.3	Retention Period for Security Audit Data .....	13
4.5.4	Protection of Security Audit Data .....	13
4.5.5	Security Audit Data Backup Procedures .....	13
4.5.6	Security Audit Collection System (Internal vs. External).....	13
4.5.7	Notification to Event Causing Subject.....	13
4.5.8	Vulnerability Assessments .....	14
4.6	RECORDS ARCHIVAL .....	14
4.6.1	Types of Events Archived.....	14
4.6.2	Retention Period for Archive .....	14
4.6.3	Protection of Archive .....	14
4.6.4	Archive Backup Procedures .....	14
4.6.5	Requirements for Time Stamping of Records .....	14
4.6.6	Archive Collection System (Internal or External).....	14
4.6.7	Procedures to Obtain and Verify Archive Information .....	14
4.7	KEY CHANGEOVER.....	14
4.8	COMPROMISE AND DISASTER RECOVERY .....	15
4.8.1	Computing Resources, Software, and/or Data Are Corrupted .....	15
4.8.1.1	Compromise Recovery .....	15
4.8.1.2	Disaster Recovery.....	15
4.8.2	CA Signature Keys Are Revoked.....	15
4.8.3	CA Signature Keys Are Compromised .....	15
4.8.4	Secure Facility Impaired after a Disaster .....	15
4.9	CA TERMINATION .....	15
<b>5.</b>	<b>PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS .....</b>	<b>15</b>
5.1	PHYSICAL CONTROLS FOR THE VTCA OR AUTHORIZED CA.....	15
5.1.1	Site Location and Construction .....	15
5.1.2	Electrical Power .....	15
5.1.3	Water Exposures .....	15
5.1.4	Fire Prevention and Protection.....	16
5.1.5	Media Storage .....	16
5.1.6	Waste Disposal.....	16

5.1.7	Offsite Backup .....	16
5.2	PROCEDURAL CONTROLS FOR THE VTCA .....	16
5.2.1	Trusted Roles .....	16
5.2.1.1	Certification Authority Administrator .....	16
5.2.1.2	Registration Authority Administrator (RAA).....	16
5.2.1.3	Other Trusted Roles.....	16
5.2.2	Number of Persons Required Per Task .....	16
5.2.3	Identification and Authentication for Each Role.....	17
5.3	PERSONNEL CONTROLS .....	17
5.3.1	Background, Qualifications, Experience, and Security Clearance Requirements.....	17
5.3.2	Background Check Procedures .....	17
5.3.3	Training Requirements.....	18
5.3.4	Retraining Frequency and Requirements .....	18
5.3.5	Job Rotation Frequency and Sequence.....	18
5.3.6	Sanctions for Unauthorized Actions .....	18
5.3.7	Contracting Personnel Requirements .....	18
5.3.8	Documentation Supplied to Personnel .....	18
<b>6.</b>	<b>TECHNICAL SECURITY CONTROLS.....</b>	<b>18</b>
6.1	KEY PAIR GENERATION AND INSTALLATION .....	18
6.1.1	Key Pair Generation by the Subscriber .....	18
6.1.2	Private Key Delivery to Subscriber.....	18
6.1.3	Public Key Delivery to Certificate Issuer .....	18
6.1.4	VTCA Public Key Availability .....	18
6.1.5	Key Sizes.....	19
6.1.6	Public Key Parameters Generation.....	19
6.1.7	Parameter Quality Checking .....	19
6.1.8	Hardware/Software Subscriber Key Pair Generation.....	19
6.1.9	Key Usage Purposes (as per X.509 v3).....	19
6.2	PRIVATE KEY PROTECTION.....	19
6.2.1	Standards for Cryptographic Module.....	19
6.2.2	CA Private Key Multi Person Control .....	19
6.2.3	Key Escrow of CA Private Signature Key .....	19
6.2.3.1	Escrow of End Entity Decryption Keys .....	19
6.2.4	Private Key Backup.....	19
6.2.4.1	Backup of CA Private Signature Key .....	19
6.2.4.2	Backup of End Entity Private Signature Key .....	19
6.2.5	Private Key Archival.....	20
6.2.6	Private Key Entry into Cryptographic Module .....	20
6.2.7	Method of Activating Private Keys.....	20
6.2.8	Methods of Deactivating Private Keys.....	20
6.2.9	Method of Destroying Subscriber Private Signature Keys .....	20
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	20
6.3.1	Public Key Archival.....	20
6.3.2	Usage Periods for the Public and Private Keys.....	20
6.4	ACTIVATION DATA.....	20
6.4.1	Activation Data Generation and Installation .....	20
6.4.2	Activation Data Protection .....	20

6.4.3	Other Aspects of Activation Data .....	20
6.5	COMPUTER SECURITY CONTROLS .....	21
6.5.1	Specific Computer Security Technical Requirements.....	21
6.5.2	Computer Security Rating.....	21
6.6	LIFE CYCLE TECHNICAL CONTROLS.....	21
6.6.1	System Development Controls.....	21
6.6.2	Security Management Controls.....	21
6.6.3	Life Cycle Security Ratings .....	21
6.7	NETWORK SECURITY CONTROLS .....	21
6.8	CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS .....	21
<b>7.</b>	<b>CERTIFICATE AND CARL/CRL PROFILES.....</b>	<b>21</b>
7.1	CERTIFICATE PROFILE.....	21
7.1.1	Version Numbers.....	21
7.1.2	Certificate Extensions .....	21
7.1.3	Algorithm Object Identifiers .....	22
7.1.4	Name Forms .....	22
7.1.5	Name Constraints .....	22
7.1.6	Certificate Policy Object Identifier .....	22
7.1.7	Usage of Policy Constraints extension.....	22
7.1.8	Policy Qualifiers Syntax and Semantics .....	22
7.1.9	Processing Semantics for the Critical Certificate Policy Extension.....	22
7.1.10	Certificate Serial Numbers.....	22
7.2	CARL/CRL PROFILE.....	22
7.2.1	Version Numbers.....	22
7.2.2	CARL and CRL Entry Extensions .....	22
7.2.3	OCSP Services .....	22
<b>8.</b>	<b>SPECIFICATION ADMINISTRATION.....</b>	<b>23</b>
8.1	SPECIFICATION CHANGE PROCEDURES.....	23
8.2	PUBLICATION AND NOTIFICATION POLICIES .....	23
8.2.1	Amendments Generally .....	23
8.2.2	Urgent Amendments Exception .....	23
8.2.3	Assent to Amendments.....	23
8.2.4	Maintenance of Prior Versions.....	23
8.3	CPS APPROVAL PROCEDURES .....	23
8.4	WAIVERS .....	23
<b>9.</b>	<b>BIBLIOGRAPHY .....</b>	<b>23</b>
	INTERNET X.509 PUBLIC KEY INFRASTRUCTURE CERTIFICATE AND CERTIFICATE REVOCATION LIST (CRL) PROFILE ,R. HOUSLEY, W. POLK, W. FORD, D. SOLO.....	24
<b>10.</b>	<b>GLOSSARY.....</b>	<b>26</b>
<b>11.</b>	<b>ACKNOWLEDGEMENTS.....</b>	<b>26</b>

RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	DATE RECEIVED	DATE ENTERED	SIGNATURE OF PERSON ENTERING CHANGE

## 1. INTRODUCTION

This Certification Practice Statement (CPS) defines the operational implementation of the terms and conditions, described in the Virginia Polytechnic Institute and State University (hereinafter Virginia Tech) Certificate Authority (VTCA) Certificate Policy identified by the object identifier 1.3.6.1.4.1.6760.5.2.1.1.1, for the VT Root Certificate Authority (RCA), a VTCA. Unless otherwise specified, all stipulations and requirements contained in this CPS are in addition to the VTCA CP with the CP taking precedence in the event of conflicting stipulations.

This CPS is structured in accordance with RFC 3647 [1]. Within this document the words **MUST**, **MUST NOT**, **REQUIRED**, **SHALL**, **SHALL NOT** **SHOULD**, **SHOULD NOT** **RECOMMENDED**, **MAY**, **OPTIONAL** are to be interpreted as in RFC 2119 [2].

### Acronyms

<b>ABADSG</b>	American Bar Association Digital Signature Guideline
<b>ANS</b>	Advanced Encryption Standard
<b>CA</b>	Certification Authority
<b>CAA</b>	Certification Authority Administrator
<b>CARL</b>	Certificate Authority Revocation List
<b>CN</b>	Common Name
<b>CP</b>	Certificate Policy
<b>CPS</b>	Certification Practice Statement
<b>CRIN</b>	Certificate Revocation Identification Number
<b>CRL</b>	Certificate Revocation List
<b>DES</b>	Data Encryption Standard
<b>DN</b>	Distinguished Name
<b>DPE</b>	Digital Processing Entity
<b>DSA/DSS</b>	Digital Signature Algorithm / Digital Signature Standard
<b>EDI</b>	Electronic Data Interface
<b>FIPS PUB</b>	(US) Federal Information Processing Standard Publication
<b>IETF</b>	Internet Engineering Task Force
<b>IRM</b>	Information Resource Management

<b>ISO</b>	International Standards Organization
<b>ITU</b>	International Telecommunications Union
<b>LOA</b>	Level of Assurance
<b>NIST</b>	National Institute of Standards and Technology
<b>NSA</b>	National Security Agency
<b>OCSP</b>	Online Certificate Status Protocol
<b>OID</b>	Object Identifier
<b>PIN</b>	Personal Identification Number
<b>PKC</b>	Public Key Certificate
<b>PKCS</b>	Public Key Certificate Standard
<b>PKI</b>	Public Key Infrastructure
<b>PKIX</b>	Public Key Infrastructure X.509
<b>PMA</b>	Policy Management Authority
<b>RA</b>	Registration Authority
<b>RAA</b>	Registration Authority Administrator
<b>RFC</b>	(IETF) Request for Comments
<b>RSA</b>	Rivest-Shimar-Adleman
<b>SHA-1</b>	Secure Hash Algorithm
<b>S/MIME</b>	Secure Multipurpose Internet Mail Extension
<b>SSL</b>	Secure Sockets Layer
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>TLS</b>	Transport Layer Security
<b>UPS</b>	Uninterrupted Power Supply
<b>URI</b>	Uniform Resource Identifier
<b>URL</b>	Uniform Resource Locator
<b>URN</b>	Uniform Resource Name

<b>vtBackup</b>	Internal Backup Utility
<b>VTCA</b>	Virginia Tech Certification Authority
<b>VTPKI</b>	Virginia Tech Public Key Infrastructure
<b>WWW</b>	World Wide Web

## **1.1 OVERVIEW**

This CPS defines the operational implementation of the requirements set forth by the VTCA CP.

This CPS is used by a PKC Relying Party to help in deciding whether a certificate and the information therein and the binding of that information to the Subject are sufficiently trustworthy for a particular application.

All PKCs issued by the RCA contain a valid reference to this CPS.

By relying on information contained in a PKC issued by the RCA, the Relying Party is agreeing with the provisions and stipulations of the VTCA CP and this CPS under which the PKC was issued.

### **1.1.1 Certificate Policy (CP)**

The RCA has digitally signed a copy of the VTCA CP, using SHA-1 with RSA encryption and its primary PKC signing key. The digitally signed copy of the RCA CPS is available online at <http://www.pki.vt.edu/rootca/cps> .

### **1.1.2 Relationship between the CP and the CPS**

No additional stipulations.

### **1.1.3 Interoperation with CAs External to this Policy Domain**

The RCA may interoperate with CAs external to this policy domain for the sole purpose of having the Virginia Tech Root Certificate signed by an external CA. The VT PKI PMA must explicitly approve any external CA signature.

## **1.2 IDENTIFICATION**

Each PKC issued by the RCA has the OID 1.3.6.1.4.1.6760.5.2.1.1.1, which identifies the VTCA CP document, in the PKC's *Certificate Policies* field. The PKC includes a URL reference to this CPS in the PKC's *CPSuri* field.

## **1.3 COMMUNITY AND APPLICABILITY**

The RCA serves as the root certificate authority within the VTPKI certificate hierarchy. Its sole function is to issue subordinate authority certificates within the VTPKI hierarchy.

**1.3.1 PKI Authorities**

The RCA has the authority to issue authority PKCs.

**1.3.2 Registration Authorities**

No additional stipulations

**1.3.3 End Entities**

The end entity that is the Subject of a PKC issued by the RCA under this policy is a subordinate authority certificate within the VTPKI hierarchy.

**1.3.4 Applicability**

A PKC certificate issued by the RCA is a subordinate authority certificate which provides certificate issuing services to a specific community. The requirements for issuing subordinate CA certificates are determined by the needs of different types of certificates within the university and are approved by the PMA. Only Relying Parties that accept in its entirety without any limitations (financial or otherwise) the VTCA CP and this CPS can make use of a PKC issued by the RCA.

The table below summarizes the recommended applicability of PKCs at each of the five levels of assurance covered by this document. The Level of Assurance specified in the authority certificate for the subordinate CA will be determined by the nature of the subordinate CA. Subordinate CAs created prior to the designation of the specific levels of assurance herein contain the policy identifier OID for the X.509 Certificate Policy for the Virginia Polytechnic Institute and State University Certification Authorities (1.3.6.1.4.1.6760.5.2.1.1.1).

<b>Assurance Level OID</b>	<b>Applicability</b>
Test 1.3.6.1.4.1.6760.5.2.2.1.1	This level is used for interoperability testing. It is solely used for this purpose and conveys no assurance information.
Rudimentary 1.3.6.1.4.1.6760.5.2.2.2.1	This level provides the lowest degree of assurance concerning identity of the Subject. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It may not be suitable for transactions requiring reliable authentication. It is generally insufficient for transactions requiring strong confidentiality, but may be used when certificates having higher levels of assurance are unavailable.
Basic	This level provides a basic level of assurance relevant to

1.3.6.1.4.1.6760.5.2.2.3.1	environments where there are risks and consequences of data compromise, but they are not considered to result in significant negative consequences. It is assumed at this security level that users are not likely to be malicious.
Medium 1.3.6.1.4.1.6760.5.2.2.4.1	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud.
High 1.3.6.1.4.1.6760.5.2.2.5.1	This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

## 1.4 CONTACT DETAILS

Questions about interpretation of this CPS are directed in writing to Information Resource Management. Concerns about possible abuse of this CPS, are directed in writing to the Virginia Tech Public Key Infrastructure Policy Management Authority (VTPKI PMA).

Information Resource Management  
1700 Pratt Dr.  
Blacksburg, VA 24060

Chair, VTPKI PMA  
1700 Kraft Dr.  
Suite 2000  
Blacksburg, VA 24060

## 2. GENERAL PROVISIONS

### 2.1 OBLIGATIONS

By making use of a subordinate authority PKC issued by the RCA within the VTPKI infrastructure, a Relying Party is accepting its obligations hereunder.

#### 2.1.1 CA Obligations

No additional stipulations.

#### 2.1.2 RA Obligations

No additional stipulations.

### **2.1.3 Subscriber Obligations**

In addition to the obligations stipulated in the VTCA CP, a Subscriber:

- adheres to or complies with the terms and conditions of this CPS
- adheres to or complies with the Usage Terms and Conditions described in the VT Subordinate CA CPS documents
- notifies Information Resource Management immediately upon either suspected or known compromise of the private key associated with a PKC issued by the RCA

### **2.1.4 Relying Party Obligations**

No additional stipulations

### **2.1.5 Repository Obligations**

No additional stipulations.

## **2.2 LIABILITY**

### **2.2.1 CA Liability**

No additional stipulations.

### **2.2.2 RA Liability**

No additional stipulations.

## **2.3 FINANCIAL CONSIDERATIONS**

No additional stipulations.

### **2.3.1 Fiduciary Relationships**

No additional stipulations.

### **2.3.2 Administrative Processes**

No additional stipulations.

## **2.4 INTERPRETATION AND ENFORCEMENT**

Interpretation of this CPS is the responsibility of the PMA and Information Resource Management.

### **2.4.1 Governing Law**

No additional stipulations.

#### **2.4.2 Severability, Survival, Merger, Notice**

No additional stipulations.

#### **2.4.3 Dispute Resolution Procedures**

No additional stipulations.

#### **2.4.4 Section Headings**

No additional stipulations.

### **2.5 Fees**

#### **2.5.1 Certificate Issuance or Renewal Fees**

No fee is charged for this service.

#### **2.5.2 Certificate Access Fees**

No fee is charged for this service.

#### **2.5.3 Revocation or Status Information Access Fees**

No fee is charged for this service.

#### **2.5.4 Fees for Other Services such as Policy Information**

No fee is charged for this service.

#### **2.5.5 Refund Policy**

No additional stipulations.

### **2.6 PUBLICATION AND REPOSITORY**

All information about the operation of the RCA and the PKCs it issues are available online, except as indicated in this section. Each PKC issued includes information sufficient to locate this online Repository.

#### **2.6.1 Publication of CA Information**

No additional stipulations.

#### **2.6.2 Frequency of Publication**

PKCs issued by the RCA are made available on the [www.pki.vt.edu](http://www.pki.vt.edu) website as part of the issuance process. Changes to this CPS are published as soon as they are approved by the PMA. Previous versions remain available online 365 days beyond the latest expiration date of any PKC that references this CPS.

Archived copies of all CPSs for which the RCA has ever issued a PKC are kept in accordance with the Commonwealth of Virginia records retention policy.

### **2.6.3 Access Controls**

There are no limitations on access to this CPS and PKCs issued by the RCA.

### **2.6.4 Repositories**

The repository is reliably web accessible.

## **2.7 COMPLIANCE AUDIT**

No additional stipulations.

### **2.7.1 Frequency of Entity Compliance Audit**

No additional stipulations.

### **2.7.2 Identity/Qualifications of Auditor**

No additional stipulations.

### **2.7.3 Auditor's Relationship to Audited Party**

No additional stipulations.

### **2.7.4 Topics Covered by Audit**

No additional stipulations.

### **2.7.5 Actions taken as a result of deficiency**

No additional stipulations.

### **2.7.6 Communication of Results**

No additional stipulations.

## **2.8 CONFIDENTIALITY**

No additional stipulations.

### **2.8.1 Types of Information to be Kept Confidential**

No additional stipulations.

### **2.8.2 Types of Information Not Considered Confidential**

No additional stipulations.

### **2.8.3 Disclosure of Certificate Revocation Information**

No additional stipulations.

### **2.8.4 Release to Law Enforcement Officials**

No additional stipulations.

### **2.8.5 Release as Part of Civil Discovery**

No additional stipulations.

### **2.8.6 Disclosure upon Subscriber's Request**

No additional stipulations.

### **2.8.7 Other Information Release Circumstances**

No additional stipulations.

## **2.9 INTELLECTUAL PROPERTY RIGHTS**

No additional stipulations.

## **3. IDENTIFICATION AND AUTHENTICATION**

### **3.1 INITIAL REGISTRATION**

Initial registration requires prior approval by the PMA.

#### **3.1.1 Types of Names**

A Subject name is present in all PKCs issued by the RCA and conforms to Section 3.1.3.

#### **3.1.2 Need for Names to be Meaningful**

The CN component of a Subject name in a PKC issued by the RCA identifies the subordinate CA and represents the certificate services it provides.

#### **3.1.3 Rules for Interpreting Various Name Forms**

The Subject names of a PKC must be in the following format:

A

CN = < name of subordinate CA as determined by the PMA > ,

O = Virginia Polytechnic Institute and State University,

C = US,  
DC = vt,  
DC = edu

### **3.1.4 Uniqueness of Names**

The CN component of a Subject name in a PKC refers to a unique and identifiable subordinate CA. Including the serial number that is assigned by the CA ensures the uniqueness of the Subject name. A unique Subject name is not reused.

### **3.1.5 Name Claim Dispute Resolution Procedure**

No additional stipulations.

### **3.1.6 Recognition, Authentication and Role of Trademarks**

No additional stipulations.

### **3.1.7 Method to Prove Possession of Private Key**

The subordinate CA CSR provides proof of the corresponding private key possession.

### **3.1.8 Authentication of Organization Identity**

No additional stipulations.

### **3.1.9 Authentication of Individual Identity**

The identity of the subordinate CA is authenticated by the PMA.

### **3.1.10 Authentication of Component Identities**

No additional stipulations.

## **3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE REKEY**

### **3.2.1 Certificate Rekey**

PKCs issued by the RCA are rekeyed ten years after issuance. Rekeying a PKC means that a new PKC is created that has the same characteristics as the old one, except that the new PKC has a new, different public key (corresponding to a new, different private key), and a different serial number.

### **3.2.2 Certificate Renewal**

PKCs issued by the RCA are not renewed.

### **3.2.3 Certificate Update**

PKCs issued by the RCA are not updated.

### **3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION**

No additional stipulations.

### **3.4 REVOCATION REQUEST**

The RCA revokes certificates upon PMA approval or request.

## **4. OPERATIONAL REQUIREMENTS**

### **4.1 APPLICATION FOR A CERTIFICATE**

#### **4.1.1 Delivery of Public Key for Certificate Issuance**

A PEM encoded the CSR containing the public key of a subordinate CA is submitted using external storage media to the RCA for approval and issuance.

### **4.2 CERTIFICATE ISSUANCE**

#### **4.2.1 Delivery of Subscriber's Private Key to Subscriber**

The RCA does not deliver private keys to the subordinate CAs, hence keys are generated onboard a FIPS 140-2 Level 3 hardware security module.

### **4.3 CERTIFICATE ACCEPTANCE**

Upon issuance of the PKC by the RCA, the certificate is exported using removable external storage media.

### **4.4 CERTIFICATE SUSPENSION AND REVOCATION**

The RCA revokes PKCs at the request and approval of the PMA. The RCA does not suspend PKCs that it issues.

#### **4.4.1 Circumstances for Revocation of a Certificate**

No additional stipulations.

#### **4.4.2 Who Can Request Revocation of a Certificate**

No additional stipulations.

#### **4.4.3 Procedure for Revocation Request**

No additional stipulations.

#### **4.4.4 Revocation Request Grace Period**

No additional stipulations.

#### **4.4.5 Suspension**

No additional stipulations.

#### **4.4.6 Who Can Request Suspension**

The RCA does not suspend PKCs that it issues.

#### **4.4.7 Procedure for Suspension Request**

The RCA does not suspend PKCs that it issues.

#### **4.4.8 Limits on Suspension Period**

The RCA does not suspend PKCs that it issues.

#### **4.4.9 Certificate Authority Revocation Lists / Certificate Revocation Lists**

The RCA does issue Certificate Authority Revocations Lists (CARL).

##### **4.4.9.1 CARL/CRL Issuance Frequency**

CARLs are issued as needed.

##### **4.4.10 CARL/CRL Checking Requirements**

CARLs are published as part of the issuance procedure to the [www.pki.vt.edu](http://www.pki.vt.edu) website.

##### **4.4.11 Online Revocation / Status Checking Availability**

No additional stipulations.

##### **4.4.12 Online Revocation Checking Requirements**

No additional stipulations.

##### **4.4.13 Other Forms of Revocation Advertisements Available**

No additional stipulations.

##### **4.4.14 Checking Requirements for Other Forms of Revocation Advertisements**

No additional stipulations.

##### **4.4.15 Special Requirements Related to Key Compromise**

No additional stipulations.

## **4.5 SECURITY AUDIT PROCEDURE**

### **4.5.1 Types of Events Recorded**

Logfiles are created either electronically or manually and include, but are not restricted to, the following events:

- system logfiles
  - startup/shutdown of system
  - changes to user accounts
  - backup and log information
  - tasks performed by users with trusted roles
- CA logfiles
  - certification requests
  - issued certificates
  - issued CRLs

The RCA database is configured to log connections made to the database, queries, query results, and errors. The database logs contain date and time of the database event.

### **4.5.2 Frequency of Processing Data**

The audit log is consolidated and reviewed upon request of the auditors.

### **4.5.3 Retention Period for Security Audit Data**

The RCA retains audit logs of a minimum period consistent with policies established by the university.

### **4.5.4 Protection of Security Audit Data**

Access to audit logs is controlled by IRM, and access is restricted to authorized employees only.

### **4.5.5 Security Audit Data Backup Procedures**

The audit log is backed up immediately after subordinate CA key generation ceremonies using a backup utility (vtBackup) which was developed at Virginia Tech. Backup audit logs of the RCA are protected against unauthorized viewing, modification, or deletion by encrypting the backup and using offsite storage in a separate secure location from the RCA host.

### **4.5.6 Security Audit Collection System (Internal vs. External)**

The audit trail collection system is internal to the RCA and operating system software. Both onsite and offsite secure storage facilities are used to maintain the audit trail logs.

### **4.5.7 Notification to Event Causing Subject**

No additional stipulations.

#### **4.5.8 Vulnerability Assessments**

The audit logs will be inspected upon request of the auditors.

### **4.6 RECORDS ARCHIVAL**

#### **4.6.1 Types of Events Archived**

No additional stipulations.

#### **4.6.2 Retention Period for Archive**

No additional stipulations.

#### **4.6.3 Protection of Archive**

Archived records are protected against unauthorized viewing, modification, and deletion by using cryptographic protection and offsite storage in a physically secure and trustworthy location. The cryptographic protection is implemented using a 512 bit DES3 symmetric key that is unique to each backup instance. The DES3 symmetric key is then encrypted using 4096 bit RSA public key encryption.

#### **4.6.4 Archive Backup Procedures**

No additional stipulations.

#### **4.6.5 Requirements for Time Stamping of Records**

System Time is monitored on a regular basis.

#### **4.6.6 Archive Collection System (Internal or External)**

No additional stipulations.

#### **4.6.7 Procedures to Obtain and Verify Archive Information**

On request by the auditors, the VT Root CA Administrator will retrieve media containing archived information from the offsite storage location. The VT Root CA Administrator maintains the record of where backups are stored as part of the VTCA Resource Inventory document. To view the CA archive, it must be decrypted. The private key needed to decrypt the symmetric key used to encrypt the backups is stored on zip disk labeled "Backup Encryption RSA Key Pair" at the offsite storage location. A duplicate copy of the private key is stored on a BIO drive kept in a locked file cabinet in the eProvisioning office area.

### **4.7 KEY CHANGEOVER**

No additional stipulations.

## **4.8 COMPROMISE AND DISASTER RECOVERY**

### **4.8.1 Computing Resources, Software, and/or Data Are Corrupted**

#### **4.8.1.1 Compromise Recovery**

No additional stipulations.

#### **4.8.1.2 Disaster Recovery**

No additional stipulations.

### **4.8.2 CA Signature Keys Are Revoked**

No additional stipulations.

### **4.8.3 CA Signature Keys Are Compromised**

No additional stipulations.

### **4.8.4 Secure Facility Impaired after a Disaster**

The RCA disaster recovery plan is provided by the Office of the Vice President for Information Technology.

## **4.9 CA TERMINATION**

No additional stipulations.

## **5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS**

### **5.1 PHYSICAL CONTROLS FOR THE VTCA OR AUTHORIZED CA**

#### **5.1.1 Site Location and Construction**

The RCA operations center is located in room 118 of the Andrews Information Systems Building. The RCA operations center has been designed to provide a physically protected environment that deters, detects, and prevents unauthorized use of, access to, and disclosure of sensitive information and systems. Access to the building and to the operations center is protected by procedural as well as technical control measures. The facility is further protected using biometric access devices and camera monitoring systems.

#### **5.1.2 Electrical Power**

The RCA operations center operates its own backup generator to provide a fail safe power supply in the event of power failure.

#### **5.1.3 Water Exposures**

No additional stipulations.

#### **5.1.4 Fire Prevention and Protection**

A fire prevention, detection and suppression system is installed to meet security and safety measure at the RCA facility.

#### **5.1.5 Media Storage**

The encrypted backup media of the RCA are stored in an offsite physically secure and trustworthy location.

#### **5.1.6 Waste Disposal**

Records containing sensitive information are destroyed in a manner to prevent the unauthorized access to the information. Paper shredders are available throughout the facility.

#### **5.1.7 Offsite Backup**

In the event of a system failure there are sufficient backups that can be used to restore the RCA system. These backups are made immediately after every subordinate CA key signing ceremony or other modifications to the RCA using the vtBackup utility. The three most recent full backups are stored at a secure offsite location which can only be accessed by authorized personnel.

### **5.2 PROCEDURAL CONTROLS FOR THE VTCA**

#### **5.2.1 Trusted Roles**

No additional stipulation.

##### **5.2.1.1 Certification Authority Administrator**

The Certification Authority Administrator (CAA) role is appointed by the Office of the Vice President for Information Technology. The CAA's responsibilities are:

- certificate generation and revocation
- CRL generation
- certificate profile, certificate template, and audit parameter configuration
- administration of the RCA Hardware Security Module

##### **5.2.1.2 Registration Authority Administrator (RAA)**

The Registration Authority Administrator (RAA) role is constituted by the PMA. The PMA accepts requests to implement a subordinate CA and is responsible for reviewing the request and insuring a CPS has been written and approved.

##### **5.2.1.3 Other Trusted Roles**

No additional stipulations.

#### **5.2.2 Number of Persons Required Per Task**

No additional stipulations.

### **5.2.3 Identification and Authentication for Each Role**

Identification and authentication for RCA personnel follow requirements identified in sections 5.3, 5.3.1, and 5.3.2. The items in these sections are performed before RCA personnel are:

- authorized for access to the RCA site
- authorized for physical access to the RCA system
- given a certificate and account on the RCA system for the performance of their role

Each of these certificates and accounts (with the exception of RCA signing certificates) are:

- directly attributable to an individual
- NOT shared
- restricted to actions authorized for that role through the use of the RCAs
- software, operating system, and procedural controls

RCA operations are secured, using mechanisms such as token based strong authentication and encryption, when accessed across a shared network.

## **5.3 PERSONNEL CONTROLS**

Personnel performing duties with respect to the operation of the RCA are:

- known and appointed by the Vice President for Information Technology
- trained with respect to the duties they are to perform
- NOT assigned duties that may cause a conflict of interest with their RCA duties.

### **5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements**

All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity.

### **5.3.2 Background Check Procedures**

All persons filling trusted roles as described in Sections 5.2.1, 5.2.1.1, 5.2.1.2 and 5.2.1.3 of this CPS are required to have a background check. Such checks are to be performed solely to determine the suitability of a person to fill a RCA role and are not released except as required by law.

The Department of Human Resources will perform background check procedures for these employees. Using social security verification, criminal history checks will be made in all localities where the search indicates the employee has resided. For resident aliens, a criminal history check will be made with the country of origin.

Factors revealed in a background check that may be considered grounds for rejecting candidates for trusted positions or for taking action against existing trusted persons generally include:

- misrepresentations made by the candidate or trusted person
- highly unfavorable or unreliable professional references
- certain criminal convictions

### **5.3.3 Training Requirements**

No additional stipulation.

### **5.3.4 Retraining Frequency and Requirements**

No additional stipulation.

### **5.3.5 Job Rotation Frequency and Sequence**

No additional stipulation.

### **5.3.6 Sanctions for Unauthorized Actions**

The PMA initiates appropriate administrative and disciplinary actions against personnel who have performed unauthorized actions involving the RCA or its Repository.

### **5.3.7 Contracting Personnel Requirements**

No additional stipulations.

### **5.3.8 Documentation Supplied to Personnel**

No additional stipulations.

## **6. TECHNICAL SECURITY CONTROLS**

### **6.1 KEY PAIR GENERATION AND INSTALLATION**

#### **6.1.1 Key Pair Generation by the Subscriber**

During a key generation ceremony, the RSA cryptographic keys are generated onboard a FIPS 140-2 Level 3 hardware security module. A hardware based random number generator is used to generate the RSA keys.

#### **6.1.2 Private Key Delivery to Subscriber**

The private key is generated onboard a hardware security module and therefore does not need to be delivered.

#### **6.1.3 Public Key Delivery to Certificate Issuer**

The Public Key is encrypted in a CSR and delivered to the RCA using removable storage media.

#### **6.1.4 VTCA Public Key Availability**

No additional stipulations.

### **6.1.5 Key Sizes**

Key sizes have a minimum of 4096 bits.

### **6.1.6 Public Key Parameters Generation**

No additional stipulations.

### **6.1.7 Parameter Quality Checking**

No additional stipulations.

### **6.1.8 Hardware/Software Subscriber Key Pair Generation**

No additional stipulations.

### **6.1.9 Key Usage Purposes (as per X.509 v3)**

No additional stipulations.

## **6.2 PRIVATE KEY PROTECTION**

### **6.2.1 Standards for Cryptographic Module**

The RCA follows the FIPS 140-2 Level 3 specification.

### **6.2.2 CA Private Key Multi Person Control**

Multi person control is implemented using an M of N authentication scheme. It also requires additional authentication from a separate person.

### **6.2.3 Key Escrow of CA Private Signature Key**

The RCA does not escrow private keys.

#### **6.2.3.1 Escrow of End Entity Decryption Keys**

The RCA does not escrow decryption keys.

### **6.2.4 Private Key Backup**

No additional stipulations.

#### **6.2.4.1 Backup of CA Private Signature Key**

No additional stipulations.

#### **6.2.4.2 Backup of End Entity Private Signature Key**

The RCA does not backup subordinate CA private signature keys.

### **6.2.5 Private Key Archival**

The RCA does not archive subordinate CA private keys.

### **6.2.6 Private Key Entry into Cryptographic Module**

No additional stipulations.

### **6.2.7 Method of Activating Private Keys**

No additional stipulations.

### **6.2.8 Methods of Deactivating Private Keys**

No additional stipulations.

### **6.2.9 Method of Destroying Subscriber Private Signature Keys**

No additional stipulations.

## **6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT**

### **6.3.1 Public Key Archival**

No additional stipulations.

### **6.3.2 Usage Periods for the Public and Private Keys**

No additional stipulations.

## **6.4 ACTIVATION DATA**

### **6.4.1 Activation Data Generation and Installation**

No additional stipulations.

### **6.4.2 Activation Data Protection**

The RCA uses a hardware security module (HSM) that is certified as FIPS 140-2 level 3. The HSM implements strong multifactor M of N authentication . This requires the RCA CAAs to use M of N key tokens in addition to another token that is PIN protected in order to access the private area of the HSM which contains the RCA public/private key pair.

### **6.4.3 Other Aspects of Activation Data**

No additional stipulations.

## **6.5 COMPUTER SECURITY CONTROLS**

### **6.5.1 Specific Computer Security Technical Requirements**

No additional stipulations.

### **6.5.2 Computer Security Rating**

No additional stipulations.

## **6.6 LIFE CYCLE TECHNICAL CONTROLS**

### **6.6.1 System Development Controls**

No additional stipulations.

### **6.6.2 Security Management Controls**

No additional stipulations.

### **6.6.3 Life Cycle Security Ratings**

No additional stipulations.

## **6.7 NETWORK SECURITY CONTROLS**

No additional stipulations.

## **6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS**

No additional stipulations.

## **7. CERTIFICATE AND CARL/CRL PROFILES**

### **7.1 CERTIFICATE PROFILE**

The certificate profiles for the RCA and the subordinate CA certificates issued by the RCA are published at <http://www.pki.vt.edu/vtroot/cps/>.

#### **7.1.1 The profiles for the CA certificates issued by the VT Root CA**

No additional stipulations.

#### **7.1.2 Certificate Extensions**

Standard extensions, when populated, are described in an appropriate Certificate Profile.

PKCs issued by the RCA have the following values in their *Key Usage* field:

- keyCertSign

- cRLSign

### **7.1.3 Algorithm Object Identifiers**

No additional stipulations.

### **7.1.4 Name Forms**

No additional stipulations.

### **7.1.5 Name Constraints**

No additional stipulations.

### **7.1.6 Certificate Policy Object Identifier**

No additional stipulations.

### **7.1.7 Usage of Policy Constraints extension**

No additional stipulations.

### **7.1.8 Policy Qualifiers Syntax and Semantics**

No additional stipulations.

### **7.1.9 Processing Semantics for the Critical Certificate Policy Extension**

No additional stipulations.

### **7.1.10 Certificate Serial Numbers**

No additional stipulations.

## **7.2 CARL/CRL PROFILE**

### **7.2.1 Version Numbers**

The RCA will issue CARLs or CRLs.

### **7.2.2 CARL and CRL Entry Extensions**

No additional stipulations.

### **7.2.3 OCSP Services**

No additional stipulations.

## **8. SPECIFICATION ADMINISTRATION**

### **8.1 SPECIFICATION CHANGE PROCEDURES**

No additional stipulation.

### **8.2 PUBLICATION AND NOTIFICATION POLICIES**

The RCA will notify its subscribers of any changes to the certificate policy via the VT Root Announce List.

#### **8.2.1 Amendments Generally**

The PMA and the sponsor of the RCA may jointly amend this CPS prospectively but not retroactively.

#### **8.2.2 Urgent Amendments Exception**

An amendment that is deemed “urgent” becomes effective immediately. “Urgent” will be designated if, in the sole discretion of the PMA, failure to make the amendment may result in a compromise of the RCA or services dependent on it.

#### **8.2.3 Assent to Amendments**

No additional stipulations.

#### **8.2.4 Maintenance of Prior Versions**

No additional stipulations.

### **8.3 CPS APPROVAL PROCEDURES**

No additional stipulation.

### **8.4 WAIVERS**

No additional stipulations.

## **9. BIBLIOGRAPHY**

The following documents can be used for guidance in the interpretation of this CPS:

ABADSG	Digital Signature Guidelines, 1996-08-01. <a href="http://www.abanet.org/scitech/ec/isc/dsgfree.html">http://www.abanet.org/scitech/ec/isc/dsgfree.html</a> .
FIPS 112	Password Usage, 1985-05-30 <a href="http://www.itl.nist.gov/fipspubs/fip112.htm">http://www.itl.nist.gov/fipspubs/fip112.htm</a>
FIPS 140-2	Security Requirements for Cryptographic Modules, <a href="http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf">http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf</a>

FIPS 180-1      Secure Hash Standard, 1995-04-17  
<http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf>

FIPS 186-2      Digital Signature Standard, 2001-01-27

FOIACT          5 U.S.C. 552, Freedom of Information Act.  
<http://www4.law.cornell.edu/uscode/5/552.html>  
 Federal Certificate Profile DRAFT, April 2000  
[http://csrc.nist.gov/pki/documents/FPKI\\_Certificate\\_Profile\\_20000418.xls](http://csrc.nist.gov/pki/documents/FPKI_Certificate_Profile_20000418.xls)

ISO9594-8      Information Technology-Open Systems Interconnection-The Directory:  
 Authentication Framework, 1997.

ITMRA           40 U.S.C. 1452, Information Technology Management Reform Act of 1996.  
<http://www4.law.cornell.edu/uscode/40/1452.html>

NAG69C         Information System Security Policy and Certification Practice Statement for  
 Certification Authorities, rev C, November 1999.

NSD42          National Policy for the Security of National Security Telecom and Information  
 Systems, 5 Jul 1990.  
[http://www.cpsr.org/cpsr/privacy/computer\\_security/nsd\\_42.txt](http://www.cpsr.org/cpsr/privacy/computer_security/nsd_42.txt)  
 (redacted version)

NS4005         NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.

NS4009         NSTISSI 4009, National Information Systems Security Glossary, January 1999.

PKCS           Public Key Cryptography Standards  
<http://www.rsasecurity.com/rsalabs/pkcs/index.html>

PKCS-12        Personal Information Exchange Syntax Standard, April 1997.  
<http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/>

RFC 2510       Certificate Management Protocol, Adams and Farrell, March 1999.

RFC 2527       Certificate Policy and Certificate Practices Framework, Chokhani and Ford, March  
 1999.

RFC 3280       INTERNET X.509 PUBLIC KEY INFRASTRUCTURE CERTIFICATE AND  
 CERTIFICATE REVOCATION LIST (CRL) PROFILE ,R. HOUSLEY, W. POLK,  
 W. FORD, D. SOLO.  
 Planning for PKI, Russ Housley, Tim Polk, Willey, John Wiley & Sons; 1 edition  
 (March 13, 2001), ISBN: 0471397024  
 Security Requirements for Certificate Issuing and Management Components, 3

November 1999, Draft

“Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption”, Warwick Ford and Michael S. Baum, Prentice Hall, April 1997, ISBN: 0134763424

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

## 10 GLOSSARY

<b>Activation Data</b>	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
<b>Applicant</b>	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
<b>Arc</b>	An arc is an individual subtree of an Object Identifier (OID) tree.
<b>Archive</b>	Long term, physically separate storage.
<b>Audit</b>	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]
<b>Audit Data</b>	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
<b>Authenticate</b>	To confirm the identity of an entity when that identity is presented.
<b>Authentication</b>	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
<b>Authority certificate</b>	A PKC that contains the distinguished name of the CA in the <i>SubjectName</i> field and contains the value TRUE in the <i>BasicConstraints CA</i> field and in which the <i>KeyUsage keyCertSign</i> bit is set. The <i>cRLSign</i> bit should be set also.
<b>Authorized CA</b>	A CA for which another CA signs an authority certificate in accordance with this CP.
<b>Backup</b>	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
<b>Binding</b>	Process of associating two related elements of information. [NS4009]
<b>Certificate</b>	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG] As used in this CP, the term "Certificate" refers to certificates that expressly reference the OID of this CP in the "Certificate Practices Statement" (CPS) referenced in the <i>CPSuri</i> field of

	an X.509 v.3 certificate
<b>Certificate Policy (CP)</b>	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
<b>Certificate Revocation List (CRL)</b>	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
<b>Certificate Status Authority</b>	A trusted entity that provides online verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
<b>Certificate Related Information</b>	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
<b>Certification Authority (CA)</b>	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs. The term "CA" as used in this CPS includes Authorizing and Authorized CAs that operate under this CPS.
<b>Certification Authority Revocation List (CARL)</b>	A signed, time stamped list of serial numbers of CA public key certificates, including cross certificates that have been revoked.
<b>Certification Practice Statement (CPS)</b>	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CPS, or requirements specified in a contract for services).
<b>Client (application)</b>	A system entity, usually a computer process acting on behalf of a human user, who makes use of a service provided by a server.
<b>Community</b>	The community or group of individuals or other entities for which the CA will issue a PKC.
<b>Compromise</b>	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
<b>Confidentiality</b>	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]

<b>CPSuri</b>	A PKC standard extension that provides a URI pointing to an online copy of the CA's CPS.
<b>Cross Certificate</b>	A PKC used to establish a trust relationship between two CAs.
<b>Cryptographic Module</b>	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
<b>Cryptoperiod</b>	Time span during which each key setting remains in effect. [NS4009]
<b>Data Integrity</b>	Assurance that the data are unchanged from creation to reception.
<b>Department Head</b>	Department Head refers to any position that functions as the administrative head of a department or program and includes titles such as, department chairs, institute or center directors, or other administrators.
<b>Digital Signature</b>	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
<b>Dual Use Certificate</b>	A certificate that is intended for use with both digital signature and data encryption services.
<b>Encryption Certificate</b>	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
<b>End Entity</b>	Relying Parties and Subscribers.
<b>Firewall</b>	Gateway that limits access between networks in accordance with local security policy. [NS4009]
<b>Integrity</b>	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
<b>Intellectual Property</b>	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
<b>Intermediate CA</b>	A CA that is subordinate to another CA and has a CA subordinate to itself.

<b>Issuer</b>	The issuer is the entity who has signed and issued the certificate.
<b>Key Escrow</b>	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
<b>Key Exchange</b>	The process of exchanging public keys in order to establish secure communications.
<b>Key Generation Material</b>	Random numbers, pseudo random numbers, and cryptographic parameters used in generating cryptographic keys.
<b>Key Pair</b>	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
<b>LOA</b>	Level of Assurance. Certificates are differentiated by the level of assurance they provide regarding the identity of the subject entry named in the certificate. The assurance level depends on how a subject's identity is verified during the certification request process.
<b>Naming Authority</b>	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
<b>Non Repudiation</b>	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non repudiation refers to how well possession or control of the private signature key can be established.
<b>Object Identifier (OID)</b>	A unique specially formatted number that is composed of a most significant part assigned by an internationally recognized standards organization to a specific owner and a least significant part assigned by the owner of the most significant part. For example, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Higher Education PKI, they are used to uniquely identify policies and cryptographic algorithms and possibly other elements contained in a PKC.
<b>Out-of-Band</b>	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S.

	Postal Service mail to communicate with another party where current communication is occurring online).
<b>Outside Threat</b>	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
<b>PKC</b>	Public Key Certificate. As used in this CP, refers to an object conforming to X.509v3 or higher.
<b>PKI Sponsor</b>	Fills the role of a Subscriber for non human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
<b>Policy Management Authority (PMA)</b>	A group established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
<b>Private Key</b>	The key of a signature key pair used to create a digital signature. Also, the key of an encryption key pair that is used to decrypt confidential information. In both cases, this key <b>MUST</b> be kept secret.
<b>Public Key</b>	The key of a signature key pair used to validate a digital signature. Also, the key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
<b>Public Key Infrastructure</b>	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public private key pairs including the ability to issue, maintain, and revoke public key certificates.
<b>Registration Authority</b>	An entity that is responsible for identification and authentication of certificate subjects but does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
<b>Rekey (a certificate)</b>	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
<b>Relying Party</b>	An individual who has received information that includes a PKC and a digital signature verifiable with reference to a public key listed in the PKC and is in a position to rely on that information.
<b>Renew (a certificate)</b>	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

<b>Repository</b>	A database containing information and data relating to certificates as specified in this CPS and may also be referred to as a directory.
<b>Responsible Individual</b>	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
<b>Revoke a Certificate</b>	To prematurely end the operational period of a certificate effective at a specific date and time.
<b>Risk</b>	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
<b>Risk Tolerance</b>	The level of risk an entity is willing to assume in order to achieve a potential desired result.
<b>Root CA</b>	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
<b>Server</b>	A system entity that provides a service in response to requests from clients.
<b>Signature Certificate</b>	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
<b>Subject</b>	The Subject is the entity associated with the public key stored in the subject public key field of the certificate.
<b>Subordinate CA</b>	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA and whose activities are constrained by that other CA. (See Superior CA).
<b>Subscriber</b>	A Subscriber is an individual who (1) either (a) is the Subject named or identified in a certificate issued to that individual or (b) is the owner or operator of an entity that is the Subject named or identified in a certificate issued to that individual and (2) holds a private key that corresponds to the public key listed in the certificate.
<b>Superior CA</b>	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA and who constrains the activities of that CA. (See Subordinate CA).
<b>Technical non repudiation</b>	The public key mechanisms that contribute technical evidence supporting a non repudiation security service.
<b>Trust List</b>	Collection of trusted certificates used by Relying Parties to authenticate other certificates.

<b>Trusted Agent</b>	Entity authorized to act as a representative of an institution in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
<b>Trusted Certificate</b>	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a “trust anchor.”
<b>Trusted Timestamp</b>	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
<b>Trustworthy System</b>	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
<b>Two Person Control</b>	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]
<b>Update (a certificate)</b>	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
<b>URI</b>	A Uniform Resource Identifier is a compact string of characters for identifying an abstract or physical resource. It is a superset of URLs and URNs and may include other UR types. See RFC2396.
<b>URL</b>	A Uniform Resource Locator refers to the subset of URI that identify resources via a representation of their primary access mechanism (e.g., their network "location") rather than identifying the resource by name or by some other attribute(s) of that resource. See RFC1738 and RFC1808.

<b>URN</b>	A Uniform Resource Name refers to the subset of URI that is required to remain globally unique and persistent even when the resource ceases to exist or becomes unavailable. A URN differs from a URL in that its primary purpose is persistent labeling of a resource with an identifier. See RFC2141.
<b>Validity Period</b>	The period of time during which a PKC is intended to be valid as of the time of issuance. This is specified as a pair of fields labeled “not before” and “not after” containing universal time indicators.
<b>vtBackup</b>	A backup utility developed at Virginia Tech by eProvisioning to provide highly secure backups utilizing symmetric and public key cryptography.
<b>VTCA</b>	Virginia Tech Certification Authority refers to any one of the CAs that comprises the VTPKI.
<b>VTPKI</b>	Virginia Tech Public Key Infrastructure refers to the Virginia Tech Root CA and all of the Subordinate CAs within the PKI hierarchy.
<b>Zeroize</b>	A method of erasing electronically stored data by altering the contents of the data storage to prevent the recovery of the data. [FIPS 140-1]

## 11 ACKNOWLEDGEMENTS

This Certification Practice Statement was derived in part from the Higher Education PKI Certificate Policy draft document developed by the Policy Activities Group (HEPKI-PAG). The HEPKI activity groups represent the cooperative efforts of CREN, EDUCAUSE/Net@EDU, and Internet2 in furtherance of PKI development for the higher education community.