

**X.509 Certification Practice Statement**  
**for the**  
**Class 1 Server**  
**Certification Authority**

**March 28, 2006**

**Amended July 7, 2009**

**OBJECT IDENTIFIER 1.3.6.1.4.1.6760.5.2.3.2.1**

**Release 1.0, Version 2.0**

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

This Certification Practice Statement (CPS) has been assigned the global Object Identifier (OID) 1.3.6.1.4.1.6760.5.2.3.2.1. 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

<b>1. INTRODUCTION.....</b>	<b>1</b>
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.....	4
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
<b>2. GENERAL PROVISIONS.....</b>	<b>5</b>
2.1 OBLIGATIONS.....	5
2.1.1 CA Obligations.....	5
2.1.2 RA Obligations.....	6
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.....	6
2.4.3 Dispute Resolution Procedures.....	6
2.4.4 Section Headings.....	6
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.....	7
2.6.4 Repositories.....	7
2.7 COMPLIANCE AUDIT.....	7

2.7.1 Frequency of Entity Compliance Audit.....	7
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
<b>2.8 CONFIDENTIALITY.....</b>	<b>8</b>
2.8.1 Types of Information to be Kept Confidential.....	8
2.8.2 Types of Information Not Considered Confidential.....	8
2.8.3 Disclosure of Certificate Revocation Information.....	8
2.8.4 Release to Law Enforcement Officials.....	8
2.8.5 Release as Part of Civil Discovery.....	8
2.8.6 Disclosure upon Subscriber's Request.....	8
2.8.7 Other Information Release Circumstances.....	8
<b>2.9 INTELLECTUAL PROPERTY RIGHTS.....</b>	<b>8</b>
<b>3. IDENTIFICATION AND AUTHENTICATION.....</b>	<b>8</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.....	9
3.1.5 Name Claim Dispute Resolution Procedure.....	9
3.1.6 Recognition, Authentication and Role of Trademarks.....	9
3.1.7 Method to Prove Possession of Private Key.....	9
3.1.8 Authentication of Organization Identity.....	9
3.1.9 Authentication of Individual Identity.....	10
3.1.10 Authentication of Component Identities.....	10
3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY.....	10
3.2.1 Certificate Re-key.....	10
3.2.2 Certificate Renewal.....	10
3.2.3 Certificate Update.....	10
3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION.....	10
3.4 REVOCATION REQUEST.....	11
<b>4. 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.....	12
4.4.2 Who Can Request Revocation of a Certificate.....	12
4.4.3 Procedure for Revocation Request.....	12

4.4.4 Revocation Request Grace Period.....	12
4.4.5 Suspension.....	12
4.4.6 Who Can Request Suspension.....	12
4.4.7 Procedure for Suspension Request.....	12
4.4.8 Limits on Suspension Period.....	12
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.....	13
4.4.12 Online Revocation Checking Requirements.....	13
4.4.13 Other Forms of Revocation Advertisements Available.....	13
4.4.14 Checking Requirements for Other Forms of Revocation Advertisements.....	13
4.4.15 Special Requirements Related to Key Compromise.....	13
<b>4.5 SECURITY AUDIT PROCEDURE.....</b>	<b>13</b>
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.....	14
4.5.6 Security Audit Collection System (Internal vs. External).....	14
4.5.7 Notification to Event-Causing Subject.....	14
4.5.8 Vulnerability Assessments.....	14
<b>4.6 RECORDS ARCHIVAL.....</b>	<b>14</b>
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).....	15
4.6.7 Procedures to Obtain and Verify Archive Information.....	15
<b>4.7 KEY CHANGEOVER.....</b>	<b>15</b>
<b>4.8 COMPROMISE AND DISASTER RECOVERY.....</b>	<b>15</b>
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
<b>4.9 CA TERMINATION.....</b>	<b>15</b>

**5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS..... .15**

<b>5.1 PHYSICAL CONTROLS FOR THE VTCA OR AUTHORIZED CA.....</b>	<b>15</b>
5.1.1 Site Location and Construction.....	16
5.1.2 Electrical Power.....	16
5.1.3 Water Exposures.....	16
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).....	17
5.2.1.3 Other Trusted Roles.....	17
5.2.2 Number of Persons Required Per Task.....	17
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.....	18
5.3.2 Background Check Procedures.....	18
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. TECHNICAL SECURITY CONTROLS.....</b>	<b>18</b>
6.1 KEY PAIR GENERATION AND INSTALLATION.....	18
6.1.1 Key Pair Generation by the Subscriber.....	19
6.1.2 Private Key Delivery to Subscriber.....	19
6.1.3 Public Key Delivery to Certificate Issuer.....	19
6.1.4 VTCA Public Key Availability.....	19
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.....	20
6.2.4 Private Key Backup.....	20
6.2.4.1 Backup of CA Private Signature Key.....	20
6.2.4.2 Backup of End-Entity Private Signature Key.....	20
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.....	21
6.5 COMPUTER SECURITY CONTROLS.....	21

6.5.1 Specific Computer Security Technical Requirements.....	21
6.5.2 Computer Security Rating.....	21
<b>6.6 LIFE-CYCLE TECHNICAL CONTROLS.....</b>	<b>21</b>
6.6.1 System Development Controls.....	21
6.6.2 Security Management Controls.....	21
6.6.3 Life Cycle Security Ratings.....	21
<b>6.7 NETWORK SECURITY CONTROLS.....</b>	<b>21</b>
<b>6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.....</b>	<b>21</b>
<b>7. 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.....	21
7.1.4 Name Forms.....	21
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. SPECIFICATION ADMINISTRATION.....</b>	<b>22</b>
8.1 SPECIFICATION CHANGE PROCEDURES.....	22
8.2 PUBLICATION AND NOTIFICATION POLICIES.....	22
8.2.1 Amendments Generally.....	22
8.2.2 Urgent Amendments Exception.....	22
8.2.3 Assent to Amendments.....	22
8.2.4 Maintenance of Prior Versions.....	22
8.3 CPS APPROVAL PROCEDURES.....	23
8.4 WAIVERS.....	23
<b>9. BIBLIOGRAPHY.....</b>	<b>24</b>
<b>10. GLOSSARY.....</b>	<b>26</b>
<b>11. ACKNOWLEDGEMENTS.....</b>	<b>35</b>

RECORD OF CHANGES CHANGE NUMBER	DATE OF CHANGE	DATE RECEIVED	DATE ENTERED	SIGNATURE OF PERSON ENTERING CHANGE
------------------------------------	-------------------	------------------	-----------------	--

1. **Cover Page** Change added July 7, 2009

Added: Amended July 7, 2009

Changed to Ver 2.0

2. **1.1.1 Certificate Policy (CP)** Change added July 7, 2009

Removed: The VTCA Root CA 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 C1SCA CPS is available online at <http://www.pki.vt.edu/vtc1sca/cps/>

Added: The C1SCA has a copy of the VTCA CP and CPS which has been digitally signed by the VTPKI-PMA chairman and one other member of the VTPKI-PMA. The VTPKI-PMA has the primary responsibility for approving policies/standards of the Virginia Tech Public Key Infrastructure (PKI) and the related Certificate Authorities operating within it. The web administrator of the VTCA PKI website publishes CP and CPS document updates to the website at the request of the VTPKI-PMA chairman and notifies the VTPKI-PMA membership whenever these updates occur.

A digitally signed copy of the VTCA CP(Certificate Policy) is available at <http://www.pki.vt.edu/rootca/cp/>.

- A digitally signed copy of the C1SCA CPS(Certification Practice Statement) is available at <http://www.pki.vt.edu/vtc1sca/cps/>.

3. **1.3 COMMUNITY AND APPLICABILITY** Change added July 7, 2009

Removed: The primary community served by the C1SCA consists of those DPEs that provide online services to the Virginia Tech community.

The C1SCA also provides certificates for the RA administrators of the C1SCA.

In the absence of a Virginia Tech User Certification Authority, the C1SCA issues a limited number of personal digital certificates to the community specified in the X.509 CPS for Virginia Tech Class 1 Server CA Digital Signature Pilot Project for the Office of

the Executive Vice President and Chief Operating Officer. Whenever the Virginia Tech User Certification Authority is able to provide personal digital certificates, the Virginia Tech Class 1 Server CA Digital Signature Pilot (DSP) Project for the Office of the Executive Vice President and Chief Operating Officer certificates will be revoked. The C1SCA does not issue a PKC to any entity that is not included in its defined communities. A Relying Party can assume that the holder of a PKC issued by the C1SCA has a relationship to Virginia Tech.

Added: The primary community served by the C1SCA consists of those DPEs that provide online services to the Virginia Tech community.

The C1SCA does not issue a PKC to any entity that is not included in its defined communities. A Relying Party can assume that the holder of a PKC issued

4. **1.3.2 Registration Authorities** Changed added July 7, 2009

Removed: Information Resource Management is the Registration Authority for the C1SCA.

Added: Identity Management Services is the Registration Authority for the C1SCA.

5. **1.4 CONTACT DETAILS** Change added July 7, 2009

Removed: 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).

Identity Management Services  
1700 Pratt Dr.  
Blacksburg, VA 24060

Chair, VTPKI PMA  
1700 Kraft Drive, Suite 2000  
Blacksburg, VA 24061

Added: Questions about interpretation of this CPS are directed in writing to Identity Management Services. Concerns about possible abuse of this CPS, are directed in writing to the Virginia Tech Public Key Infrastructure Policy Management Authority (VTPKI

PMA).  
Identity Management Services  
1700 Pratt Dr.  
Blacksburg, VA 24060

Chair, VTPKI PMA  
1700 Pratt Dr.  
Blacksburg, VA 24061

6. **2.1.3 Subscriber Obligations** Change added July 7, 2009

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

- read and agree to the terms and conditions of this CPS
- notify Information Resource Management immediately upon either suspected or known compromise of the private key associated with a PKC

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

- read and agree to the terms and conditions of this CPS
- notify Identity Management Services

7. **2.4 INTERPRETATION AND ENFORCEMENT** Change added July 7, 2009

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

Added: Interpretation of this CPS is the responsibility of the PMA and Identity Management Services.

8. **3.1 INITIAL REGISTRATION** Change added July 7, 2009

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

Initial registration requires the signature of the applicant for the service and signature of the department head. The signature of a higher level manager in the reporting line may be substituted. IRM verifies that the signatures comprise appropriate authentication and that the signing party is the appropriate authority. The registration process also provides contact information for the individual person who has responsibility for the client.

Added: Interpretation of this CPS is the responsibility of the PMA and Identity Management Services.

Initial registration requires the signature of the applicant for the service and signature of the department head. The signature of a higher level manager in the reporting line may be substituted. IMS verifies that the signatures comprise appropriate authentication and that the signing party is the appropriate authority. The registration process also provides contact information for the individual person who has responsibility for the client.

9. **3.1.2 Need for Names to be Meaningful** Change added July 7, 2009

Removed: The CN component of a Subject name in a PKC issued by the C1SCA is directly representative of the digital processing entity or natural person to which the PKC is issued.

Added: The CN component of a Subject name in a PKC issued by the C1SCA is directly representative of the digital processing entity to which the PKC is issued.

10. **3.1.3 Rules for Interpreting Various Name Forms** Change added July 7, 2009

Removed: The Subject names for a digital processing entity PKC are issued using the following format:

serialNumber=<unique number assigned by the CA at PKC issuance>,

CN = <digital processing entity identifier>, (i.e.; host name, application name)

OU = <department name>,

O = Virginia Polytechnic Institute and State University,

L = Blacksburg

S = Virginia,

C = US,

DC = vt,

DC = edu

The Subject names for a natural person entity PKC are issued using the following format:

serialNumber=<unique number assigned by the CA at PKC issuance>,

CN = <name of natural person>,

OU = Employee,

DC = vt,

DC = edu

The community designation must be a "Departmental Name" with any roles (i.e.; Web Server, Application Server) that pertain to those belonging to the community of digital

processing entities that provide online services to the Virginia Tech community. The community designation must be an "Employee" with an "RA Operator" role for those belonging to the community of certificates for the RA administrators for the C1SCA. The community designation must be an "Employee" with an "EVP User Pilot" role for those belonging to the community of certificates for the Digital Signature Pilot Project for the Office of the Executive Vice President and Chief Operating Officer.

Added: The Subject names for a digital processing entity PKC are issued using the following format:

CN = <digital processing entity identifier>, (i.e.; host name, application name)  
OU = <department name>,  
O = Virginia Polytechnic Institute and State University,  
L = Blacksburg  
ST = Virginia,  
DC = vt,  
DC = edu,  
C=US

#### 11. **3.1.4 Uniqueness of Names** Change added July 7, 2009

Removed: The Subject name in a PKC refers to a unique and identifiable digital processing entity or person. Including the serial number that is assigned by the CA ensures the uniqueness of the Subject name. A unique Subject name may not be reused.

Added: The Subject name in a PKC refers to a unique and identifiable digital processing entity. The accuracy of the DN details is checked by the registration authority using identification information provided during the enrollment process. A subscriber's DN must be unique and must not be assigned to different subscribers. Only when a subscriber possesses a number of certificates with different key uses can a DN appear several times, although the respective serial numbers of the issuing CA always remain unique.

#### 12. **3.1.9 Authentication of Individual Identity** Change added July 7, 2009

Removed: IRM will verify that the person listed as department head is the head of department, as claimed. IRM confirms any designations with the department head. Once signatures are on file, IRM will verify signatures associated with requests.

Added: IMS will verify that the person listed as department head is the head of department, as claimed. IMS confirms any designations with the department head. Once signatures are on file, IMS will verify signatures associated with requests.

13. **4.4 CERTIFICATE SUSPENSION AND REVOCATION** Change added July 7, 2009

Removed: The C1SCA revokes PKCs after receiving a valid revocation request. IRM initiates revocation when the departmental unit that has requested the certificate is no longer an identifiable university unit.

Added: The C1SCA revokes PKCs after receiving a valid revocation request. IMS initiates revocation when the departmental unit that has requested the certificate is no longer an identifiable university unit.

14. **4.4.2 Who Can Request Revocation of a Certificate** Change added July 7, 2009

Removed: Certificate Revocation Requests are accepted from:

- the Subscriber
- the Subscriber's department head

Added: Certificate Revocation Requests are accepted from:

- the Subscriber
- the Subscriber's department head
- IMS

15. **4.4.3 Procedure for Revocation Request** Change added July 7, 2009

Removed: A Certificate Revocation Request (CRR) is initiated through:

- submission of the online CRR form that contains the Certificate Revocation Identification Number (CRIN) from the CSR
- the signing of the CRR form by the appropriate department head
- creation of the CRR by the RAA on behalf of the subscriber

The C1SCA RAA approves and digitally signs the CRR. All CRRs are processed by the RAA immediately upon receipt. The CAA revokes the certificate and issues a new CRL within two business days of approval by the RAA.

Added: A Certificate Revocation Request is initiated through:

- Users email **IMScerts@vt.edu** and request the certificate be revoked.
- Users include the certificate common name and serial number in their revocation request.
- The C1SCA RAA approves the CRR. All Revocation Requests should be processed by the RAA immediately upon receipt.
- When approved, the CA immediately revokes the certificate and issues a new CRL within two business days of approval by the RAA.

16. **4.4.11 Online Revocation / Status Checking Availability** Change added July 7, 2009

Removed: Online Revocation/Status Checking (OCSP) is not available.

Added: Online Revocation/Status Checking (OCSP) is available.

17. **4.5.2 Frequency of Processing Data** Change added July 7, 2009

Removed: The audit logs are consolidated and reviewed on a regular basis by IRM.

Added: The audit logs are consolidated and reviewed on a regular basis by IMS.

18. **4.5.4 Protection of Security Audit Data** Change added July 7, 2009

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

Added: Access to audit logs is controlled by IMS, and access is restricted to authorized employees only.

19. **4.5.5 Security Audit Data Backup Procedures** Change added July 7, 2009

Removed: The C1SCA audit log is backed up on the same schedule as the rest of the data on the C1SCA host using a backup utility (vtBackup) which was developed at Virginia Tech. Backup audit logs of the C1SCA are protected against unauthorized viewing, modification, or deletion by encrypting the backup and storing it in a separate secure physical location offsite from the C1SCA host.

The audit logs for the C1SCA RA are backed up using the central IT Legato Networker network backup service for the host on which the RA resides.

Added: The C1SCA audit log is backed up on the same schedule as the rest of the data on VTCA servers using VT Information Systems and Computing network backup service providing:

- **Scheduled daily backup of server files and directories**
- **Offsite storage in compliance with computing standards**
- **Restoration of files as needed**

#### 20. **4.6.3 Protection of Archive** Change added July 7, 2009

Removed: 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.

Added: Archived records are protected against unauthorized viewing, modification, and deletion by using offsite storage in a physically secure and trustworthy location. The offsite backup location provides the following key features:

- **Storage in a secure, fire resistant Vault Room.**
- **A stable, secure storage environment:** The room is maintained at a constant 70 degrees and 35% - 55% humidity. It's secured with intrusion alarms and motion detectors.
- **Controlled access:** The interior door to the building remains locked at all times. After admittance to the building, access to the Vault Room can only be obtained with the use of a valid VT ID card entered into the cipher lock.
- **Enhanced fire protection:** Constructed with a concrete floor, and walls, the Vault Room is rated to withstand as a minimum three hours of fire. Additionally the entire building has an automated fire suppression system and a fire alarm wired into the campus police office.

#### 21. **4.6.4 Archive Backup Procedures** Change added July 7, 2009

Removed: Daily backups created with vtBackup serve as archives for the C1SCA CA application. The backups created with Legato Networker serve as archives for the C1SCA RA application.

Added: Daily backups created using the network backup service provided by Storage Management Team of the Systems Support Department serve as archives for the C1SCA CA application

22. **4.6.7 Procedures to Obtain and Verify Archive Information** Change added July 7, 2009

Removed: On request by the auditors, IRM will authorize Operations Center personnel to retrieve media containing archived information from the offsite storage location. 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 removable media 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.

Added: On request by the auditors, IMS will authorize Operations Center personnel to retrieve media containing archived information from the offsite storage location.

23. **5.1.5 Media Storage** Change added July 7, 2009

Removed: The encrypted backup media of the C1SCA are stored in an offsite physically secure and trustworthy location.

Added: The backup media of the C1SCA are stored in an offsite physically secure and trustworthy location.

24. **5.1.7 Offsite Backup** Change added July 7, 2009

Removed: In the event of a system failure, there are sufficient backups that can be used to restore the C1SCA system. These backups are made on a daily schedule using the vtBackup utility and maintained for a period of 90 days. The daily backups are incremental with the exception of full backups which are done on the first day of each month, The most recent 14 daily backups are stored at a secure offsite location which can only be accessed by authorized personnel.

Added: In the event of a system failure there are sufficient backups that can be used to restore the C1SCA system. Full monthly, weekly differential, and daily incremental backups are created during normal daily scheduled backups by the Information Systems and Computing network backup service. The backup media of the C1SCA are stored in an offsite physically secure and trustworthy location.

25. **5.2.1.1 Certification Authority Administrator** Change added July 7, 2009

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

- certificate generation and revocation
- CRL generation

- electronic certificate issuance for a C1SCA RAA

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

- Certificate profile, certificate template, and audit parameter configuration
- Develop VTCA key generation and backup procedures
- Assignment of VTCA security privileges and access controls of users
- Install and configure new CA software releases
- Startup/Shutdown of the VTCA

26. **5.2.1.2 Registration Authority Administrator (RAA)** Change added July 7, 2009

Removed: The Registration Administrator (RAA) role is constituted by IRM. The RA's responsibilities are:

Added: The Registration Authority Administrator (RAA) role is constituted by IMS. The RAA's responsibilities are:

27. **7.1.2 Certificate Extensions** Change added July 7, 2009

Removed: Standard extensions, when populated, are described in an appropriate Certificate Profile which is published at <http://www.pki.vt.edu/vtc1sca/cps/.\\> PKCs issued from the C1SCA have the following values in their Key Usage field:

- digital signature
- non repudiation
- key encipherment

Added: Standard extensions, when populated, are described in Certificate Profiles published at: <http://www.pki.vt.edu/vtc1sca/cps>

28. **7.2.3 OCSP Services** Change added July 7, 2009

Removed: OCSP is supported but not currently implemented.

Added: An OCSP (Online Certificate Status Protocol) responder service is available.

# 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 Class 1 Server Certificate Authority (C1SCA), 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 2527 [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

**ABADSG** American Bar Association Digital Signature Guideline

**CA** Certification Authority

**CAA** Certification Authority Administrator

**CARL** Certificate Authority Revocation List

**CN** Common Name

**CP** Certificate Policy

**CPS** Certification Practice Statement

**CRIN** Certificate Revocation Identification Number

**CRL** Certificate Revocation List

**CRR** Certificate Revocation Request

**DES** Data Encryption Standard

**DN** Distinguished Name

**DPE** Digital Processing Entity

**DSA/DSS** Digital Signature Algorithm / Digital Signature Standard

**DSP** Digital Signature Pilot

**EDI** Electronic Data Interface

**FIPS PUB (US)** Federal Information Processing Standard Publication

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

**URI** Uniform Resource Identifier

**URL** Uniform Resource Locator

**URN** Uniform Resource Name

**VTCA** Virginia Tech Certification Authority

**VTPKI** Virginia Tech Public Key Infrastructure

**WWW** 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, the information therein and the binding of that information to the Subject are sufficiently trustworthy for a particular application.

Any PKC issued by the C1SCA contains a valid reference to this CPS.

By relying on information contained in a PKC issued by the C1SCA, 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 C1SCA has a copy of the VTCA CP and CPS which has been digitally signed by the VTPKI-PMA chairman and one other member of the VTPKI-PMA. The VTPKI-PMA has the primary responsibility for approving policies/standards of the Virginia Tech Public Key Infrastructure (PKI) and the related Certificate Authorities operating within it. The web administrator of the VTCA PKI website publishes CP and CPS document updates to the website at the request of the VTPKI-PMA chairman and notifies the VTPKI-PMA membership whenever these updates occur.

- A digitally signed copy of the VTCA CP (Certificate Policy) is available at <http://www.pki.vt.edu/rootca/cp> .
- A digitally signed copy of the C1SCA CPS (Certification Practice Statement) is available at <http://www.pki.vt.edu/vtc1sca/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 C1SCA does not interoperate with CAs external to this policy domain.

## 1.2 IDENTIFICATION

The *Certificate Policies* field of the PKC includes the OID indicating the Levels of Assurance (LOA), as they are defined in this CPS.

## 1.3 COMMUNITY AND APPLICABILITY

The primary community served by the C1SCA consists of those DPEs that provide online services to the Virginia Tech community.

The C1SCA does not issue a PKC to any entity that is not included in its defined communities. A Relying Party can assume that the holder of a PKC issued by the C1SCA has a relationship to Virginia Tech.

### 1.3.1 PKI Authorities

The C1SCA does not have the authority to issue authority PKCs.

### 1.3.2 Registration Authorities

Identity Management Services is the Registration Authority for the C1SCA.

### 1.3.3 End Entities

The end entities that may be the Subject of a PKC issued under this policy are a Virginia Tech digital processing entity or a natural person.

### 1.3.4 Applicability

A DPE uses a PKC issued by the C1SCA to identify itself to other DPEs. In addition, the PKC provides confidentiality and data integrity of network communications.

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 C1SCA.

The table below summarizes the applicability of PKCs at each of the five levels of assurance offered by the C1SCA.

<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 to identify PKCs that are used in testing environments. It is solely used for this purpose and conveys no assurance information. Production systems <b>SHOULD</b> never trust PKCs

	with this LOA.
Rudimentary 1.3.6.1.4.1.6760.5.2.2.2.1	This level is not used.
Basic 1.3.6.1.4.1.6760.5.2.2.3.1	This level provides a sufficient level of assurance relevant to production environments where there are risks and consequences of data compromise. PKCs issued at this assurance level require the approval and signature of the subscriber's dean, director, department head, or designee. This guarantees that the subject entry named in the PKC is a member of the C1SCA communities
Medium 1.3.6.1.4.1.6760.5.2.2.4.1	This level is reserved for future use when stricter identity verification mechanisms are available and in use.
High 1.3.6.1.4.1.6760.5.2.2.5.1	This level is reserved for future use when stricter identity verification mechanisms are available and in use.

## 1.4 CONTACT DETAILS

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

Identity Management Services  
1700 Pratt Dr.  
Blacksburg, VA 24061

Chair, VTPKI PMA  
1700 Pratt Dr.  
Blacksburg, VA 24061

## 2 GENERAL PROVISIONS

### 2.1 OBLIGATIONS

Each party to the issuance and use of a PKC has an obligation to perform certain duties as detailed in this section. By accepting an issued PKC, a Subscriber accepts the obligations described hereunder. By making use of a PKC issued by the C1SCA, 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 MUST:

- Read and agree to the terms and conditions of this CPS
- Notify Identity Management Services immediately upon either suspected or known compromise of the private key associated with a PKC issued by the C1SCA

### **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 Identity Management Services.

### **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 C1SCA and the PKCs it issued is available online, except as indicated in this section 2.6. 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 are made available on the PKI website ([www.pki.vt.edu](http://www.pki.vt.edu)) 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 under which the C1SCA has ever issued a PKC are kept in accordance with the Virginia records retention policy.

### **2.6.3 Access Controls**

There are no limitations on access to this CPS and PKCs.

### **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 the signature of the applicant for the service and signature of the department head. The signature of a higher level manager in the reporting line may be substituted.

IMS verifies that the signatures comprise appropriate authentication and that the signing party is the appropriate authority. The registration process also provides contact information for the individual person who has responsibility for the client.

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

A Subject name is always present in a PKC issued by the C1SCA.

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

The CN component of a Subject name in a PKC issued by the C1SCA is directly representative of the digital processing entity to which the PKC is issued.

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

The Subject names for a digital processing entity PKC are issued using the following format:

CN = <digital processing entity identifier>, (i.e.; host name, application name)

OU = <department name>,

O = Virginia Polytechnic Institute and State University,

L = Blacksburg

ST = Virginia,

DC = vt,

DC = edu

C = US

#### **3.1.4 Uniqueness of Names**

The Subject name in a PKC refers to a unique and identifiable digital processing entity. The accuracy of the DN details is checked by the registration authority using identification information provided during the enrollment process. A subscriber's DN must be unique and must not be assigned to different subscribers. Only when a subscriber possesses a number of certificates with different key uses can a DN appear several times, although the respective serial numbers of the issuing CA always remain

#### **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**

Since the CSR is a self signed certificate, the CSR submitted to the C1SCA provides proof of possession of the private key that corresponds to the public key contained in the CSR.

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

No additional stipulations.

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

Class 1 Server Online Services Community

Initial registration requires:

- Contact information for the service administrator and the alternate service administrator, if any
- The name and signature of the service administrator's department head or designee
- The network identifier (i.e.; host name or IP address) of host on which the service runs

IMS will verify that the person listed as department head is the head of department, as claimed. IMS confirms any designations with the department head. Once signatures are on file, IMS will verify signatures associated with requests.

Class 1 Server Digital Signature Pilot Community

Initial registration requirements are described in the CPS for the Virginia Tech Class 1 Server CA Digital Signature Pilot for the Office of the Executive Vice President and Chief Operating Officer.

Class 1 Server RA Administrators

Initial registration requires the:

- Signature of the appointed RAA
- Signature of the Vice President for Information Technology or designee

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

No additional stipulations.

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

### **3.2.1 Certificate Rekey**

C1SCA PKCs are issued for a maximum of two years. Prior to expiration, the PKC can be rekeyed. Rekeying a PKC means that a new PKC is created that has the same characteristics and level of assurance 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 C1SCA cannot be renewed.

### **3.2.3 Certificate Update**

PKCs issued by the C1SCA cannot be updated.

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

A public key with an associated PKC that has been revoked for private key compromise cannot be recertified.

## **3.4 REVOCATION REQUEST**

The Revocation Request must identify the certificate to be revoked and explain the reason for revocation.

# **4 OPERATIONAL REQUIREMENTS**

## **4.1 APPLICATION FOR A CERTIFICATE**

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

A PEM encoded CSR containing the public key is submitted through the PKI website by the PKC subscriber.

## **4.2 CERTIFICATE ISSUANCE**

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

The private key is generated by the subscriber and does not leave the subscriber's possession. If the private key is mistakenly submitted along with the CSR or in some other way leaves the subscriber's possession, the C1SCA will not issue a PKC containing the now compromised private key. Instead, a new key pair must be generated and a new request submitted.

## **4.3 CERTIFICATE ACCEPTANCE**

Upon issuance of the PKC by the C1SCA, the subscriber is sent an email with:

- Instructions where to obtain the PKC
- Information about where the subscriber may view their responsibilities as a PKC holder

## **4.4 CERTIFICATE SUSPENSION AND REVOCATION**

The C1SCA revokes PKCs after receiving a valid revocation request. IMS initiates revocation when the departmental unit that has requested the certificate is no longer an identifiable university unit.

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

A certificate is revoked when:

- Identifying information or an attribute for the certificate changes before the certificate expires

- The certificate subject can be shown to have violated the stipulations of the CP or this CPS
- The certificate is shown to not have been issued in accordance with this CPS
- The private key is suspected of compromise
- The user or other authorized party requests revocation
- Any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of the certificate or the C1SCA

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

Certificate Revocation Requests are accepted from:

- The Subscriber
- The Subscriber's department head
- IMS

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

A Certificate Revocation Request (CRR) is initiated through:

- Users email IMScerts@vt.edu and request the certificate be revoked. Users include the certificate common name and serial number in their revocation request.
- The C1SCA RAA approves the CRR. All Revocation Requests should be processed by the RAA immediately upon receipt.
- When approved, the CA immediately revokes the certificate and issues a new CRL within two business days of approval by the RAA.

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

No additional stipulations.

#### **4.4.5 Suspension**

No additional stipulations.

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

No additional stipulations.

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

No additional stipulations.

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

No additional stipulations.

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

The C1SCA will issue Certificate Revocations Lists (CRL) and publish them at a location referenced at <http://www.pki.vt.edu/>.

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

Revocation lists are published at least every 30 days.

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

No additional stipulations.

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

Online Revocation/Status Checking (OCSP) is available.

#### **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
  - o Start up/shutdown of system
  - o Changes to user accounts
  - o Backup and log information
  - o Tasks performed by users with trusted roles
- CA logfiles
  - o Certification requests
  - o Issued certificates
  - o Issued CRLs

C1SCA databases are 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 logs are consolidated and reviewed on a regular basis by IMS.

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

The VTCA retains audit logs for at least one year.

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

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

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

The C1SCA audit log is backed up on the same schedule as the rest of the data on VTCA servers using VT Information Systems and Computing network backup service providing:

- **Scheduled daily backup of server files and directories**
- **Offsite storage in compliance with computing standards**
- **Restoration of files as needed**

#### **4.5.6 Notification to Event Causing Subject**

No additional stipulations.

#### **4.5.7 Vulnerability Assessments**

The audit logs are 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**

The backups serve as archives and are retained for at least one year.

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

Archived records are protected against unauthorized viewing, modification, and deletion by using offsite storage in a physically secure and trustworthy location. The offsite backup location provides the following key features:

- **Storage in a secure, fire resistant Vault Room.**
- **A stable, secure storage environment:** The room is maintained at a constant 70 degrees and 35% - 55% humidity. It's secured with intrusion alarms and motion detectors.
- **Controlled access:** The interior door to the building remains locked at all times. After admittance to the building, access to the Vault Room can only be obtained with the use of a valid VT ID card entered into the cipher lock.

- **Enhanced fire protection:** Constructed with a concrete floor, and walls, the Vault Room is rated to withstand as a minimum three hours of fire. Additionally the entire building has an automated fire suppression system and a fire alarm wired into the campus police office.

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

Daily backups created using the network backup service provided by Storage Management Team of the Systems Support Department serve as archives for the C1SCA CA application.

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

No additional stipulations.

#### **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, IMS will authorize Operations Center personnel to retrieve media containing archived information from the offsite storage location.

### **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 Information Technology 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 C1SCA operations center is located in room 118 of the Andrews Information Systems Building. This 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 visual camera monitoring systems.

#### **5.1.2 Electrical Power**

The C1SCA operations center operates its own backup generator as 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 measures at the C1SCA facility.

#### **5.1.5 Media Storage**

The backup media of the C1SCA 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 C1SCA system. Full monthly, weekly differential, and daily incremental backups are created during normal daily scheduled backups by the Information Systems and Computing network backup service. The backup media of the C1SCA are stored in an offsite physically secure and trustworthy location.

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

#### **5.2.1 Trusted Roles**

No additional stipulations.

##### **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. Primarily, a CAA's responsibilities are:**

- Certificate profile, certificate template, and audit parameter configuration
- Develop VTCA key generation and backup procedures
- Assignment of VTCA security privileges and access controls of users
- Install and configure new CA software releases
- Startup/Shutdown of the VTCA

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

The Registration Authority Administrator (RAA) role is constituted by IMS. The RA's responsibilities are:

- Acceptance of subscription and certificate revocation requests
- Verification of an applicant's identity and the applicant's span of authority
- Transmission of applicant information to the CAA
- Electronic reception and distribution of subscriber certificates
- Publication of CRLs and certificates

#### **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 C1SCA personnel follow requirements identified in sections 5.3, 5.3.1, and 5.3.2. The items in these sections are performed before C1SCA personnel are:

- Authorized for access to a C1SCA site
- Authorized for physical access to a C1SCA system
- Given a certificate and account on a C1SCA system for the performance of their role

Each of these certificates and accounts (with the exception of C1SCA signing certificates) are:

- Directly attributable to an individual
- NOT shared
- Restricted to actions authorized for that role through the use of a C1SCA's software, operating system, and procedural controls

C1SCA 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 C1SCA are:

- Known and appointed by the Vice President for Information Technology or his designee
- Trained with respect to the duties they are to perform
- NOT assigned duties that may cause a conflict of interest with their C1SCA duties

Procedures for verifying a Virginia Tech employee's identity are documented at <http://www.hr.vt.edu>.

### **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 C1SCA role and are not released except as required by law.

The Department of Human Resources initiates 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 stipulations.

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

No additional stipulations.

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

No additional stipulations.

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

The PMA initiates appropriate administrative and disciplinary actions against personnel who have performed unauthorized actions involving the C1SCA 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**

The subscriber generates cryptographic keys for end entity certificates using the RSA public key algorithm. The private key should be pass phrase protected with an algorithm that employs 128 bit or better encryption. AES is the preferred method.

Subscribers should use a good source of randomness when generating their keys. Hardware based random number generators are preferred.

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

The private key is generated by the Subscriber and thus does not need to be delivered.

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

Cryptographic public keys for end entity certificates are delivered to the C1SCA encapsulated in the CSR.

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

No additional stipulations.

#### **6.1.5 Key Sizes**

The C1SCA requires the key size to be a minimum of 2048 bits for digital processing entities. The required key size for certificates issued to natural persons is a minimum of 1024 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**

No additional stipulations.

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

No additional stipulations.

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

The C1SCA does not escrow private signature keys.

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

The C1SCA 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 C1SCA does not backup end entity private signature keys.

#### **6.2.5 Private Key Archival**

The C1SCA does not archive end entity 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 C1SCA uses a hardware security module (HSM) that is certified as FIPS 140-2 level 3. The HSM implements strong multifactor authentication. This requires the C1SCA CAA to use a key token and associated PIN in order to access the private area of the HSM which contains the C1SCA 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 C1SCA and the end entity certificates issued by the C1SCA are published at <http://www.pki.vt.edu/vtc1sca/cps/>.

#### **7.1.1 Version Numbers**

No additional stipulations.

### **7.1.2 Certificate Extensions**

Standard extensions, when populated, are described in Certificate Profiles published at: <http://www.pki.vt.edu/vtc1sca/cps>

### **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**

Information on CRL extensions is documented in the certificate profiles for the C1SCA. The certificate profiles for the C1SCA and the end entity certificates issued by the C1SCA are published at <http://www.pki.vt.edu/vtc1sca/cps/>

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

No additional stipulations.

### **7.2.3 OCSP Services**

An OCSP (Online Certificate Status Protocol) responder service is available.

## **8 SPECIFICATION ADMINISTRATION**

### **8.1 SPECIFICATION CHANGE PROCEDURES**

No additional stipulations.

## **8.2 PUBLICATION AND NOTIFICATION POLICIES**

The C1SCA notifies its subscribers of any changes to the certificate policy via email.

### **8.2.1 Amendments Generally**

The PMA and the sponsor of the C1SCA will jointly amend this CPS prospectively but not retroactively.

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

No additional stipulations.

## **8.3 CPS APPROVAL PROCEDURES**

No additional stipulations.

## **8.4 WAIVERS**

No additional stipulations.

## 9. BIBLIOGRAPHY

The following documents SHALL be used as guidance in interpretation of this CP to the extent that information in these documents is not inconsistent with this CP:

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 140-1	Security Requirements for Cryptographic Modules, 1994-01-11 <a href="http://csrc.nist.gov/publications/fips/fips1401.pdf">http://csrc.nist.gov/publications/fips/fips1401.pdf</a>
FIPS 180-1	Secure Hash Standard, 1995-04-17 <a href="http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf">http://csrc.nist.gov/publications/fips/fips180-1/fip180-1.pdf</a>
FIPS 186-2	Digital Signature Standard, 2001-01-27
FOIACT	5 U.S.C. 552, Freedom of Information Act. <a href="http://www4.law.cornell.edu/uscode/5/552.html">http://www4.law.cornell.edu/uscode/5/552.html</a>  Federal Certificate Profile DRAFT, April 2000 <a href="http://csrc.nist.gov/pki/documents/FPKI_Certificate_Profile_20000418.xls">http://csrc.nist.gov/pki/documents/FPKI_Certificate_Profile_20000418.xls</a>
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. <a href="http://www4.law.cornell.edu/uscode/40/1452.html">http://www4.law.cornell.edu/uscode/40/1452.html</a>
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. <a href="http://www.cpsr.org/cpsr/privacy/computer_security/nsd_42.txt">http://www.cpsr.org/cpsr/privacy/computer_security/nsd_42.txt</a> (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 sub tree 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 Subject Name field and contains the value TRUE in the Basic Constraints CA field and in which the KeyUsage keyCertSign bit is set. The cRLSign 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 CPSuri 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 it has issued which have been 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 CP includes Authorizing and Authorized CAs that operate under this CP.
<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 CP, 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 that 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>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>	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
<b>Private Key</b>	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key <b>MUST</b> be kept secret.
<b>Public Key</b>	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
<b>Public Key Infrastructure (PKI)</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

<b>(RA)</b>	certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
<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>	A 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 CP; 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 (URI) 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 (URL) 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 (URN) refers to the subset of URI that are 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>VTCA</b>	Virginia Tech Certification Authority refers to any one of the CAs comprising 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 Certificate Policy was derived largely 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.