

**X.509 Certification Practice Statement
for Virginia Tech**

User Certification Authority

May 30, 2007

Amended September 9, 2009

OBJECT IDENTIFIER 1.3.6.1.4.1.6760.5.2.3.3.1

Identification and Validation of this Policy

This Certification Practice Statement (CPS) has been assigned the global Object Identifier (OID) 1.3.6.1.4.1.6760.5.2.3.3.1. 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.....	6
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.....	7
2.3.2 Administrative Processes.....	7
2.4 INTERPRETATION AND ENFORCEMENT.....	7
2.4.1 Governing Law.....	7
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.....	8
2.6.2 Frequency of Publication.....	8
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.....	9
2.8.1 Types of Information to be Kept Confidential.....	9
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
3. IDENTIFICATION AND AUTHENTICATION.....	9
3.1 INITIAL REGISTRATION.....	9
3.1.1 Types of Names.....	10
3.1.2 Need for Names to be Meaningful.....	10
3.1.3 Rules for Interpreting Various Name Forms.....	10
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.....	11
3.1.10 Authentication of Component Identities.....	11
3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY.....	11
3.2.1 Certificate Re-key.....	11
3.2.2 Certificate Renewal.....	12
3.2.3 Certificate Update.....	12
3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION.....	12
3.4 REVOCATION REQUEST.....	12
4. OPERATIONAL REQUIREMENTS.....	13
4.1 APPLICATION FOR A CERTIFICATE.....	13
4.1.1 Delivery of Public Key for Certificate Issuance.....	13
4.2 CERTIFICATE ISSUANCE.....	13
4.2.1 Delivery of Subscriber's Private Key to Subscriber.....	13
4.3 CERTIFICATE ACCEPTANCE.....	13
4.4 CERTIFICATE SUSPENSION AND REVOCATION.....	13
4.4.1 Circumstances for Revocation of a Certificate.....	13
4.4.2 Who Can Request Revocation of a Certificate.....	13
4.4.3 Procedure for Revocation Request.....	13
4.4.4 Revocation Request Grace Period.....	14
4.4.5 Suspension.....	14
4.4.6 Who Can Request Suspension.....	14

4.4.7 Procedure for Suspension Request.....	14
4.4.8 Limits on Suspension Period.....	14
4.4.9 Certificate Authority Revocation Lists / Certificate Revocation Lists... ..	14
4.4.9.1 CARL/CRL Issuance Frequency.....	14
4.4.10 CARL/CRL Checking Requirements.....	14
4.4.11 Online Revocation / Status Checking Availability.....	15
4.4.12 Online Revocation Checking Requirements.....	15
4.4.13 Other Forms of Revocation Advertisements Available.....	15
4.4.14 Checking Requirements for Other Forms of Revocation Advertisements.....	15
4.4.15 Special Requirements Related to Key Compromise.....	15
4.4.16 Special Requirements Related to Failed Attempts to Enter a Password.....	15
4.5 SECURITY AUDIT PROCEDURE.....	15
4.5.1 Types of Events Recorded.....	15
4.5.2 Frequency of Processing Data.....	16
4.5.3 Retention Period for Security Audit Data.....	16
4.5.4 Protection of Security Audit Data.....	16
4.5.5 Security Audit Data Backup Procedures.....	16
4.5.6 Security Audit Collection System (Internal vs. External).....	16
4.5.7 Notification to Event-Causing Subject.....	16
4.5.8 Vulnerability Assessments.....	16
4.6 RECORDSARCHIVAL.....	16
4.6.1 Types of Events Archived.....	16
4.6.2 Retention Period for Archive.....	16
4.6.3 Protection of Archive.....	17
4.6.4 Archive Backup Procedures.....	17
4.6.5 Requirements for Time-Stamping of Records.....	17
4.6.6 Archive Collection System (Internal or External).....	17
4.6.7 Procedures to Obtain and Verify Archive Information.....	17
4.7 KEY CHANGEOVER.....	17
4.8 COMPROMISE AND DISASTER RECOVERY.....	17
4.8.1 Computing Resources, Software, and/or Data Are Corrupted.....	17
4.8.1.1 Compromise Recovery.....	17
4.8.1.2 Disaster Recovery.....	17
4.8.2 CA Signature Keys Are Revoked.....	17
4.8.3 CA Signature Keys Are Compromised.....	18
4.8.4 Secure Facility Impaired after a Disaster.....	19
4.9 CA TERMINATION.....	19

5. PHYSICAL, PROCEDURAL AND PERSONNEL

SECURITY CONTROLS.....19

5.1 PHYSICAL CONTROLS FOR THE VTCA OR AUTHORIZED CA.....	19
5.1.1 Site Location and Construction.....	19
5.1.2 Electrical Power.....	19
5.1.3 Water Exposures.....	19
5.1.4 Fire Prevention and Protection.....	19
5.1.5 Media Storage.....	19
5.1.6 Waste Disposal.....	19
5.1.7 Offsite Backup.....	19
5.2 PROCEDURAL CONTROLS FOR THE VTCA.....	20
5.2.1 Trusted Roles.....	20

5.2.1.1 Certification Authority Administrator.....	20
5.2.1.2 Registration Authority Administrator (RAA)	20
5.2.1.3 Other Trusted Roles.....	20
5.2.2 Number of Persons Required Per Task.....	22
5.2.3 Identification and Authentication for Each Role.....	22
5.3 PERSONNEL CONTROLS.....	22
5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements.....	22
5.3.2 Background Check Procedures.....	22
5.3.3 Training Requirements.....	22
5.3.4 Retraining Frequency and Requirements.....	22
5.3.5 Job Rotation Frequency and Sequence.....	22
5.3.6 Sanctions for Unauthorized Actions.....	22
5.3.7 Contracting Personnel Requirements.....	23
5.3.8 Documentation Supplied to Personnel.....	23
6. TECHNICAL SECURITY CONTROLS.....	23
6.1 KEYPAIR GENERATION AND INSTALLATION.....	23
6.1.1 Key Pair Generation by the Subscriber.....	23
6.1.2 Private Key Delivery to Subscriber.....	23
6.1.3 Public Key Delivery to Certificate Issuer.....	23
6.1.4 VTCA Public Key Availability.....	23
6.1.5 Key Sizes.....	23
6.1.6 Public Key Parameters Generation.....	23
6.1.7 Parameter Quality Checking.....	23
6.1.8 Hardware/Software Subscriber Key Pair Generation.....	23
6.1.9 Key Usage Purposes (as per X.509 v3)	23
6.2 PRIVATE KEY PROTECTION.....	24
6.2.1 Standards for Cryptographic Module.....	24
6.2.2 CA Private Key Multi-Person Control.....	24
6.2.3 Key Escrow of CA Private Signature Key.....	24
6.2.3.1 Escrow of End-Entity Decryption Keys.....	24
6.2.4 Private Key Backup.....	24
6.2.4.1 Backup of CA Private Signature Key.....	24
6.2.4.2 Backup of End-Entity Private Signature Key.....	24
6.2.5 Private Key Archival.....	24
6.2.6 Private Key Entry into Cryptographic Module.....	24
6.2.7 Method of Activating Private Keys.....	24
6.2.8 Methods of Deactivating Private Keys.....	24
6.2.9 Method of Destroying Subscriber Private Signature Keys.....	25
6.3 OTHER ASPECTS OF KEY-PAIR MANAGEMENT.....	25
6.3.1 Public Key Archival.....	25
6.3.2 Usage Periods for the Public and Private Keys.....	25
6.4 ACTIVATION DATA.....	25
6.4.1 Activation Data Generation and Installation.....	25
6.4.2 Activation Data Protection.....	25
6.4.3 Other Aspects of Activation Data.....	25
6.5 COMPUTER SECURITY CONTROLS.....	25
6.5.1 Specific Computer Security Technical Requirements.....	25
6.5.2 Computer Security Rating.....	25
6.6 LIFE-CYCLE TECHNICAL CONTROLS.....	25
6.6.1 System Development Controls.....	25

6.6.2 Security Management Controls.....	25
6.6.3 Life Cycle Security Ratings.....	25
6.7 NETWORK SECURITY CONTROLS.....	26
6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.....	26
7. CERTIFICATE AND CARL/CRL PROFILES.....	26
7. CERTIFICATE PROFILE.....	26
7.1.1 Version Numbers.....	26
7.1.2 Certificate Extensions.....	26
7.1.3 Algorithm Object Identifiers.....	26
7.1.4 Name Forms.....	26
7.1.5 Name Constraints.....	26
7.1.6 Certificate Policy Object Identifier.....	26
7.1.7 Usage of Policy Constraints extension.....	27
7.1.8 Policy Qualifiers Syntax and Semantics.....	27
7.1.9 Processing Semantics for the Critical Certificate Policy Extension.....	27
7.1.10 Certificate Serial Numbers.....	27
7.2 CARL/CRL PROFILE.....	27
7.2.1 Version Numbers.....	27
7.2.2 CARL and CRL Entry Extensions.....	27
7.2.3 OCSP Services.....	27
8. SPECIFICATION ADMINISTRATION.....	27
8.1 SPECIFICATION CHANGE PROCEDURES.....	27
8.2 PUBLICATION AND NOTIFICATION POLICIES.....	27
8.2.1 Amendments Generally.....	27
8.2.2 Urgent Amendments Exception.....	27
8.2.3 Assent to Amendments.....	28
8.2.4 Maintenance of Prior Versions.....	28
8.3 CPS APPROVAL PROCEDURES.....	28
8.4 WAIVERS.....	28
9. BIBLIOGRAPHY.....	29
INTERNET X.509 PUBLIC KEY INFRASTRUCTURE CERTIFICATE AND CERTIFICATE REVOCATION LIST (CRL) PROFILE R. HOUSLEY, W. POLK, W. FORD, D. OLO.....	30
10. GLOSSARY.....	31
11. ACKNOWLEDGEMENTS.....	40

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

1. **Various** Change made July 7, 2009

Removed IRM and Identity Resource Management

Added IMS and Identity Management Services

2. **1. INTRODUCTION** Change made July 7, 2009

Removed: vtBackup

3. **1.4 Contact details** Change made July 7, 2009

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

Added: Chair, VTPKI PMA
1700 Pratt Dr.
Blacksburg, VA 24060

4. **3.1.9 Authentication of Individual Identity** Change made August 5, 2009

Removed: Subscriber must present two forms of photo identification to the RAA:

Hokie Passport. The VT identification number on the Hokie Passport is entered into TAS to retrieve information about the subscriber from ED-Id.

Photo identification from the following list:

U.S. Passport (expired or unexpired)

Foreign passport with *I-551 stamp* (expired or unexpired)

Permanent Resident Card or Alien Registration Receipt Card with photograph (*form I-151 or I-551*)

Naturalization Certificate (photo id prior to 1983)

Current, valid driver's license or ID card issued by a state or outlying possession of the United States, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address. *Information varies by state*

ID card issued by federal or state entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address. *Information varies by issuing agency*

U.S. Military card

U.S. Military dependent's ID card

The RAA compares likeness of subscriber to photographs. If the RAA is satisfied the likeness is true, the RAA compares information on the ids to information presented by TAS. The RAA may ask the subscriber questions and compare the answers to the information presented by TAS.

Note: If the subscriber does not have a second form of photo identification, the subscriber's department head or academic advisor must accompany the subscriber to the RAA and sign a document stating that he/she verifies the identity of the subscriber. This document will be retained by IMS.

Added: Subscriber must possess a PID and must present his or her Virginia Tech identification number to the RAA. The VT ID number is entered into TAS to retrieve information about the subscriber from ED-Id. Additionally, subscriber must present two forms of photo identification from the following list:

- Hokie Passport. The VT identification number on the Hokie Passport is entered into TAS to retrieve information about the subscriber from ED-Id.
- U.S. Passport (expired or unexpired)
- Foreign passport with *I-551 stamp* (expired or unexpired)
- Permanent Resident Card or Alien Registration Receipt Card with photograph (*form I-151 or I-551*)
- Naturalization Certificate (photo id prior to 1983)
- Current, valid driver's license or ID card issued by a state or outlying possession of the United States, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address. *Information varies by state*

- ID card issued by federal or state entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address.

Information varies by issuing agency

- U.S. Military card
- U.S. Military dependent's ID card

The RAA compares likeness of subscriber to photographs. If the RAA is satisfied the likeness is true, the RAA compares information on the ids to information presented by TAS. The RAA may ask the subscriber questions and compare the answers to the information presented by TAS. Note: If the subscriber does not have a second form of photo identification, the subscriber's department head or designee as registered with IMS must accompany the subscriber to the RAA and sign a document stating that he/she verifies the identity of the subscriber. This document will be forwarded to and retained by IMS.

5. **1.3 COMMUNITY AND APPLICABILITY** Change made September 9, 2009

Remove:

This CPS serves four communities. These communities are defined below, and are based on the "Person Affiliations Explained" section on the Middleware website (<http://www.middleware.vt.edu>):

- VT-employee-state (VT-faculty, VT-staff): Any person who works at the university and is paid with state dollars.
- VT-employee-wage: Any person who works for Virginia Tech in a wage position that does not act in the capacity of a faculty or staff member.
- VT-student-enrolled: any person enrolled in a class for the current term at Virginia Tech.
- VT-student-wage: Any student who works for Virginia Tech in a wage position that does not act in the capacity of a faculty or staff member.

The UCA also provides certificates for the RAA and CAA of the UCA. The UCA does NOT issue a PKC to any entity that is not included in the defined communities. A Relying Party assumes that the holder of a PKC issued by the UCA has a relationship to one of the communities defined in this CPS.

Add:

This CPS serves four primary communities. These communities are defined below, and are based on the "Person Affiliations Explained" section on the Middleware website (<http://www.middleware.vt.edu>):

- VT-employee-state (VT-faculty, VT-staff): Any person who works at the university and

is paid with state dollars.

- VT-employee-wage: Any person who works for Virginia Tech in a wage position that does not act in the capacity of a faculty or staff member.
- VT-student-enrolled: any person enrolled in a class for the current term at Virginia Tech.
- VT-student-wage: Any student who works for Virginia Tech in a wage position that does not act in the capacity of a faculty or staff member.

Other communities may be served with approval from the VTPKI PMA.

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 User Certificate Authority (UCA), a VTCA. Unless otherwise specified, all stipulations and requirements contained in this CPS are in addition to the VT 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
DES	Data Encryption Standard
DN	Distinguished Name
DPE	Digital Processing Entity
DSA/DSS	Digital Signature Algorithm / Digital Signature Standard
EDI	Electronic Data Interface
FIPS PUB	(US) Federal Information Processing Standard Publication
IETF	Internet Engineering Task Force
IMS	Identity Management Services (an entity specific to Virginia Tech)

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
PKIX	Public Key Infrastructure X.509
PMA	Policy Management 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
TAS	Token Administration System
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UCA	User Certification Authority
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 and the information therein and the binding of that information to the Subject are sufficiently trustworthy for a particular application.

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

By relying on information contained in a PKC issued by the UCA, 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 VTCA Root CA has digitally signed a copy of the VTCA CP using SHA-1 with RSA encryption and its primary PKC signing key <http://www.pki.vt.edu/rootca/cp/index.html>. The digitally signed copy of the User CPS is available online at <http://www.pki.vt.edu/vtuca/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 UCA does not interoperate with CAs external to this policy domain.

1.2 IDENTIFICATION

The PKC includes a URL reference to this CPS in the PKC's *CPSUri* field. The PKC also includes the OID(s) indicating the Level of Assurance (LOA), as they are defined in this CPS.

1.3 COMMUNITY AND APPLICABILITY

This CPS serves four primary communities. These communities are defined below, and are based on the "Person Affiliations Explained" section on the Middleware website (<http://www.middleware.vt.edu>):

- VT-employee-state (VT-faculty, VT-staff): Any person who works at the university and is paid with state dollars.
- VT-employee-wage: Any person who works for Virginia Tech in a wage position that does not act in the capacity of a faculty or staff member.
- VT-student-enrolled: any person enrolled in a class for the current term at Virginia Tech.
- VT-student-wage: Any student who works for Virginia Tech in a wage position that does not act in the capacity of a faculty or staff member.

Other communities may be served with approval from the VTPKI PMA.

1.3.1 PKI Authorities

The Virginia Tech UCA does not have the authority to issue authority PKCs.

1.3.2 Registration Authorities

The Registration Authority for the UCA will be the Student Telecommunication Office.

1.3.3 End Entities

The end entity that is the Subject of a PKC issued under this policy is a verified person in the defined community of Virginia Tech employees and students.

1.3.4 Applicability

A PKC issued by the UCA to the User community members is used to identify subscribers to both other individuals and to PKI-enabled applications.

In all cases, a PKC issued by the UCA to an individual in the defined community carries a Medium level of Assurance.

Only Relying Parties who 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 UCA.

The table below summarizes the applicability of PKC's at each of the five levels of assurance offered by the UCA.

Assurance Level	Applicability
Test 1.3.6.1.4.1.6760.5.2.2.1.1	This level is not used. .
Rudimentary	This level is not used.

1.3.6.1.4.1.6760.5.2.2.2.1	
Basic 1.3.6.1.4.1.6760.5.2.2.3.1	This level is not used.
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 reserved for future use, where 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 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 24060

Chair, VTPKI PMA
1700 Pratt Dr.
Blacksburg, VA 24060

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 UCA, a Relying Party is accepting its obligations hereunder.

2.1.1 CA Obligations

The CAA has the following responsibilities:

- Requires the Subscriber to sign the Usage Agreement for using the assigned digital certificate
- Issues the token containing the certificate

2.1.2 RA Obligations

The RAA has these responsibilities:

- Authenticates Subscriber by comparing requestor data in university databases to 1) information on photo ids, and 2) answers to questions asked by the RAA (Forms of identification provided are recorded and maintained.)
- Approves the Subscriber's certificate request
- Accepts revocation requests from authorized sources

Issuance is a two-step, two-person process; a single person cannot complete the issuance process.

2.1.3 Subscriber Obligations

A Subscriber has these responsibilities:

- Read and agree to the Usage Agreement for using the assigned digital certificate
- Promptly notify the RAA if token containing the private key is lost, or when unauthorized use of the private key associated with a PKC issued by the UCA is known or suspected
- Return token to RA upon graduation or when employment is terminated

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 shall be charged for this service. Fees may be charged for replacement of certificates should replacement be necessary because of loss, negligence or neglect.

2.5.2 Certificate Access Fees

No fee shall be charged for this service.

2.5.3 Revocation or Status Information Access Fees

No fee shall be charged for this service.

2.5.4 Fees for Other Services such as Policy Information

Fee may be charged for replacement of lost token.

2.5.5 Refund Policy

No additional stipulations.

2.6 PUBLICATION AND REPOSITORY

All information about the operation of the UCA and the PKCs it issues 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

Certificates may be published in the Enterprise Directory at the owner's discretion.

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 UCA has ever issued a PCA are kept in accordance with the Virginia Record retention policy.

No additional stipulations.

2.6.3 Access Controls

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

2.6.4 Repositories

For additional information on repositories, see www.pki.vt.edu .

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

PKCs issued by the UCA must be kept confidential according to university policy external to this CPS.

2.8.1 Types of Information to be Kept Confidential

No additional stipulations.

2.8.2 Types of Information Not Considered Confidential

PKCs issued by the UCA must be kept confidential according to university policy external to this CPS.

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 is performed by the subscriber, in person, to the RAA.

The RAA and the CAA are required to participate in the issuance process. Each performs a set of tasks that are, both procedurally and technically, mutually exclusive of each other.

The subscriber must bring two forms of photo identification from a pre-defined list, described in section 3.1.9 of this CPS.

Once the subscriber is authenticated by the RAA, he/she must:

- Create and maintain a strong token password that follows the guidelines provided at: http://www.computing.vt.edu/accounts_and_access/pickinggoodpasswords.html
- Agree to the Usage Agreement issued by the UCA (The Usage Agreement can be found at <http://www.pki.vt.edu>.)

3.1.1 Types of Names

A Subject name, uniquely identifying the holder of the certificate, is present in all PKCs issued by the UCA. The subject name must follow the X.500 standard

3.1.2 Need for Names to be Meaningful

The CN component of a Subject name in a PKC issued by the UCA is the name of the Subscriber to which the PKC is issued. First name, middle initial and last name (legal name per ED-ID) will be used in the Subject name.

3.1.3 Rules for Interpreting Various Name Forms

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

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

UID = <university assigned UID for the person from ED-ID>

CN = <person's Legal Name is taken from Ed-ID>

O = Virginia Polytechnic Institute and State University

C = US,

DC = vt

DC= edu

The Subject Alternative Name Field:

RFC822Name=PID@vt.edu

3.1.4 Uniqueness of Names

The Subject name in the PKC refers to a person. Including the UID that is assigned to each individual ensures the uniqueness of the Subject name. A unique subject name may not be 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

No additional stipulations.

3.1.8 Authentication of Organization Identity

No additional stipulation.

3.1.9 Authentication of Individual Identity

Subscriber must possess a PID and must present his or her Virginia Tech identification number to the RAA. The VT ID number is entered into TAS to retrieve information about the subscriber from ED-Id. Additionally, subscriber must present two forms of photo identification from the following list:

- Hokie Passport. The VT identification number on the Hokie Passport is entered into TAS to retrieve information about the subscriber from ED-Id.
- U.S. Passport (expired or unexpired)
- Foreign passport with *I-551 stamp* (expired or unexpired)

- Permanent Resident Card or Alien Registration Receipt Card with photograph (*form I-151 or I-551*)
- Naturalization Certificate (photo id prior to 1983)
- Current, valid driver's license or ID card issued by a state or outlying possession of the United States, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address. *Information varies by state*
- ID card issued by federal or state entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color, and address. *Information varies by issuing agency*
- U.S. Military card
- U.S. Military dependent's ID card

The RAA compares likeness of subscriber to photographs. If the RAA is satisfied the likeness is true, the RAA compares information on the ids to information presented by TAS. The RAA may ask the subscriber questions and compare the answers to the information presented by TAS. Note: If the subscriber does not have a second form of photo identification, the subscriber's department head or designee as registered with IMS must accompany the subscriber to the RAA and sign a document stating that he/she verifies the identity of the subscriber. This document will be forwarded to and retained by IMS.

3.1.10 Authentication of Component Identities

No component shall be issued PKCs.

3.2 CERTIFICATE RENEWAL, UPDATE AND ROUTINE RE-KEY

3.2.1 Certificate Re-key

The certificates are being issued for a period of two years. Prior to expiration, certificates can only be re-keyed in person. The person must be a member of an approved community at the time of re-keying. Re-keying a PKC means that a new PKC is created that has the same characteristics and level of authority 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 UCA MAY NOT be renewed.

3.2.3 Certificate Update

PKCs issued by the UCA MAY NOT be updated. Should information on the certificate need to be updated, a new certificate will need to be issued.

3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION

Once a PKC has been revoked, procedures for obtaining a new certificate must be followed. Certificates that have been revoked will not be restored. Suspensions are not supported.

3.4 REVOCATION REQUEST

Revocation requests are accepted. The revocation request must identify the certificate to be revoked and explain the reason. See Section 4.4

4. OPERATIONAL REQUIREMENTS

4.1 APPLICATION FOR A CERTIFICATE

4.1.1 Delivery of Public Key for Certificate Issuance

In the face-to-face registration process, the Subscriber receives his/her token, which is loaded with his/her certificate, containing the public key.

4.2 CERTIFICATE ISSUANCE

4.2.1 Delivery of Subscriber's Private Key to Subscriber

The private key is generated onto the token at the time of issuance and should not leave the subscriber's possession. The private key cannot be exported off of the token. If the token needs to be replaced, a new private key will be generated on a new token. The private key will be generated on the token provided by the CAA; user-provided tokens, or tokens from other sources will not be accepted.

4.3 CERTIFICATE ACCEPTANCE

- Once the RAA verifies the person's identity, the CAA approves the request.
- Prior to issuing a new certificate to a subscriber, the subscriber is:
 1. Shown the contents of the subject area of the certificate. Subscriber is asked to verify the data and re-enter their password.
 2. Shown an electronic version of the Usage Agreement associated with receiving a certificate.
 3. Asked to digitally sign the Usage Agreement as documentation that he/she has read, understands, and agrees to abide by these conditions.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

No additional stipulation.

4.4.1 Circumstances for Revocation of a Certificate

Circumstances under which a certificate can be revoked:

- Identifying information or an attribute for the certificate changes before the certificate expires (subscriber request)
- 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 (authenticated) subscriber or other authorized party requests revocation.
- The subscriber is no longer associated with the university. (Changing departments is not a reason for revoking a certificate.)
- The token has been lost.
- The subscriber has exceeded the blocking threshold (15 invalid attempts) for the administrative token password. In addition, the subscriber has either forgotten his/her token password or exceeded the blocking threshold for the subscriber token password (10 invalid attempts). The token password cannot be reset.

4.4.2 Who Can Request Revocation of a Certificate from UCA

The RAA or authorized TAS operator whose role includes access to the “Revoke” form can use TAS to create a Certificate Revocation Request (CRR) based upon a request initiated from:

- The (authenticated) subscriber
- The subscriber’s department head, or someone higher in the department head’s supervisory chain
- IMS
- Tokens deposited in a designated lockbox

4.4.3 Procedure for Revocation Request

- Revocation requests must be made by using one of the following procedures:
- Subscriber reports the token as lost or compromised to 4Help
- Subscriber appears before the RAA with their token and their Hokie Passport
- Subscriber reports the token as lost by appearing in person before the RAA with their Hokie Passport
- Subscriber deposits token in designated lock box

- Subscriber's department head or someone higher in the department head's supervisory chain returns the token to the RAA when the subscriber leaves the university. The RAA must verify, via Banner, that the employee is no longer associated with the university
- Subscriber's department head or someone higher in the department head's supervisor chain contacts 4help to revoke employee's certificate
- IMS sends digitally signed email to the RAA, or email that is verified via a phone call by the RAA to IMS
- The procedure will be initiated through TAS by the RAA or authorized TAS operator whose role includes access to the "Revoke" form.
- A CRR is automatically created by TAS, approved and submitted to the UCA.
- Revoked certificate serial number will be included in the CRL within 24 hours.

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 UCA will issue Certificate Revocations Lists (CRL) and publish them at:

<http://www.pki.vt.edu/vtuca/crl/cacrl.crl>.

4.4.9.1 CARL/CRL Issuance Frequency

Revocation lists are published daily.

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.

4.4.16 Special Requirements Related to Failed Attempts to Enter a Token password

Use of the token will be blocked after 10 consecutive unsuccessful attempts to enter a subscriber token password. Resetting will require face-to-face authentication before the RAA. Subscriber must present token. The serial number from the certificate in that token is used to display information, stored in the TAS database, about the subscriber to who the token was issued. This information is used to ensure the authenticated subscriber is the owner of the token.

4.5 SECURITY AUDIT PROCEDURE

4.5.1 Types of Events Recorded

- System logfiles:
 - Start-up/shutdown of system
 - Changes to subscriber accounts
 - Backup and log information
 - Tasks performed by operators with trusted roles (identify operator, task, time, success/failure)
- CA logfiles:
 - Certification requests (identification of the RAA and the CAA, time stamp of each)
 - Issued certificates
 - Certification Revocation Requests (identification of who, time stamp)
 - Revoked certificates
 - Issued Certificate Revocation Lists (CRLs) (time stamp)
 - Re-keys (who, time stamp)
 - TAS logs
 - Logins/logouts by TAS operators

- Token password Reset
- Token inventory information
- Token recycling
- Operations errors

4.5.2 Frequency of Processing Data

The audit logs are consolidated weekly.

4.5.3 Retention Period for Security Audit Data

The VTCA retains audit logs for one year.

4.5.4 Protection of Security Audit Data

Access to audit logs is prescribed by IMS and is restricted to authorized employees. Exceptions are approved by IMS.

4.5.5 Security Audit Data Backup Procedures

The UCA audit log is backed up on the same schedule as the rest of the data on the UCA host. Backup audit logs of the UCA are protected against unauthorized viewing, modification, or deletion by encrypting the backup and storing it in a separate secure physical location offsite from the UCA host.

The UCA uses an encrypted backup. Backups are performed daily.

4.5.6 Security Audit Collection System (Internal vs. External)

No additional stipulations.

4.5.7 Notification to Event-Causing Subject

No additional stipulation

4.5.8 Vulnerability Assessments

The weekly consolidated audit log will be reviewed by the IT security office on a monthly basis.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Archived

No additional stipulations.

4.6.2 Retention Period for Archive

The archives are kept for three years.

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.

4.6.4 Archive Backup Procedures

Daily backups contain archives for the UCA application. The UCA database is backed up according to database backup procedures for used for Oracle.

4.6.5 Requirements for Time-Stamping of Records

No additional stipulation.

4.6.6 Archive Collection System (Internal or External)

No additional stipulation.

4.6.7 Procedures to Obtain and Verify Archive Information

On request by the auditors, the IT Security Office will authorize Operations Center personnel to retrieve media containing archived information from the offsite storage location. To view the archive, it must be decrypted. The key needed to decrypt the backups is stored on non-rewriteable media labeled “Backup UCA Encryption RSA Key Pair” at the offsite storage location. A duplicate copy of the key is stored on a BIO drive kept in a locked file cabinet in the IT Security 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 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

No additional stipulations.

5.1 PHYSICAL CONTROLS FOR THE VTCA OR AUTHORIZED CA

5.1.1 Site Location and Construction

The UCA operations center is located in room 118 of the Andrews Information Systems Building. The UCA 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 visual camera monitoring systems.

5.1.2 Electrical Power

The UCA 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 UCA facility.

5.1.5 Media Storage

The encrypted backup media of the UCA 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 UCA system. Daily backups are stored at a secure offsite location which can only be accessed by authorized personnel.

5.2 PROCEDURAL CONTROLS FOR THE UCA

Where appropriate, UCA procedures are performed using the Token Administration System (TAS).

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, or designee. The CAA's responsibilities are to:

- Generate certificate request
- Transmit subscriber information to the UCA
- Issue certificates via TAS

5.2.1.2 Registration Authority Administrator (RAA)

The Registration Authority Administrator (RAA) role is appointed by the Office of the Vice President for Information Technology, or designee. The RAA's responsibilities are to:

- Verify a subscriber's identity.
- Accept subscription requests
- Accept and process revocation requests

5.2.1.3 Other Trusted Roles

Access to TAS functionality is provided via five different roles. Each individual TAS operator is assigned a single role. The TAS roles and their associated functions are defined below:

1. Role Manager

The Role Managers are appointed by the Office of the Vice President for Information Technology or designee. A role manager will validate requests for managing TAS operators prior to performing the following tasks:

- Add and assign operators to roles
- Reassign operators to roles
- Delete operators
- Initialize RSA key pairs for each TAS site
- Specify the required forms of identification (credentials) for subscriber registration
- Add and remove participating departments

2. TAS Installer

This role is responsible for setting up the initial system parameters. These parameters are initially entered by the Installer, but can be changed after the installation by the TAS Administrator. These parameters include:

- ED-ID attributes
- CA chain to be loaded onto tokens during the enrollment process
- TAS operators certificate validation CA
- Email notification to the new subscribers
- Terms and conditions for TAS

The installer has access to the following forms:

- Login
- Installer
- Main

3. TAS Administrator

This role is responsible for maintaining the system functionality through the TAS administrator console, after the initial installation. TAS administrator tasks include the following:

- Set up initial default administrative password and a default subscriber password for the tokens (This value is setup during the initialization of the token and stored in the TAS database.)
- Setup database connection parameters
- Select a department RSA key
- Apply software upgrades and patches

The Administrator has access to the following forms:

- Login
- Admin
- Installer
- Main

4. RAA (Registration Authority Administrator)

This role is responsible for authenticating and registering the subscribers into TAS. This role has access to the following functions forms:

- Login
- Main
- Register
- Token Password reset
- Revoke
- Recycle
- View subscribers

5. CAA (Certificate Authority Administrator)

This role is responsible for issuing certificates and tokens to subscribers who have registered with the RAA. This role has access to the following forms:

- Login
- Main
- Issue
- Token Password reset
- View subscribers
- Recycle

6. Password Reset Administrator

This role is responsible for resetting subscriber token passwords and has access to the following forms:

- Login
- Main
- Token Password reset
- View subscribers

7. Certificate Revocation Administrator

This role is responsible for revoking subscriber certificates, and has access to the following forms:

- Login
- Main
- Revoke

5.2.2 Number of Persons Required Per Task

A minimum of two individuals must be involved in the issuance process. Once the subscriber's identity is verified in person by the RAA, the token password is created by the subscriber. This token password is used to authenticate to the CAA, who issues the token to the subscriber.

5.2.3 Identification and Authentication for Each Role

No additional stipulation.

5.3 PERSONNEL CONTROLS

Personnel with UCA operational responsibilities must meet all of the following requirements:

- Virginia Tech employees
- Known and appointed by the Vice President for Information Technology or designee
- Trained with respect to the duties they are to perform
- Not be assigned duties that may cause a conflict of interest with their UCA 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 completed background check. Such checks are to be performed solely to determine the suitability of a person to fill a UCA or VTCA role, and are not released except as required by law.

The Department of Human Resources will perform background check procedures for these employees consistent with trusted roles.

5.3.3 Training Requirements

Personnel with access to personal information will be trained as to the confidentiality of the information and to not disclose this information to any 3rd party.

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 UCA or its Repository.

5.3.7 Contracting Personnel Requirements

Contracting Personnel will not be used in these positions.

5.3.8 Documentation Supplied to Personnel

All individuals with access to TAS will be presented with a reminder as to their responsibility toward personal information and the need to not disclose this information to any 3rd party.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

The CAA prepares the token for the Subscriber and generates the private/public key pair on the token.

6.1.2 Private Key Delivery to Subscriber

The private key is generated on the token and delivered to the Subscriber during the enrollment process.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 VTCA Public Key Availability

No additional stipulations.

6.1.5 Key Sizes

Key sizes are 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)

Key usage will include:

- Digital signature
- Non-repudiation
- Key encipherment
- Email protection
- Authentication

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

The cryptographic device used to store a private key and certificates is a token that meets FIPS 140-2 Level 2 security requirements.

6.2.2 CA Private Key Multi-Person Control

No additional stipulations.

6.2.3 Key Escrow of CA Private Signature Key

Private signature keys Are NOT escrowed.

6.2.3.1 Escrow of End-Entity Decryption Keys

No additional stipulations.

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 UCA does NOT backup end-entity private signature keys.

6.2.5 Private Key Archival

The UCA DOES NOT archive end-entity private signature keys.

6.2.6 Private Key Entry into Cryptographic Module

A Private Key is generated onboard the cryptographic token device and protected with a subscriber token password.

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

Private signature keys will be destroyed by reformatting the token.

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

Public and private keys will be issued for a two year period.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

No additional stipulations.

6.4.2 Activation Data Protection

The UCA uses a hardware security module (HSM) that is certified as FIPS 140-2 level 3. The HSM implements strong multifactor authentication. This requires the UCA operator to use a key token and associated PIN in order to access the private area of the HSM which contains the UCA 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 UCA and the end entity certificates issued by the UCA are published at <http://www.pki.vt.edu/vtuca/cps/>.

7.1.1 Version Numbers

No additional stipulations.

7.1.2 Certificate Extensions

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

PKCs issued from the UCA have the following values in their *Key Usage* field:

- Digital signature
- Non-repudiation
- Key encipherment

PKCs issued from the UCA have the following values in their *Enhanced Key Usage* field:

- Web Client Authentication
- Email Protection
- MS Smartcard Login

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 UCA. The certificate profiles for the UCA and the end entity certificates issued by the UCA are published at <http://www.pki.vt.edu/vtuca/cps/>.

7.2.2 CARL and CRL Entry Extensions

Detailed CARL/CRL profiles addressing the use of each extension are defined at <http://www.pki.vt.edu/vtuca/cps/>.

7.2.3 OCSP Services

OCSP is supported and is as up to date as the CRL.

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

No additional stipulations.

8.2 PUBLICATION AND NOTIFICATION POLICIES

The UCA notifies its subscribers of any changes to the certificate policy via email and via information posted at www.pki.vt.edu/vtuca/cps.

8.2.1 Amendments Generally

Any amendments to this policy must be approved by the PMA. Amendments are not retroactive.

8.2.2 Urgent Amendments Exception

An amendment that is deemed “urgent” becomes effective immediately. “Urgent” will be designated by the PMA if failure to make the amendment may result in a compromise of the UCA 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 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. http://www.abanet.org/scitech/ec/isc/dsgfree.html .
FIPS 112	Password Usage, 1985-05-30 http://www.itl.nist.gov/fipspubs/fip112.htm
FIPS 140-1	Security Requirements for Cryptographic Modules, 1994-01-11 http://csrc.nist.gov/publications/fips/fips1401.pdf
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
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 (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

--	--

Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Arc	An arc is an individual sub tree of an Object Identifier (OID) tree.
Archive	Long term, physically separate storage.
Audit	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]
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Authority certificate	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.
Authorized CA	A CA for which another CA signs an authority certificate in accordance with this CP.

Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Certificate	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
Certificate Policy (CP)	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.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates it has issued which have been revoked prior to their stated expiration date.
Certificate Status Authority	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.
Certificate Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certification Authority (CA)	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.

Certification Authority Revocation List (CARL)	A signed, time stamped list of serial numbers of CA public key certificates, including cross certificates that have been revoked.
Certification Practice Statement (CPS)	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).
Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Community	The community or group of individuals or other entities for which the CA will issue a PKC.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
CPSuri	A PKC standard extension that provides a URI pointing to an online copy of the CA's CPS.
Cross Certificate	A PKC used to establish a trust relationship between two CAs.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can

	determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
End Entity	Relying Parties and Subscribers.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Issuer	The issuer is the entity who has signed and issued the certificate.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, 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"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation	Random numbers, pseudo random numbers, and cryptographic

Material	parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
LOA	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.
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
Non Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	A 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.
Out of Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has

	the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
PKC	Public Key Certificate. As used in this CP, refers to an object conforming to X.509v3 or higher.
PKI Sponsor	Fills the role of a Subscriber for non human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this CP.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key MUST be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Rekey (a certificate)	To change the value of a cryptographic key that is being used in a

	cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	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.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Responsible Individual	A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Server	A system entity that provides a service in response to requests from clients.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subject	The subject is the entity associated with the public key stored in the subject public key field of the certificate.
Subordinate CA	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).
Subscriber	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.
Superior CA	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).
Technical non repudiation	The public key mechanisms that contribute technical evidence supporting a non repudiation security service.
Trust List	Collection of trusted certificates used by Relying Parties to authenticate other certificates.
Trusted Agent	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.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a “trust anchor.”
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures.
Two Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements. [NS4009]

Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
URI	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.
URL	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.
URN	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.
Validity Period	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.
VTCA	Virginia Tech Certification Authority refers to any one of the CAs comprising the VTPKI.
VTPKI	Virginia Tech Public Key Infrastructure refers to the Virginia Tech Root CA and all of the Subordinate CAs within the PKI hierarchy.
Zeroize	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.