X.509 Certificate Policy

For The

Virginia Polytechnic Institute and State University

Certification Authorities

May 13, 2004

Amended March 16, 2011

OBJECT IDENTIFIER 1.3.6.1.4.1.6760.5.2.1.1.1

Release 1.0 Version 3.0

Identification and Validation of this Policy

This Certificate Policy (CP) has been assigned the global Object Identifier (OID) 1.3.6.1.4.1.6760.5.2.1.1.1. A Virginia Tech Certificate Authority (VTCA) MAY NOT SIGN ANY PUBLIC KEY CERTIFICATE (PKC) OR OTHER DOCUMENT THAT ASSERTS BY REFERENCE TO THIS OID ITS CONFORMANCE TO THIS CERTIFICATE POLICY 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) (see Section 1.4.1), will result in a document with a different OID assignment.

A copy of this document SHALL be digitally signed by the chairman of the VTPKI-PMA who 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 signed document SHALL be available online at the location specified by certificates issued under this policy (see Section 7.1.8).

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

Data Universal Number System: 003137015

Table of Contents

RECORD OF CHANGES

1. Section 6.7 Change made 9/19/06

Removed: "The Virginia Tech Root and Subordinate CA equipment SHALL be implemented using a stand-alone (offline) configuration."

Added: "The Virginia Tech Root CA equipment SHALL be implemented using a stand-alone (offline) configuration. Subordinate CA equipment MAY be implemented using either an on-line or off-line configuration."

2. Cover Page Change made 7/7/09

Removed: **Amended September 19, 2006 OBJECT IDENTIFIER 1.3.6.1.4.1.6760.5.2.1.1.1 Release 1.0 Version 1.0**

Added: Amended July 7, 2009 OBJECT IDENTIFIER* **1.3.6.1.4.1.6760.5.2.1.1.1 Release 1.0 Version 2.0**

3. Identification and Validation of this Policy Change made 7/7/09
Removed: A copy of this document SHALL be digitally signed using SHA-1 with RSA encryption and the private key associated with the authority certificate of a VTCA operating under this policy.

Added: A copy of this document SHALL be digitally signed by the chairman of the VTPKI-PMA who has the primary responsibility for approving policies/standards of the Virginia Tech Public Key Infrastructure (PKI) and the related Certificate Authorities operating within it.

4. Section 1.1 OVERVIEW Change made 7/7/09
Removed: Any PKC issued by a VTCA MUST contain a valid reference to the applicable CP. This CP may be referenced only if a VTCA is in compliance with all aspects of this CP.

Added: Any authority PKC issued by a VTCA MUST contain a valid reference to the applicable CP. This CP may be referenced only if a VTCA is in compliance with all aspects of this CP.

5. Section 1.2 IDENTIFICATION Change made 7/7/09
Removed: Each PKC issued by a VTCA MUST reference an Object Identifier (OID) that identifies this CP document. The PKC MUST also include an OID indicating the Level of Assurance (LOA) that applies to that PKC. How this is to be achieved is described in the remainder of this section with further detail provided in the associated CPS document
.
.
A copy of this CP may be found at http://www.pki.vt.edu/VirginiaTech/cp. A digitally signed copy of the CP may be found at http://www.pki.vt.edu/VirginiaTech/cp/signed/

Added: Each authority PKC issued by a VTCA MUST reference an Object Identifier (OID) that identifies this CP document. End entity PKCs SHOULD include an OID indicating the Level of Assurance (LOA) that applies to that PKC. How this is to be achieved is described in the remainder of this section with further detail provided in the associated CPS document
.
.
 This CP and a digitally signed copy of it may be found at
http://www.pki.vt.edu/rootca/cp/index.html.

6. Section 1.1.3 Interoperation with CAs External to this Policy Domain Change made 7/7/09
Removed: No Stipulation.

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

7. Section 1.4.1 Specification Administration Organization Change made 7/7/09
Removed: The Policy Management Authority (PMA) for this CP MUST be identified by postal address, office location, and other contact information in the applicable CPS. The Policy Management Authority (PMA) is appointed by the Vice President for Information Technology who reports to the President.

Added: The Policy Management Authority (PMA) for this CP MUST be identified by postal address, office location, and other contact information in the applicable CPS. The Policy Management Authority (PMA) is appointed by the Vice President for Information Technology/Chief Information Officer (VPIT/CIO) who reports to the President.

8. Section 1.4.2 Contact Person Change made 7/7/09
Removed: Questions about interpretation of this CP should be directed to Information Resource Management. Concerns about possible abuse of this CP, should be directed in writing to the Virginia Tech Public Key Infrastructure Policy Management Authority (VTPKI PMA).
Information Resource Management
1700 Pratt Dr.
Blacksburg, VA 24061

Chair, VTPKI PMA
1700 Kraft Dr. Suite 2000
Blacksburg, VA 24061

Added: Questions about interpretation of this CP should be directed to Identity Management
Services. Concerns about possible abuse of this CP, 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

9, Section 2.1.1 CA Obligations Change made 7/7/09
Removed: A VTCA SHALL NOT issue any PKC with a Level of Assurance higher than that in
its authority PKC.

- not issuing more than one PKC with the same public key unless the Subject entity is the
  same in all instances

Added: Delete this sentence: "A VTCA SHALL NOT issue any PKC with a Level of Assurance
higher than that in its authority PKC." The specifics of LOA implemenatation are defined in
the associated CPS documents.
Delete this bullet: "not issuing more than one PKC with the same public key unless the Subject
entity is the same in all instances" The EJBCA does not check to see if a public key is being
reused. Key management is the responsibility of the user.

10. Section 3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION Change
made 7/7/09
Removed: A public key with an associated PKC which has been revoked for private key
compromise MUST NOT be recertified. The public key MAY be recertified if the PKC was
merely suspended. In the
latter case, identification of the Subject MAY be accomplished with the same procedure
indicated in section 3.1 for initial registration, or by using a digitally signed request using the

x

suspended PKC. Such a request MUST be sent to a VTCA during the period of validity of the PKC to be restored.

Added: A public key with an associated PKC which has been revoked for private key compromise MUST NOT be recertified. The Subscriber is responsible for rekeying when submitting a new certificate signing request to insure that when the new PKC is created, it has a new, different public key (corresponding to a new, different private key) and a different serial number is assigned by the CA.

11. Section 3.4 REVOCATION REQUEST Change made 7/7/09
Removed: A VTCA MUST accept as a revocation request an appropriate message digitally signed with the PKC to be revoked as long as it is still valid and not already revoked or suspended. The same procedures adopted for Subject identity during initial registration MAY also be used. Alternative procedures MAY be supported but MUST be detailed in the relevant CPS.

Added: A VTCA MUST accept as appropriate, a revocation request sent as a digitally signed message which specifies the PKC to be revoked. The same procedures adopted for Subject identity during initial registration MAY also be used. Alternative procedures MAY be supported but MUST be detailed in the relevant CPS.

12. Section 4.2 CERTIFICATE ISSUANCE Change made 7/7/09
Removed: Upon receiving the request, a VTCA SHALL:
• verify the authority of the requestor
• build and sign a certificate, if all certificate requirements have been met (in the case of an RA, have the VTCA sign the certificate)
• send the certificate to the user
The certificate request MAY contain an already built ("to be signed") certificate. This certificate SHALL NOT be signed until all verifications and modifications, if any have been completed to a VTCA's satisfaction. If a certificate request is denied, then a VTCA SHALL NOT sign the requested certificate, and will work with the RA to resolve the problem.
While the user may do most of the data entry, it is the responsibility of a VTCA to verify the information is correct and accurate. This may be accomplished either through a system approach linking databases containing personnel information or through personal contact with the program's attribute authority (as put forth in the applicable CPS).

Added: Upon receiving the request, a VTCA SHALL:
  - verify the authority of the requestor
  - approve the certificate request if all the requirements have been met and notify the requestor
  - deny the certificate request if it does not meet requirements

13. Section 5.2.1.1 Certification Authority Administrator (CAA) Change made 7/7/09
Removed: The Certification Authority Administrator (CAA) role and the corresponding procedures a CAA will follow shall be defined in detail in the applicable CPS. Primarily, a CAA's responsibilities are:
• certificate generation and revocation
• CRL generation
• certificate profile, certificate template, and audit parameter configuration
• certificate issuance for a VTCA administrator account
• VTCA key generation and backup

Added: The Certification Authority Administrator (CAA) role and the corresponding procedures a CAA will follow shall be defined in detail in the applicable CPS. 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

14 Section 5.2.1.2 Registration Authority Administrator (RAA) Change made 7/7/09
Removed: The Registration Authority Administrator (RAA) role and the corresponding procedures a RAA will follow shall be defined in detail in the applicable CPS. Primarily, an RAA's responsibilities are:
• acceptance of subscription, certificate change, certificate revocation/suspension and key recovery requests
• verification of an applicant's identity
• transmission of applicant information to the Virginia Tech certification authority
• reception and distribution of subscriber certificates
• publication of CRLs and certificates

Added: The Registration Authority Administrator (RAA) role and the corresponding procedures a RAA will follow shall be defined in detail in the applicable CPS. Primarily, an RAA's responsibilities are:
• acceptance of subscription, certificate change, certificate revocation/suspension and key recovery requests
• verification of an applicant's identity
• transmission of applicant information to the Virginia Tech certification authority
• reception and distribution of subscriber certificates <delete this bullet, the subscriber downloads their certificate immediately after their enrollment request has been approved>
• publication of CRLs and certificates <delete this bullet, publication of CRLs is done automatically, certificates can be published automatically to LDAP if needed>

15. Section 5.2.1.3 Other Trusted Roles Change made 7/7/09
Removed: A VTCA SHALL, in its CPS, define other trusted roles to which shall be allocated responsibilities that ensure the proper, safe, and secure operation of a VTCA's equipment and procedures. These responsibilities include:
• initial configuration of the system, including installation of applications, initial setup of new accounts, and configuration of the initial host and network interface.
• creation of devices to support recovery from catastrophic system loss
• performance of system backups, software upgrades, and recovery
• secure storage and distribution of the backups and upgrades to an offsite location
• changing the host or network interface configuration
• performance of proper system shutdown as required
• assignment of security privileges and access controls of users
• performance of archive and delete functions of the audit log and other archive data
• reviewing audit logs and performing compliance audits
To ensure system integrity, the CAA and RAA SHALL be prohibited from performing these responsibilities. Those who perform these responsibilities for a certification authority within the VTPKI SHALL NOT be a CAA or an RAA in the same domain. A VTCA SHALL maintain lists, including names, organizations, and contact information, of those who act in these trusted roles, and SHALL make them available during compliance audits

Added: A VTCA SHALL, in its CPS, define other trusted roles to which shall be allocated responsibilities that ensure the proper, safe, and secure operation of a VTCA's equipment and procedures. These responsibilities include:
• initial configuration of the operating system, including installation of applications, initial setup of new accounts, and configuration of the initial host and network interface.

• creation of devices to support recovery from catastrophic system loss
• performance of system backups, software upgrades, and recovery
• secure storage and distribution of the backups and upgrades to an offsite location
• changing the host or network interface configuration
• performance of proper system shutdown as required <delete this bullet, it is done by both CAA and Operating Systems support staff>
• assignment of operating system security privileges and access controls of host user accounts
• performance of archive and delete functions of the operating system audit log and other archive data
• reviewing audit logs and performing compliance audits

To ensure system integrity, the RAA/CAA SHALL be prohibited from performing these responsibilities. Those who perform these responsibilities for a certification authority within the VTPKI SHALL NOT be an RAA/CAA in the same domain. A VTCA SHALL maintain lists, including names, organizations, and contact information, of those who act in these trusted roles, and SHALL make them available during compliance audits

16. **Cover page** Change made March 16, 2011

Removed: X.509 Certificate Policy
For The
Virginia Polytechnic Institute and State University
Certification Authorities
May 13, 2004
Amended July 7, 2009
OBJECT IDENTIFIER 1.3.6.1.4.1.6760.5.2.1.1.1
Release 1.0 Version 2.0

Added: X.509 Certificate Policy
For The
Virginia Polytechnic Institute and State University
Certification Authorities
May 13, 2004
Amended March 16, 2011
OBJECT IDENTIFIER 1.3.6.1.4.1.6760.5.2.1.1.1
Release 1.0 Version 3.0

17. **1. INTRODUCTION** Change made March 16, 2011

Removed: The VTCAs that comprise the VTPKI are part of a Public Key Infrastructure (PKI) hierarchy consisting of a Root CA and one or more Subordinate CA(s). This CP applies to the Virginia Tech Root CA and all of the Subordinate CAs within the VTPKI hierarchy. Any VTCA for which the Virginia Tech Root CA signs an authority certificate MUST adopt this CP or one that is consistent with all of the requirements of this CP as determined by the Policy Management Authority for the VTPKI.

Added: The VTCAs that comprise the VTPKI are defined by independent Self Signed Root and Global Root CA hierarchies. Each Root CA hierarchy consists of one or more Subordinate CA(s). This CP applies to both Virginia Tech Root CA hierarchies and all of the Subordinate CAs within each hierarchy. Any VTCA for which the Virginia Tech Self Signed Root or Global Root CA signs an authority certificate MUST adopt this CP or one that is consistent with all of the requirements of this CP as determined by the Policy Management Authority for the VTPKI.

18. **1.3.1 PKI Authorities** Change made March 16, 2011

Removed: **The Virginia Tech Root CA** MAY issue a PKC with certificate issuance rights ("authority PKC") to another VTCA and in that case the Authorized Subordinate VTCA assumes the role of a CA under this CP. For all purposes under this CP, the Authorized Subordinate CA SHALL conform to, and operate under, this CP.

Added: A Virginia Tech Root CA MAY issue a PKC with certificate issuance rights ("authority PKC") to another VTCA and in that case the Authorized Subordinate VTCA assumes the role of a CA under this CP. For all purposes under this CP, the Authorized Subordinate CA SHALL conform to, and operate under, this CP.

19. **3.1.2 Need for Names to be Meaningful** Change made March 16, 2011

Removed: In the case where **the Virginia Tech Root CA** certifies another Authorized Subordinate CA within its policy domain, the Virginia Tech Root Authorizing CA MUST impose restrictions on the name space that MAY be used by the Authorized Subordinate CA that are at least as restrictive as its own name constraints.

Added: In the case where a Virginia Tech Root CA certifies another Authorized Subordinate CA within its policy domain, the Virginia Tech Root Authorizing CA MUST impose restrictions on the name space that MAY be used by the Authorized Subordinate CA that are at least as restrictive as its own name constraints.

20. **3.1.4 Uniqueness of Names** Change made March 16, 2011

Removed: **The Virginia Tech Root CA** and Authorized Subordinate CAs SHALL document in their respective CPSs:
• What name forms will be used.
• How **the Virginia Tech Root CA** and Authorized Subordinate CAs will interact to ensure this is accomplished.

• How **the Virginia Tech Root CA** and Authorized Subordinate CAs will allocate names within the Community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith" leaves a Community, and a new, different "Joe Smith" enters the Community, how these two people will be provided unique Subject names).

Added: A Virginia Tech Root CA and Authorized Subordinate CAs SHALL document in their respective CPSs:
• What name forms will be used.
• How a Virginia Tech Root CA and Authorized Subordinate CAs will interact to ensure this is accomplished.
• How a Virginia Tech Root CA and Authorized Subordinate CAs will allocate names within the Community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith" leaves a Community, and a new, different "Joe Smith" enters the Community, how these two people will be provided unique Subject names).

21**. 3.2.3 Certificate Update** Change made March 16, 2011

Removed: When **the Virginia Tech Root CA** updates its private signature key and thus generates a new public key, the Virginia Tech Root CA SHALL notify all Authorized Subordinate or cross certified CAs, and SHOULD make a best effort to notify any Subscribers that rely on the VTCA's PKC, that it has been changed. For **self signed ("root") PKCs**, such PKCs SHALL be made available online along with separately retrievable verification information to enable a relying party to verify that it has received a valid copy of the new "root" PKC.

Added: When a Virginia Tech Root CA updates its private signature key and thus generates a new public key, the Virginia Tech Root CA SHALL notify all Authorized Subordinate or cross certified CAs, and SHOULD make a best effort to notify any Subscribers that rely on the VTCA's PKC, that it has been changed. For self signed or globally trusted ("root") PKCs, such PKCs SHALL be made available online along with separately retrievable verification information to enable a relying party to verify that it has received a valid copy of the new "root" PKC.

22**. 4.8.1.1 Compromise Recovery** Change made March 16, 2011

Removed: If the VTCA is **the Virginia Tech Root CA**, the trusted self signed certificate MUST be removed from each Relying Party application, and a new one distributed via secure out of band mechanisms. **The Virginia Tech Root CA** SHALL describe its approach to reacting to a Root CA key compromise in their CPSs.

Added: If the VTCA is a Virginia Tech Root CA, the trusted self signed certificate MUST be removed from each Relying Party application, and a new one distributed via secure out of band mechanisms. A Virginia Tech Root CA SHALL describe its approach to reacting to a Root CA key compromise in their CPSs.

23. **6.2.2 CA Private Key Multi Person Control** Change made March 16, 2011

Removed: **The Virginia Tech Root CA** of the VTPKI SHALL implement M of N authentication.(M number of persons from N total number of persons).

Added: A Virginia Tech Root CA of the VTPKI SHALL implement M of N authentication.(M number of persons from N total number of persons).

24. **6.7 NETWORK SECURITY CONTROLS** Change made March 16, 2011

Removed: **The Virginia Tech Root CA** equipment SHALL be implemented using a stand-alone (offline) configuration.

Added: The equipment of a Virginia Tech Root CA SHALL be implemented using a stand-alone (offline) configuration.

25**. 10. GLOSSARY**

Removed: VTPKI: **Virginia Tech Public Key Infrastructure refers to the Virginia Tech Root CA and all of the Subordinate CAs within the PKI hierarchy.**

Added: VTPKI: Virginia Tech Public Key Infrastructure refers collectively to the Self Signed Root and Global Virginia Tech Root CAs and all of the Subordinate CAs within each PKI hierarchy.

1. INTRODUCTION

This Certificate Policy (CP) statement defines the terms and conditions under which a Virginia Polytechnic Institute and State University (hereinafter Virginia Tech) Certificate Authority (VTCA) operating within the Virginia Tech Public Key Infrastructure (VTPKI) issues Public Key Certificates (PKC) that reference the policy object identifier (OID) for this CP MUST operate. Operation includes management of the PKCs it issues and management of its own infrastructure. The term "issues" in this context refers to the process of digitally signing with the private key associated with its authority certificate a structured digital object conforming to the ISO X.509, version 3 or compatible PKC format.

One or more companion Certification Practice Statement(s) (CPS) MUST be defined for each Virginia Tech Certification Authority VTCA operating under this CP. Such a statement MUST articulate how a VTCA implements the provisions of this policy.

The VTCAs that comprise the VTPKI are defined by independent Self Signed Root and Global Root CA hierarchies. Each Root CA hierarchy consists of one or more Subordinate CA(s). This CP applies to both Virginia Tech Root CA hierarchies and all of the Subordinate CAs within each hierarchy.

Any VTCA for which the Virginia Tech Self Signed Root or Global Root CA signs an authority certificate MUST adopt this CP or one that is consistent with all of the requirements of this CP as determined by the Policy Management Authority for the VTPKI. This CP 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
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 CP defines a set of requirements that helps to determine the viability and applicability of a PKC issued by a conforming VTCA to the University community of users, subject entities, and/or class of applications.

This CP MAY be 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 authority PKC issued by a VTCA MUST contain a valid reference to the applicable CP. This CP may be referenced only if a VTCA is in compliance with all aspects of this CP.

Each VTCA MUST make available its own CPS(s) in order to provide information to potential clients of a VTCA and Relying Parties about the underlying technical, procedural and legal foundations which are not otherwise specified in this policy. The PMA may delegate any administrative responsibilities of a VTCA on condition that compliance with the current provisions in this CP are maintained.

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

1.1.1 Certificate Policy (CP)

Any VTCA that intends to refer to this CP in a PKC that it issues MUST digitally sign a copy of this document, using SHA-1 with RSA encryption and its primary PKC signing key, and make the signed copy available online as specified in Section 1.2.

1.1.2 Relationship Between the CP and the CPS

This CP states what assurance can be placed in a certificate issued by the VTCA. The associated CPS states how the VTCA establishes that assurance.

1.1.3 Interoperation with CAs External to this Policy Domain

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

1.1.3.1 Relationship Between a Bridge CP and this CP

No Stipulation.

1.2 IDENTIFICATION

Each authority PKC issued by a VTCA MUST reference an Object Identifier (OID) that identifies this CP document. End entity PKCs SHOULD also include an OID indicating the Level of Assurance (LOA) that applies to that PKC. How this is to be achieved is described in the remainder of this section with further detail provided in the associated CPS document

The base of the Object Identifier (OID) MUST be registered under the ANSI (or equivalent) arc. Sub arcs SHALL be defined for both this CP itself and for the different LOAs defined by this CP. OIDs also SHOULD be assigned to all associated CPSs referencing this CP.

When referencing this CP as governing a PKC, the OID given on the cover page SHALL be used in addition to any textual description. If this CP is changed in any substantive way, a new CP OID SHALL be assigned for the new version.

There are five Levels of Assurance (LOAs) covered by this CP as defined in subsequent sections. It is the intent of this CP for these LOAs to map directly to the Federal PKI (FPKI) Policy Authority LOAs.

The LOA asserted in any PKC issued by the VTCA SHALL be indicated by the OID in the CertPolicyID field in the PKC. The LOA OIDs for this CP are defined in the associated CPS document of each VTCA CP. The CPS URI extension field in a PKC asserting one of these LOAs MUST point to an online copy of the CPS that implements that LOA. The CPS should include a URI pointing to an online digitally signed copy of the CPS as specified in Section 1.1.1. That CPS

in turn MUST identify explicitly by an appropriate OID the CP to which it is conforming and specify how a Relying Party may obtain a copy of that CP. It SHOULD also include a URI pointing to an online, digitally signed copy of that CP.

Subsequent major revisions of this CP SHALL have a new OID assignment under the same OID arc. Minor revisions MAY be indicated by a suffix appended to the OID given on the cover page to this CP. The Level of Assurance (LOA) identifiers represent abstractions and SHALL remain the same unless or until new LOAs are required.

This CP and a digitally signed copy of it may be found at http://www.pki.vt.edu/rootca/cp/index.html .

The object identifier for this CP statement is 1.3.6.1.4.1.6760.5.2.1.1.1.

1.3 COMMUNITY AND APPLICABILITY

A VTCA MUST include in its CPS a definition of the Communities to which the VTCA will issue a PKC. The VTCA SHOULD NOT issue a PKC to any individual or other entity that is not included in one of the Communities. A Relying Party may not assume that the holder of a PKC issued by this VTCA has any particular relationship to any of the communities defined in the CPS unless explicitly stated in the CPS that such an assumption is warranted.

A VTCA MUST include in any CPS a definition of the applicability or any restrictions on the use of any resulting PKC. Such applicability MUST be indicated in the appropriate PKC fields, e.g. Key Usage. A Relying Party MUST respect any applicability limitations indicated in the PKC.

1.3.1 PKI Authorities

A Virginia Tech Root CA MAY issue a PKC with certificate issuance rights ("authority PKC") to another VTCA and in that case the Authorized Subordinate VTCA assumes the role of a CA under this CP. For all purposes under this CP, the Authorized Subordinate CA SHALL conform to, and operate under, this CP.

The PMA for the VTPKI SHALL have oversight responsibility for the operation of the Authorized Subordinate CA to ensure its conformance with this CP. A VTCA MAY delegate any of its responsibilities to a PMA associated with the Authorized Subordinate CA, provided that the VTCA remains responsible for conformance with all provisions of this CP.

A VTCA operating at Basic or lower LOA does not have the authority to issue authority PKCs.

1.3.2 Registration Authorities

The function of a Registration Authority (RA) is to verify the credentials that establish the binding between an individual or other entity that is the Subject of a PKC and the Subject's

Public/Private Key Pair that is associated with that PKC and approve the issuance of a PKC for that Subject. A VTCA MAY perform the function of a Registration Authority. A VTCA remains responsible for conformance with all provisions of this CP and associated CPS(s).

1.3.3 End Entities

The end entities that may be the Subject of a PKC issued under this policy can be (1) a natural person representing himself or herself, (2) an organization that is defined as part of the Community and is represented by a natural person authorized to act for that organization, or (3) a digital processing entity (e.g., a computer, a router or a defined application program or system), that is capable of performing cryptographic operations and that is owned or operated by an organization that is as part of the Community and that is represented by a natural person authorized to act for that organization ("PKC Sponsor"). In the latter case, the method of verification of the authorization of the person acting on behalf of the digital processing entity SHALL be set forth in the CPS.

1.3.4 Applicability

PKCs issued by a VTCA MAY be used for any application, provided that the uses are within the limitations imposed by the CPS or as indicated in the PKC itself.

However, only Relying Parties that accept in its entirety this CP and that accept in their entirety any limitations (financial or otherwise) contained in the PKC itself MAY make use of a PKC issued by a VTCA

If a Subscriber wishes to have any limitations (financial or otherwise) on transactions authenticated by the PKCs that are not contained in the PKC itself, that Subscriber MUST have a signed agreement with each Relying Party agreeing to such limitations. Any Relying Party that wants to make use of a PKC issued by a VTCA to authenticate transactions of significant financial value or otherwise of import to the Relying Party SHOULD have a signed agreement with the Subscriber stating any specific limitations.

The table below summarizes the recommended applicability of PKCs at each of the five levels of assurance covered by this CP.

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

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

1.4 CONTACT DETAILS

Questions about interpretation of this CP and associated CPSs, or concerns about possible abuse of this CP SHALL be directed in writing to the PMA identified under section 1.4.1.

1.4.1 Specification Administration Organization

The Policy Management Authority (PMA) for this CP MUST be identified by postal address, office location, and other contact information in the applicable CPS. The Policy Management Authority (PMA) is appointed by the Vice President for Information Technology /Chief Information Officer (VPIT/CIO) who reports to the President. The PMA will have, at a minimum, decision making representation from university administration, academic colleges, and university Internal Audit department, as well as advisory individuals with expertise in PKI.

1.4.2 Contact Person

Questions about interpretation of this CP should be directed to Identity Management Services. Concerns about possible abuse of this CP, 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

1.4.3 Person Determining Certification Practice Statement Suitability for the Policy

The PMA is responsible for reviewing and approving with an authorized signature any proposed CPS that is to be associated with this CP.

2. GENERAL PROVISIONS

This section defines the responsibilities of each party involved in the issuance and use of PKCs issued by a VTCA. These responsibilities bear on any potential responsibility that might be associated with a VTCA operating under the CP as a result of use of an issued PKC. Relying Parties MUST understand the provisions of this section.

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 a VTCA, a Relying Party is accepting its obligations hereunder.

2.1.1 CA Obligations

A VTCA must operate a certification authority service in accordance with all provisions of this CP and any associated CPS(s). Its obligations include:

- Accepting certification requests and issuing PKCs according to a published CPS

- Accepting certificate revocation requests and effecting certificate revocation or suspension, as defined in section 4.4

A VTCA that issues a PKC to a Subscriber MUST have explicit authorization to do so. A VTCA MUST adhere to any restrictions or limitations specified in its authority PKC and/or written agreement with the authorizing Virginia Tech Root CA.

2.1.2 RA Obligations

A subset of the responsibilities in 2.1.1 may be delegated to an RA in accordance with the applicable CPS. In addition, an RA MUST also:

- Confirm to a VTCA in a secure manner the validation of the connection between a public/private key pair and the requester's identity including the successful use of a suitable proof of possession method

- Adhere to the CPS(s) and the written agreement made with a VTCA

2.1.3 Subscriber Obligations

A Subscriber MUST:

- Read and agree to the terms and conditions under which a VTCA issues PKCs

- Present legitimate credentials as required by the CPS for the PKC to be issued

- Protect the private key associated with an issued PKC. Specific requirements are stated in the CPS for the PKC to be issued. Some types of PKCs MAY require that the private key be put in escrow

- Notify a VTCA immediately upon either suspected or known compromise of the private key associated with a PKC issued by that VTCA

2.1.4 Relying Party Obligations

Parties who rely upon the certificates issued under a policy defined in this document are REQUIRED to:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information

- Ensure the certificate is of the required assurance level, as indicated in the certificate information

- Check each certificate for validity prior to reliance

- Establish trust in a VTCA that issued the certificates they are about to use by verifying the chain of certificates at root of which a trusted VTCA exists

- Be aware of and abide by all rules, regulations and statues applicable to all information contained in a PKC

A relying party who is found to have acted in a manner inconsistent with these obligations SHALL have no claim against Virginia Tech in the event of a dispute.

2.1.5 Repository Obligations

A Repository is responsible for maintaining a secure system for storing and retrieving Virginia Tech Certificates, a current copy of this Policy, information relevant to Virginia Tech Certificates, and for providing information regarding the status of Virginia Tech Certificates as valid or invalid for the use of any Relying Party.

2.2 LIABILITY

2.2.1 CA Liability

The CA Group disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided, and further disclaims any and all liability for negligence and lack of reasonable care with respect to all PKCs issued by it. The CA Group shall not incur liability for representations of information contained in any PKC. Without limiting the generality of the foregoing, the CA Group accepts no liability of any sort if a Relying Party fails to fulfill its obligations as stated herein.

Liability, if any, shall be limited to actual monetary damages assessed by a court of competent jurisdiction in accordance with the laws of the Commonwealth of Virginia.

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

In no event will the aggregate liability of the CA Group to all parties (including without limitation a Subscriber, an applicant, a recipient, or a Relying Party) exceed $1,000. This limitation on damages applies to loss and damages of all types, including but not limited to direct, compensatory, indirect, special, consequential, exemplary, or incidental damages incurred by any person, including without limitation a Subscriber, an applicant, a recipient, or a Relying Party, that are caused by reliance on or use of a certificate the CA Group issues, manages, uses, suspends or revokes, or a certificate that expires. This limitation on damages applies as well to liability under contract, tort, and any other form of liability claim. The liability cap on each certificate shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. In the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall the CA Group be obligated to pay more than the aggregate liability cp for each certificate, regardless of the method of apportionment among claimants to the mount of liability cap. Noting herein shall be deemed a waiver of the sovereign immunity of Virginia Tech or the Commonwealth of Virginia.

2.2.2 RA Liability

No stipulation.

2.3 FINANCIAL CONSIDERATIONS

The VTPKI assumes no financial responsibility with respect to use or management of any issued PKC by one of its VTCAs.

2.3.1 Fiduciary Relationships

Issuance of Certificates in accordance with this Policy does not make an Issuing CA or any RA, an agent, fiduciary, trustee, or other representative of Subscribers or Relying Parties.

2.3.2 Administrative Processes

Administrative processes pertaining to this CP SHALL be described in the associated CPS.

2.4 INTERPRETATION AND ENFORCEMENT

Interpretation of this CP or any associated CPS(s) is the responsibility of the PMA.

2.4.1 Governing Law

The laws of the United States and the Commonwealth of Virginia SHALL govern the enforceability, construction, interpretation, and validity of this policy.

2.4.2 Severability, Survival, Merger, Notice

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect.

2.4.3 Dispute Resolution Procedures

The PMA SHALL have the exclusive authority to resolve any disputes associated with the use of the PKCs issued by a VTCA. If a dispute regarding interpretation of provisions in this CP arises between two VTCAs that issue PKCs referencing this CP's OID and that obtain their authority to issue PKCs from the same Authorizing Virginia Tech Root CA, all such disputes SHALL be resolved by the PMA identified in the Authorizing Virginia Tech Root CA's CPS

2.4.4 Section Headings

Headings used throughout this CP are for convenience only and SHALL NOT affect the interpretation of this CP.

2.5 Fees

No stipulation.

2.5.1 Certificate Issuance or Renewal Fees

No stipulation.

2.5.2 Certificate Access Fees

No stipulation.

2.5.3 Revocation or Status Information Access Fees

No stipulation.

2.5.4 Fees for Other Services such as Policy Information

No stipulation.

2.5.5 Refund Policy

No stipulation.

2.6 PUBLICATION AND REPOSITORY

All information about the operation of a VTCA and the PKCs it issued SHALL be available online, except as indicated in this section 2.6. Each PKC issued SHALL include information sufficient to locate this online Repository.

2.6.1 Publication of CA Information

A VTCA SHALL make available online and MAY make available in other forms:

• This CP and any CPS(s) under which it operates

• Its authority PKC(s) and other PKCs as described in Section 2.1.5

• All issued PKCs except those PKCs of Subscribers that explicitly request that their PKC not be made publicly available

• Signed certificate revocation and other certificate status information

The CPS referenced by the CPS URI in the PKC SHALL define how a Relying Party can locate and retrieve the rest of the above information.

2.6.2 Frequency of Publication

PKCs SHALL be made available as part of the issuing process except as provided in Section 2.6.1. This process MUST be described in associated CPS(s).

The frequency of certificate revocation publication is specified in 4.4.9.

Changes to this CP or its associated CPS(s) SHALL be published as soon as they are approved. Previous versions SHALL remain available online beyond the latest expiration date of any PKC that references that CP or CPS for a period of time as defined in the governing CPS(s). Archived copies of all CPs under which the CA has ever issued a PKC SHOULD be kept in accordance with the Commonwealth of Virginia records retention policy. (See Section 8.2.4).

2.6.3 Access Controls

There SHALL NOT be limitations for access to this CP, CPS(s) or certificate revocation information. There MAY be limitations on access to PKCs, for example to prevent bulk acquisition of data such as e-mail addresses.

2.6.4 Repositories

Repositories MUST be operated in a reliable and secure manner as detailed in CPS(s). Repository contents MUST be replicated offline for disaster recovery and independent validation purposes. See section 2.1.5.

2.7 COMPLIANCE AUDIT

A hierarchically superior Virginia Tech Root CA SHALL reserve the right to require periodic and intervallic inspections and audits of any subordinate VTCA facility within the superior Root CA's domain to validate that the subordinate VTCA is operating in accordance with the security practices and procedures laid out in its, the subordinate VTCA's CPS.

A VTCA SHALL reserve the right to require periodic and intervallic inspections and audits of any RA facility within the VTCA's domain to validate that the RA is operating in accordance with the security practices and procedures laid out in the VTCA's CPS.

2.7.1 Frequency of Entity Compliance Audit

A VTCA SHALL be subject to a periodic compliance audit that is no less frequent than once per calendar year.

2.7.2 Identity/Qualifications of Auditor

Periodic audits MAY be conducted by the Virginia Tech Department of Internal Audit and the

state Auditor of Public Accounts (APA) or by an independent, trusted, third party chosen by CAAs of a VTCA or the PMA.

2.7.3 Auditor's Relationship to Audited Party

The auditor SHALL have no participatory, administrative or policy development relationship to a VTCA being reviewed.

2.7.4 Topics Covered by Audit

All aspects of a VTCA operation as specified in its CPS SHALL be subject to any audit compliance inspection. Operational parameters, not originally included in a VTCA CPS, may be reviewed, at the discretion of the auditor, if determined to be material and relevant to continued operational integrity and reliability of the VTCA.

2.7.5 Actions taken as a result of deficiency

Action plans, in response to audit recommendations, shall be negotiated and coordinated, as required, through all affected VTCAs and the PMA. The PMA SHALL direct any actions to be taken.

2.7.6 Communication of Results

Results of compliance audits SHALL be provided to the VTCA CAAs and the PMA. Additional notification of affected VTCAs, subscribers or relying parties SHALL be communicated at the discretion of the PMA.

2.8 CONFIDENTIALITY

A VTCA collects and stores information from Subjects of a PKC that may be personally identifying. These data MUST be processed in a way that ensures privacy and other protections according to the laws applicable to Virginia Tech, as specified in section 2.4.1. However, nothing herein shall be construed to contravene the Virginia Freedom of Information Act.

2.8.1 Types of Information to be Kept Confidential

All information presented to a VTCA that is not included in a resulting PKC or certificate revocation record issued by a VTCA is considered confidential and SHALL NOT be released by the VTCA to third parties without the Subscriber's authorization unless such a release is required by federal or Virginia State law by a legal authority of competent jurisdiction.

2.8.2 Types of Information Not Considered Confidential

Information included in published PKCs or certificate revocation records issued by a VTCA is not considered confidential except as may be required by law.

2.8.3 Disclosure of Certificate Revocation Information

When a PKC is revoked, a reason code SHALL be included in the certificate revocation record for the action. This reason code is not considered confidential and MAY be shared with all other users and Relying Parties. However, other details concerning the revocation SHALL NOT be disclosed unless required by a legal authority of competent jurisdiction or permitted elsewhere in this CP.

2.8.4 Release to Law Enforcement Officials

A VTCA SHALL NOT disclose confidential PKC or PKC related information to any third party, except when required by a legal authority of competent jurisdiction under a duly issued warrant or subpoena or as might be required by the laws applicable to the VTCA, as specified in section 2.4.1.

2.8.5 Release as Part of Civil Discovery

A VTCA SHALL NOT disclose confidential PKC or PKC related information to any third party, except when required by a legal authority of competent jurisdiction under a duly issued warrant or subpoena or as might be required by the laws applicable to the VTCA, as specified in section 2.4.1.

2.8.6 Disclosure upon Subscriber's Request
A VTCA MAY release a Subscriber's confidential information upon validation of a request signed by the Subscriber.

2.8.7 Other Information Release Circumstances
No stipulation.

2.9 INTELLECTUAL PROPERTY RIGHTS

A VTCA MUST NOT claim any intellectual property rights with respect to issued PKCs. If any Subject's private key is escrowed, ownership of and all rights to that key remain with the Subject.

Any party MAY make use of any or all of the language in this CP or associated CPS(s) providing that appropriate attribution is included.

3. IDENTIFICATION AND AUTHENTICATION

The validity of a PKC for use as a digital credential is dependent heavily upon the validity of the credentials offered during initial verification of the Subject. A VTCA MUST ensure proper binding between the Subject of a PKC and the credentials provided by the Subscriber or the Subject's agent during the registration process, as detailed in the applicable CPS. Similar assurance MUST be obtained when renewing or revoking an issued PKC.

In addition, if contents of an issued PKC constitute a direct link to records in a supplemental database containing additional attributes of the Subject, the binding between the Subject and any such database entries MUST be verified before the PKC is issued or renewed. Details of this verification MUST be described in the applicable CPS.

3.1 INITIAL REGISTRATION

The CPS(s) associated with this CP SHALL detail how initial registration is performed. Specific requirements MUST be given for each type of PKC issued by a VTCA, including the types of credentials to be presented by the applicant, how they are verified, and how the resulting PKC is bound to a private key in the Subscriber's possession. A Relying Party must be able to assess whether the level of assurance and security required for each step in the initial registration process results in a PKC of sufficient trustworthiness for its intended use.

3.1.1 Types of Names
If a Subject name is present in a PKC issued by a VTCA, it SHOULD be reasonably relevant to the Subject. It need not be unique, depending on the nature and intended use of the PKC as defined in the CPS. For example, a Subject name MAY be an abstract object assigned to the class of entities, such as "student," of which the Subject is a member. A Subject name MUST NOT be misleading such that a Relying Party reasonably might assume that the Subject is a physical entity other than the actual holder of the PKC.

3.1.2 Need for Names to be Meaningful
The CPS defines whether a PKC will contain Subject names that are meaningful. Meaningful in this context means that the name can be interpreted to refer to a defined class of entities. A class that, by definition, includes only a single entity becomes an identity credential for the Subject.

In the case where a Virginia Tech Root CA certifies another Authorized Subordinate CA within its policy domain, the Virginia Tech Root Authorizing CA MUST impose restrictions on the name space that MAY be used by the Authorized Subordinate CA that are at least as restrictive as its own name constraints.

3.1.3 Rules for Interpreting Various Name Forms
A VTCA MUST detail in the associated CPS(s) the rules for interpreting various name forms used in the PKCs it issues.

3.1.4 Uniqueness of Names
The Subject names in a PKC MUST refer to a unique, identifiable entity or class of entities. The Subject name, if present and meaningful, MUST have the same meaning and interpretation whenever that Subject name is included in a PKC issued by a VTCA.

A Virginia Tech Root CA and Authorized Subordinate CAs SHALL document in their respective CPSs:

• What name forms will be used.

• How a Virginia Tech Root CA and Authorized Subordinate CAs will interact to ensure this is accomplished.

• How a Virginia Tech Root CA and Authorized Subordinate CAs will allocate names within the Community to guarantee name uniqueness among current and past Subscribers (e.g., if "Joe Smith" leaves a Community, and a new, different "Joe Smith" enters the Community, how these two people will be provided unique Subject names).

3.1.5 Name Claim Dispute Resolution Procedure
There SHOULD NOT be reason for two entities to dispute a Subject name.

The PMA SHALL investigate and correct if necessary any name collisions brought to its attention. If appropriate, the PMA SHALL coordinate with and defer to the appropriate naming authority.

3.1.6 Recognition, Authentication and Role of Trademarks

The PMA SHOULD honor private trademark rights. A corporate entity is not guaranteed that its name will contain a trademark if requested. The PMA SHALL NOT deliberately allow an entity to hold a name that a civil court has determined it has no right to use; however, it is not required to issue subsequently that name to the rightful owner if it has already issued one sufficient for identification within Virginia Tech. The PMA is not obligated to seek evidence of trademarks or court orders..

3.1.7 Method to Prove Possession of Private Key

A VTCA MUST detail in the CPS how it will verify that the applicant has possession and use of the private key associated with the public key to be included in the PKC. A VTCA MUST NOT issue a PKC for which the above proof of possession fails.

3.1.8 Authentication of Organization Identity

No stipulation.

3.1.9 Authentication of Individual Identity

A VTCA MUST ensure strong binding between the PKC applicant and any attributes of identity that are to be asserted by the PKC. The specific documents required and the method of their verification MUST be detailed in the CPS(s) associated with this CP.

Records will be kept in accordance with the record retention requirements of Virginia Tech and the Commonwealth of Virginia.

3.1.10 Authentication of Component Identities

Some computing and communications components (routers, firewalls, servers, etc.) MAY be named as PKC Subjects. In such cases, the component MUST have a PKC Sponsor. The PKC Sponsor is responsible for providing the following registration information:

- Equipment identification

- Equipment public key(s)

- Equipment attributes and authorizations (if any are to be included in the PKC)

- Contact information to enable a VTCA to communicate with the PKC Sponsor when required

The registration information SHALL be verified to an assurance level commensurate with the certificate assurance level being requested.

3.2 CERTIFICATE RENEWAL, UPDATE, AND ROUTINE REKEY

Renewal of an issued PKC SHALL only be performed by the same VTCA that issued it and MUST be performed while the prior PKC is still valid. Renewal MAY be based on a digitally signed request using the still valid PKC without in person identification as required in section 3.1.

Renewal SHOULD require generation of a new key pair.

3.2.1 Certificate Rekey

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and reestablishes its identity. Rekeying a PKC means that a new PKC is created that has the same characteristics and level as the old one, except that the new PKC has a new, different public key (corresponding to a new, different private key); a different serial number; and MAY be assigned a different validity period.

Rekeying requirements will be approved by the PMA.

3.2.2 Certificate Renewal

Renewing a PKC means creating a new PKC with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. PKCs MAY be renewed in order to reduce the size of the certificate revocation database. A PKC MAY be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subject name and attributes are unchanged.

3.2.3 Certificate Update

Updating a PKC means creating a new PKC that has the same or a different key, a different serial number, and differs in one or more other fields, from the old PKC. For example, a VTCA MAY choose to update a PKC of a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The old PKC may or may not be revoked, but MUST NOT be further rekeyed, renewed, or updated.

When a Virginia Tech Root CA updates its private signature key and thus generates a new public key, the Virginia Tech Root CA SHALL notify all Authorized Subordinate or cross certified CAs, and SHOULD make a best effort to notify any Subscribers that rely on the VTCA's PKC, that it has been changed. For self signed or globally trusted ("root") PKCs, such PKCs SHALL be made available online along with separately retrievable verification information to enable a relying party to verify that it has received a valid copy of the new "root" PKC. The CPS SHALL define how this is accomplished.

3.3 OBTAINING A NEW CERTIFICATE AFTER REVOCATION

A public key with an associated PKC which has been revoked for private key compromise MUST NOT be recertified. The Subscriber is responsible for rekeying when submitting a new certificate signing request to ensure that when the new PKC is created, it has a new, different public key (corresponding to a new, different private key) and a different serial number is assigned by the CA.

3.4 REVOCATION REQUEST

A VTCA MUST accept as appropriate, a revocation request sent as a digitally signed message which specifies the PKC to be revoked. The same procedures adopted for Subject identity during

initial registration MAY also be used. Alternative procedures MAY be supported but MUST be detailed in the relevant CPS.

4. OPERATIONAL REQUIREMENTS

This section specifies requirements imposed upon entities involved in the certification and certificate revocation process.

4.1 APPLICATION FOR A CERTIFICATE

VTCAs implementing this certificate policy SHALL NOT certify other CAs (to include cross certification) unless authorized by the PMA to do so. The PMA MAY authorize certain VTCAs to certify multiple CAs on their own authority within the restrictions imposed by the PMA.

Requests by Certification Authorities for VTCA certificates SHALL be submitted to the Virginia Tech Policy Management Authority using the contact provided in section 1.4 and SHALL be accompanied by a Certification Practices Statement written to the format of the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework defined in RFC2527.

The PMA will evaluate the submitted CPS for acceptability. The PMA MAY require an initial compliance audit, performed by parties of the PMA's choosing, to ensure that the CA is prepared to implement all aspects of the submitted CPS, prior to the PMA authorizing the VTCA to issue and manage certificates asserting the Virginia Tech certificate policies.

VTCAs SHALL only issue certificates asserting Virginia Tech certificate policies upon receipt of written notification from the PMA that they are authorized to do so, and then MAY only do so within the constraints imposed by the PMA or its designated representatives.

4.1.1 Delivery of Public Key for Certificate Issuance
No stipulation.

4.2 CERTIFICATE ISSUANCE

Upon receiving the request, a VTCA SHALL:

• Verify the authority of the requestor

• Approve the certificate request if all the requirements have been met and notify the requestor

• Deny the certificate request if it does not meet requirements

4.2.1 Delivery of Subscriber's Private Key to Subscriber
No stipulation.

4.3 CERTIFICATE ACCEPTANCE

Acceptance is the action by a subscriber that triggers the subscriber's duties and potential liability[1].

[1] *Digital Signature Guidelines,* 1996-08-01, section 1.1.2.

A VTCA SHALL define, in its CPS, a technical or procedural mechanism to:

- Explain to the subscriber its responsibilities as defined in Section 2.1.3

- Inform the subscriber of the creation of a certificate and the contents of the certificate

- Require the subscriber to verifiably indicate acceptance of the responsibilities and the certificate

The ordering of this process, and the mechanisms used, will depend on factors such as where the key is generated and how certificates are posted or delivered.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

A VTCA is also responsible for maintaining and making available certification revocation information, herein referred to as a Certificate Revocation List (CRL). Such information MUST be made available in the form of a complete list of all revoked but unexpired certificates.

4.4.1 Circumstances for Revocation of a Certificate

A PKC SHALL be revoked when the binding between the Subject and the Subject's public key contained within a PKC is no longer considered valid within the Level of Assurance indicated. Under the following circumstances a certificate will be revoked:

- Identifying information or attributes in the user certificate changes before the certificate expires

- The certificate subject can be shown to have violated the stipulations of this CP, or the CPS of a VTCA who issued the certificate

- The private key is suspected of compromise

- The user or other authorized party (as defined in a VTCA's CPS) request the certificate to be revoked

Whenever any of the above circumstances occur, the associated PKC SHALL be revoked and notification placed on the CRL.

4.4.2 Who Can Request Revocation of a Certificate

A VTCA MAY summarily revoke certificates within its domain (in practice, notice and cause would be given). A Registration Authority Administrator (RAA) can request the revocation of a subscriber's certificate on behalf of the subscriber, the subscriber's authorizing organization, or other authorized party. The subscriber is authorized to request the revocation of his or her own certificate.

4.4.3 Procedure for Revocation Request

A subscriber or other authorized party MAY request revocation of the subscriber's certificate using any format that identifies the certificate to be revoked, explains the reason for revocation, and allows the request to be authenticated (e.g., digitally or manually signed). Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties.

In particular, if the revocation is being requested for a reason of key compromise or suspected fraudulent use, then the subscriber's and the RAA's revocation request MUST so indicate. If a RAA performs this on behalf of a user, a formal, signed message format known to a VTCA SHALL be employed. All requests SHALL be authenticated; for signed requests from the certificate subject, or from a RAA, verification of the signature is sufficient.

Upon receipt of a revocation request a VTCA MAY, at the VTCA's discretion, ascertain the circumstances prompting the request. If the circumstances justify it, or if there is no outstanding reason to deny the request, the VTCA SHALL revoke the certificate by placing its serial number and other identifying information on a CRL, in addition to any other revocation mechanisms used.

4.4.4 Revocation Request Grace Period

There is no revocation grace period for the revocation of PKCs issued under this CP.

4.4.5 Suspension

Certificates are not to be suspended under this policy.

4.4.6 Who Can Request Suspension

No stipulation.

4.4.7 Procedure for Suspension Request

No stipulation.

4.4.8 Limits on Suspension Period

No stipulation.

4.4.9 Certificate Authority Revocation Lists / Certificate Revocation Lists

CRLs are issued periodically, even if there are no changes or updates to be made, to ensure timeliness of information. CRLs MAY be issued more frequently than required; if there are circumstances under which a VTCA will post early updates, these SHALL be spelled out in its CPS.

VTCAs SHALL make public the details of certificate revocation information posting, and an explanation of the consequences of using dated revocation information. This information SHALL be given to subscribers during certificate request or issuance, and SHALL be readily available to any potential relying party.

4.4.9.1 CARL/CRL Issuance Frequency

Details of Certificate Authority Revocation List (CARL) and CRL issuance periods SHALL be defined in the applicable CPS.

4.4.10 CARL/CRL Checking Requirements

Reliance on revoked PKCs could have serious consequences for the Relying Party. The matter of how often new revocation data should be obtained is a determination to be made by the Relying

Party, considering the risk, responsibility, and consequences for using a PKC whose revocation status may be unknown.

4.4.11 Online Revocation / Status Checking Availability

In addition to download access to CARL/CRLs, conforming VTCAs and Relying Party client software MAY optionally support Online Certificate Status checking Protocol (OCSP). Client software using online status checking need not obtain or process file based CARL/CRLs. The CPS will specify when and under what circumstances the VTCA will provide online status checking of issued PKCs.

4.4.12 Online Revocation Checking Requirements

Certificates MAY be revoked prior to their expiration. Use of revoked certificates could have damaging or catastrophic consequences in certain applications. Therefore, parties relying on online status checking MUST, via their applications, check the status of the certificate via the online status check. If for any reason an application cannot use online status checking the application MAY use CRLs to check the status of the certificate. If it is temporarily infeasible to obtain revocation information, then the relying party MUST either reject use of the certificate, or make an informed decision to accept the risk, responsibility and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use MAY occasionally be necessary to meet urgent operational requirements.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Related to Key Compromise

No stipulations beyond sections 4.4.2 – 4.4.9.

4.5 SECURITY AUDIT PROCEDURE

This section describes the security requirements of a VTCA's certificate issuing system. These requirements cover the equipment used to register users; generate, sign, and manage certificates; and generate, sign, and manage revocation information.

4.5.1 Types of Events Recorded

All applicable auditing capabilities of a VTCA's host operating system and public key applications required by this CP SHALL be enabled.

All logs, whether electronic or manual, should contain the date and time of the event along with the identity of the entity which caused the event. In addition, for some types it will be appropriate to record the success or failure, the source and destination of a message, or the disposition of a created object (e.g., a filename).

A VTCA must ensure that the applicable CPS specifies what information is logged.

4.5.2 Frequency of Processing Data

The audit log SHALL be consolidated and reviewed on a regular basis. The audit data SHALL be available for audit at the request of the auditor. A VTCA's CPS SHALL specify the auditor and the frequency of audit log reviews, or the organization responsible for audit.

4.5.3 Retention Period for Security Audit Data

The information generated on VTCA equipment SHALL be kept on the VTCA equipment until the information is moved to an appropriate archive facility. The individual who removes audit logs from a VTCA SHALL be different from any of the individuals who, in combination, manage a VTCA signature key. This entity SHALL be identified in the VTCA's applicable CPS.

4.5.4 Protection of Security Audit Data

The audit log, to the extent possible, will not be open for reading or modification by any human, or by any automated process other than those that perform audit processing. Any entity that does not have modification access to the audit log may archive it (note that deletion requires modification access). Audit logs SHALL be moved to a safe, secure storage location separate from VTCA equipment.

4.5.5 Security Audit Data Backup Procedures

The audit log MAY be backed up on the same schedule as the rest of the data on VTCA equipment.

4.5.6 Security Audit Collection System (Internal vs. External)

A VTCA must identify and specify the operation of an audit collection system in its applicable CPS.

4.5.7 Notification to Event Causing Subject

No stipulation.

4.5.8 Vulnerability Assessments

VTCA, system administrator, and other operating personnel SHALL be watchful for attempts to violate the integrity of the certificate management system, including the equipment, physical location, and personnel. The daily audit log SHOULD be checked for anomalies in support of any suspected violation. The weekly consolidated audit log SHALL be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Auditors SHALL check for continuity of the audit log.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Archived

VTCA archive records SHALL be detailed enough to establish the validity of a signature and of the proper operation of a VTCA.

The following data shall be recorded for archive at the initialization of VTCA equipment:

   • VTCA system equipment configuration files

- VTCA accreditation (if necessary)

- Certification Practice Statement

- Any contractual agreements to which a VTCA is bound

The following data shall archived:
- Modifications or updates to any of the above data items

- All certificates and CRLs (or other revocation information) as issued or published

- Audit logs (in accordance with Section 4.5)

- Other data or applications sufficient to verify archive contents

4.6.2 Retention Period for Archive
Archive records SHALL be preserved, maintained, and disposed of in accordance with local university retention policies.

4.6.3 Protection of Archive
Record archive material MUST be protected against unauthorized access either by physical security alone, or a combination of physical and cryptographic protection. Any archive retention site must provide adequate protection from environmental threats such as temperature, humidity, and magnetism.

A VTCA MUST identify the record archive protection in its applicable CPS.

4.6.4 Archive Backup Procedures
No stipulation.

4.6.5 Requirements for Time Stamping of Records
No stipulation.

4.6.6 Archive Collection System (Internal or External)
No stipulation.

4.6.7 Procedures to Obtain and Verify Archive Information
Procedures detailing how to create, package, transmit, and store the archive information SHALL be published in a VTCA's applicable CPS.

4.7 KEY CHANGEOVER
A VTCA uses a signing (private) key for creating certificates; however, relying parties employ a VTCA certificate for the life of the user certificate beyond that signing. Therefore, a VTCA MUST NOT issue subscriber certificates that extend beyond the expiration dates of their own certificates and public keys. To minimize risk to a VTCA through compromise of its key, the private signing

key will be changed more frequently, and only the new key will be used for certificate signing purposes from that time. The older, but still valid, certificate will be available to verify old signatures until all of the user certificates signed under it have also expired. The old private key MUST be protected, for it MUST be used to sign CRLs that contain certificates signed with that (old) key. For a thorough discussion of key changeover, see [RFC2510].

4.8 COMPROMISE AND DISASTER RECOVERY

Note: This content is supplemental to that contained within the IT Disaster Recovery Plan, and/or other applicable disaster recovery plans for recovery of a VTCA and other Virginia Tech IT enterprise services.

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

4.8.1.1 Compromise Recovery

In case of a VTCA key compromise, a superior VTCA SHALL revoke that VTCA's certificate, and the revocation information SHALL be published immediately in the most expedient manner. Subsequently, the VTCA installation SHALL be reestablished as above. If the VTCA is a Virginia Tech Root CA, the trusted self signed certificate MUST be removed from each Relying Party application, and a new one distributed via secure out of band mechanisms. The Virginia Tech Root CA SHALL describe its approach to reacting to a Root CA key compromise in their CPSs.

4.8.1.2 Disaster Recovery

VTCAs not explicitly covered by the IT Disaster Recovery plan are required to develop and maintain their own Disaster Recovery Plan. This plan is to be submitted to the PMA for approval at the same time as the CPS.

In the case of a disaster in which the VTCA equipment is damaged and inoperative, VTCA's operations SHALL be reestablished as quickly as possible, giving priority to the ability to revoke Subscriber's certificates. If a VTCA cannot reestablish revocation capabilities within one week, then the VTCA MUST report its keys as compromised, and reestablish the VTCA keys and certificates, all cross certificates, and finally all Subscriber certificates. The PMA MAY grant extensions to VTCAs on a case by case basis.

In the case of a disaster whereby a VTCA installation is physically damaged and all copies of the VTCA signature key are destroyed as a result, the VTCA SHALL request that its certificates be revoked. The VTCA installation SHALL then be completely rebuilt, by reestablishing the VTCA equipment, generating new private and public keys, being recertified, and reissuing all cross certificates. Finally, all Subscriber certificates SHALL be reissued. At their own risk, relying parties may make a judgment to continue to use certificates signed with the destroyed private key in order to meet urgent operational requirements.

4.8.2 VTCA Signature Keys Are Revoked

If a VTCA cannot issue a revocation prior to the time specified in the next update field of its currently valid CARL/CRL, then the PMA SHALL be immediately and securely notified. The PMA SHALL determine whether to revoke the authority certificate issued to any Authorized Subordinate VTCA. A VTCA SHALL reestablish revocation capabilities as quickly as possible in accordance with procedures set forth in the applicable CPS. A VTCA SHALL immediately

and securely advise the PMA in the event of a disaster where the VTCA installation is physically damaged and all copies of the VTCA signature keys are destroyed.

4.8.3 VTCA Signature Keys Are Compromised

If a VTCA's signature keys are compromised or lost (such that compromise is possible even though not certain):

• The PMA SHALL be immediately and securely notified so that the VTCA from whom a cross certification certificate has been issued MAY issue revocations for any authority or cross certificates it has issued

• VTCAs that have issued PKCs to the affected VTCA SHALL immediately publish a CARL revoking the affected VTCA's PKC as set forth above

• A new VTCA key pair SHALL be generated by the VTCA in accordance with procedures set forth in the applicable CPS

• New VTCA authority PKCs SHALL be acquired or generated by the VTCA and made available in the Repository immediately

• New cross certificates SHALL be acquired and issued by the VTCA also in accordance with the applicable CPS

• All Subscribers SHALL be required to recertify following the initial identification procedures defined in section 3.1 and the CPS

A VTCA SHALL investigate and report to the PMA what caused the compromise or loss and what measures have been taken to preclude recurrence. Auditor(s) SHOULD review the proposed and/or implemented measures.

4.8.4 Secure Facility Impaired after a Disaster

A VTCA MUST establish a disaster recovery plan which outlines the steps to be taken to reestablish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the VTCA, a VTCA MUST ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

A VTCA must identify the disaster recovery process in its CPS.

4.9 VTCA TERMINATION

All issues relating to the termination of a VTCA must be presented to the PMA for oversight of the termination process. In the event of termination, a VTCA in cooperation with the PMA must notify its Subscribers, notify all CA's with whom it is cross certified, revoke all certificates it issued, and arrange for the continued retention of the VTCA's keys and information.

A VTCA's archives SHOULD be retained in the manner and for the time indicated in Section 4.6.2.

5. PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS FOR THE VTCA OR AUTHORIZED CA

A VTCA SHALL impose physical security requirements that provide similar levels of protection to those specified below.

5.1.1 Site Location and Construction

A VTCA SHALL be located in an area approved by the PMA. The site will be consistent with facilities used for housing other equipment of equivalent security and trust (for example network authentication or authorization services) with access limited to authorized personnel. The associated CPS SHALL specify the type of facility or mechanism used for controlling access to the VTCA.

The system components and operation of a VTCA SHALL be contained within a physically protected environment to deter, detect, and prevent unauthorized use of, access to, or disclosure of sensitive information. This includes the servers, workstations, and any external cryptographic hardware modules or tokens used in connection with providing VTCA services.

Access to VTCA hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section 5.2.1. Access shall be controlled through the use of: electronic access controls, mechanical, combination locksets, or deadbolts. The implemented access controls shall be manually or electronically monitored for unauthorized intrusion at all times.

Subscribers are responsible for ensuring that their private keys are physically secured or protected with an appropriate access control product.

A VTCA MUST conduct regular security and privacy threat risk assessments

5.1.2 Electrical Power

The facility that houses VTCA equipment shall be supplied with power and air conditioning sufficient to create a reliable operating environment.

A VTCA's equipment shall have backup capability sufficient to allow its orderly shutdown in the event primary electrical power is lost.

5.1.3 Water Exposures

This CP makes no stipulation on prevention of exposure of the VTCA equipment to water beyond that called for by best business practice. A VTCA's equipment shall be installed such that it is not in danger of exposure to water.

5.1.4 Fire Prevention and Protection

This CP makes no stipulation on prevention of exposure of the VTCA's equipment to fire beyond that called for by best business practice. An automatic fire extinguishing system shall be installed in accordance with local policy and code.

5.1.5 Media Storage

Storage media used by the VTCA system SHALL be protected from environmental threats such as temperature, humidity, magnetism and fire. Media that contains audit, archive, or backup information SHALL be stored in a separate offsite location from VTCAs equipment.

5.1.6 Waste Disposal

All media used for the storage of information such as keys, activation data or VTCA files will be sanitized or destroyed before being released for disposal in accordance with local policy.

5.1.7 Offsite Backup

System backups, sufficient to recover from system failure, SHALL be made on a periodic schedule, described in the applicable CPS. At least one backup copy SHALL be stored at an offsite location separate from VTCA's equipment. The backup SHALL be stored at a site with physical and procedural controls commensurate to those of the operational VTCA system.

5.2 PROCEDURAL CONTROLS FOR THE VTCA

5.2.1 Trusted Roles

All employees that have access to or control over cryptographic operations that may materially affect the issuance, use, suspension, or revocation of a VTCAs certificates, including access to restricted operations of a VTCA repository, are serving in a trusted role.

Such personnel include, but are not limited to, system administration personnel, operators, engineering personnel, technical support personnel, auditors, and administrators who are designated to manage the operations of a VTCA.

The primary trusted roles defined by this CP are the Certification Authority Administrator (CAA) and the Registration Authority Administrator (RAA). Other trusted roles may be defined in other documents, which describe or impose requirements on the operation of a VTCA.

5.2.1.1 Certification Authority Administrator

The Certification Authority Administrator (CAA) role and the corresponding procedures a CAA will follow shall be defined in detail in the applicable CPS. 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 and the corresponding procedures a RAA will follow shall be defined in detail in the applicable CPS. Primarily, an RAA's responsibilities are:

- Acceptance of subscription, certificate change, certificate revocation/suspension and key recovery requests

- Verification of an applicant's identity

- Transmission of applicant information to the Virginia Tech certification authority

5.2.1.3 Other Trusted Roles

A VTCA SHALL, in its CPS, define other trusted roles to which shall be allocated responsibilities that ensure the proper, safe, and secure operation of a VTCA's equipment and procedures. These responsibilities include:

- Initial configuration of the operating system, including installation of applications, initial setup of new accounts, and configuration of the initial host and network interface.

- Creation of devices to support recovery from catastrophic system loss

- Performance of system backups, software upgrades, and recovery

- Secure storage and distribution of the backups and upgrades to an offsite location

- Changing the host or network interface configuration

- Assignment of operating system security privileges and access controls of host user accounts

- Performance of archive and delete functions of the operating system audit log and other archive data

- Reviewing audit logs and performing compliance audits

To ensure system integrity, the RAA/CAA SHALL be prohibited from performing these responsibilities. Those who perform these responsibilities for a certification authority within the VTPKI SHALL NOT be a RAA/CAA in the same domain. A VTCA SHALL maintain lists, including names, organizations, and contact information, of those who act in these trusted roles, and SHALL make them available during compliance audits.

5.2.2 Number of Persons Required Per Task

To help ensure that one person acting alone cannot circumvent safeguards, multiple roles and individuals should share responsibilities for operation of a VTCA. Each VTCA account shall have limited capabilities commensurate with the role of the account holder.

A VTCA should recognize multiple distinct roles to accomplish its cryptographic operations. No one individual should perform multiple roles. Duties should be split between multiple personnel so that the approach taken provides reasonable resilience to insider attack.

5.2.3 Identification and Authentication for Each Role

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

- Authorized for access to a VTCA site

- Authorized for physical access to a VTCA system

- Given a certificate and account on a VTCA system for the performance of their role

Each of these certificates and accounts (with the exception of VTCA signing certificates) MUST:

- Be directly attributable to an individual

- NOT be shared.

- Be restricted to actions authorized for that role through the use of a VTCA's software, operating system, and procedural controls

VTCA operations MUST be 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 a VTCA MUST:

- Be appointed by the PMA

- Have received comprehensive training with respect to the duties they are to perform

- NOT be assigned duties that may cause a conflict of interest with their VTCA duties

A VTCA SHALL identify in its applicable CPS, the individual or group responsible for its operation.

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling trusted roles SHALL be selected on the basis of trustworthiness and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit a VTCA SHALL be set forth in the applicable CPS.

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 CP shall be required to have a background check. Such checks are to be performed solely to determine the suitability of a person to fill a VTCA role, and SHALL NOT be released except as required by Virginia State law.

5.3.3 Training Requirements

All personnel involved in the operation of a VTCA MUST be appropriately trained. Topics will include:

- Security principles and mechanisms of a VTCA and registration authority service

- Stipulations of this CP and its corresponding CPS

- The operation of the software and/or hardware used in a VTCA system

- The duties they are expected to perform

5.3.4 Retraining Frequency and Requirements

The requirements of 5.3.3 must be kept current to accommodate changes in a VTCA system. Refresher training SHALL be conducted in accordance with these changes.

5.3.5 Job Rotation Frequency and Sequence

This CP makes no stipulation regarding frequency or sequence of job rotation. Local policies, which do impose requirements, SHALL provide for continuity and integrity of a VTCA service.

5.3.6 Sanctions for Unauthorized Actions

The PMA SHALL take appropriate administrative and disciplinary actions against personnel who have performed actions involving a VTCA or its Repository not authorized in this CP or the applicable CPS.

5.3.7 Contracting Personnel Requirements

Contractor personnel employed to perform functions pertaining to a VTCA SHALL meet the same set of requirements described in this section 5.3.

5.3.8 Documentation Supplied to Personnel

A VTCA MUST make available to its CAA and RAA personnel the certificate policies it supports, its applicable CPS, and documentation sufficient to define duties and procedures relevant to their positions.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation by the VTCA

Cryptographic keys for the authority certificates used by a VTCA SHALL be generated in FIPS 140 validated cryptographic modules with the possible exception of the PKC used to issue "Test" certificates.

Cryptographic keys for end entity certificates SHALL be generated by the end entity, not by a VTCA, except possibly in the case of keys to be used for data encryption where escrow of the private key is required (see Section 6.2.3.1). Except as defined in section 6.2.3.1, the end entity SHALL NOT reveal their private key(s) to a VTCA or any other entity.

6.1.2 Private Key Delivery to Subscriber

In most cases VTCA Subscribers will generate their own key pairs and thus will not require delivery of their private key. Whenever keys are generated by an entity other than the Subscriber (see Section 6.2.3.1), delivery of the private key to the Subscriber shall be effected in such a manner that no entity other than the key generating agent, the escrow agent (if any) and the Subscriber have access to an unencrypted version of the private key at any time. Only the escrow agent (if any) and the Subscriber may retain copies of the private key. Subscribers must provide proof of the private key possession. The Procedure to implement the requirements of this section MUST be documented in the CPS.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys SHALL be delivered to the certificate issuer in an authenticated manner set forth in the applicable CPS.

6.1.4 VTCA Public Key Availability

A VTCA SHALL post a copy of its authority certificate, and a copy of any VTCA authority PKC that it signs, to its public Repository. In addition, a VTCA SHOULD post to its Repository a copy of any cross certificate that it signs and any cross certificate issued to it by another CA.

6.1.5 Key Sizes

Key sizes MUST be commensurate with the risk that they might be compromised during the validity period of the certificate or any document signed with the private key. Details of the specific key sizes and the relative LOAs MUST be documented in the associated CPS.

All FIPS approved signature algorithms SHALL be considered acceptable.

If the PMA determines that the security of a particular algorithm might be compromised, it MAY require a VTCA to revoke the affected PKCs.

6.1.6 Public Key Parameters Generation

No stipulation.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Hardware/Software Subscriber Key Pair Generation

For subscribers, software or hardware SHALL be used to generate pseudo random numbers, key pairs, and symmetric keys. Any pseudo random numbers used for key generation material SHALL be generated by a FIPS approved method.

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

Digital signature key pairs may be used for authentication, non repudiation and message integrity. Encryption key pairs may be used for session key establishment, and data encryption. A VTCA signing key pair are the only keys permitted to be used for signing certificates, CRLs, and CARLs.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [latest version of FIPS 140 series]. A VTCA MAY determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published in the associated CPS.

6.2.2 CA Private Key Multi Person Control

A Virginia Tech Root CA of the VTPKI SHALL implement M of N authentication.(M number of persons from N total number of persons).

6.2.3 Key Escrow of CA Private Signature Key

Under no circumstances SHALL a signature key, which is used to support non repudiation services, be escrowed.

6.2.3.1 Escrow of End Entity Decryption Keys

A VTCA MAY escrow keys which are used to support data encryption.

6.2.4 Private Key Backup

A VTCA SHALL maintain a backup copy of its private key in order to reestablish functionality in case of destruction of the key.

6.2.4.1 Backup of CA Private Signature Key

An Entity MAY optionally back up its own Digital Signature private key. If so, the keys MUST be copied and stored in encrypted form and protected at a level no lower than that stipulated for the primary version of the key.

6.2.4.2 Backup of End Entity Private Signature Key

An issuing VTCA SHALL NOT back up, escrow, or copy Subscriber's private signature keys, except as provided under section 6.2.3.1.

6.2.5 Private Key Archival

If a VTCA is acting as a key recovery agent, then it SHALL archive private key management keys as part of its service, if required by local policy or law. Private signature keys supporting non repudiation services SHALL NOT be archived.

6.2.6 Private Key Entry into Cryptographic Module

The private keys of a VTCA SHALL be generated by and remain in a cryptographic module. A VTCAs private key MAY be backed up only in accordance with Section 6.2.4.1.

6.2.7 Method of Activating Private Keys

Activation of a VTCA signing key SHALL require one or more authorized individual, as described in section 6.2.2. Activation of an end entity private key MUST require authentication of the Subject to the cryptographic module, either hardware or software.

6.2.8 Methods of Deactivating Private Keys

Cryptographic modules that have been activated MUST NOT be left unattended or otherwise open to unauthorized access. After use, they MUST be deactivated, e.g. via a manual logout procedure, or by a passive timeout. Hardware cryptographic modules SHOULD be removed and stored when not in use.

6.2.9 Method of Destroying Subscriber Private Signature Keys

Subscriber private signature keys SHOULD be destroyed when they are no longer needed, or when all PKCs to which they correspond have expired or are revoked and no reinstatement is anticipated.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

A VTCA's public key is archived as part of the certificate archival.

6.3.2 Usage Periods for the Public and Private Keys

The key usage periods for keying material are described in Section 3.2.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock VTCA or Subscriber private keys, in conjunction with any other access control, SHALL have an appropriate level of strength for the keys or data to be protected. Activation data SHALL be generated in conformance with the most current version of the related FIPS standard. If the activation data MUST be transmitted, it SHALL be via a channel of appropriate protection, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Data used to unlock private keys SHALL be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data SHALL NOT be shared. Details are set forth in the applicable CPS.

6.4.3 Other Aspects of Activation Data

This policy makes no stipulation on the life of activation data. A VTCA MAY define activation data requirements in the applicable CPS.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions MUST be provided. They MAY be provided by the operating system, or through a combination of operating system, software, and physical safeguards. A VTCA SHALL provide for the following functionality:

• Require authenticated logins using credentials with at least as high an LOA as a VTCA itself

• Provide a security audit capability

• Restrict access control to a VTCA

• CA services and PKI roles

• Enforce separation of duties for PKI roles

• Identification and authentication of PKI roles and associated identities

• Trusted paths for identification of PKI roles and associated identities

• Non reuse of object or require separation for VTCA random access memory

• Use of cryptography for session communication and database security

• Archive VTCA history and audit data

• Require a recovery mechanism(s) for keys and a VTCA system

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The System Development Controls for a VTCA are as follows:

• The design and development process MUST provide sufficient documentation

• VTCA hardware and software SHALL be dedicated to performing the task(s) of the VTCA. There SHALL NOT be any applications, hardware devices, network connections, or component software which are not required by the operation of a VTCA

• Hardware and software procured to operate a VTCA SHALL be obtained in a fashion to reduce the likelihood of tampering with any particular component

• Care SHALL be taken to prevent malicious software from being loaded onto a VTCA. Hardware and software updates SHALL be obtained or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined and documented manner

6.6.2 Security Management Controls

A formal configuration management methodology MUST be used for installation and ongoing maintenance of a VTCA system. When the VTCA software is first loaded, there must be a method for a VTCA to verify the software on the system:

• Originated from the software developer

• Has not been modified prior to installation

• Has been adequately tested and verifiably approved for use in a production environment

• Is the tested and approved version

A VTCA MUST provide a mechanism to periodically verify the integrity of the software. A VTCA MUST also have mechanisms and policies in place to control and monitor the configuration of the VTCA system.

6.6.3 Life Cycle Security Ratings

Integrity of the system SHALL be checked according to the current local operating and system integrity check policy.

6.7 NETWORK SECURITY CONTROLS

Protection of Certificate Management equipment SHALL be provided against known network attacks. Use of appropriate boundary controls SHALL be employed. All unused network ports and services SHALL be turned off. Any network software present on the Certificate Management equipment SHALL be necessary to the functioning of the Certificate Management application. The equipment of a Virginia Tech Root CA SHALL be implemented using a stand-alone (offline) configuration. Subordinate CA equipment MAY be implemented using either an on-line or off-line configuration.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

Requirements for cryptographic modules are as stated above in Section 6.2.

7. CERTIFICATE AND CARL/CRL PROFILES

In order to promote interoperability, a VTCA MUST issue PKCs and CARL/CRLs which are compatible with the IETF RFC 2459 (or successor). The profiles for these documents SHALL be published or identified in the applicable VTCA's CPS. These profiles SHALL include the format, syntax, and semantics of each field used.

7.1 CERTIFICATE PROFILE

A VTCA SHALL issue X.509 version 3 (or higher) PKCs.

7.1.1 Version Numbers

X.509 version 3 PKCs MUST be identified with an integer "2" in the Version Number field.

7.1.2 Certificate Extensions

Standard extensions, when populated, SHALL be described in an appropriate Certificate Profile. Certificate Profiles SHALL be documented or referenced in the CPS in such a manner that a Relying Party can locate an online copy of the profile for any PKC issued by a VTCA.

Whenever private extensions are used, they SHALL be identified and fully defined in the applicable CPS. Private extensions MUST be assigned appropriate OIDs.

VTCAs that support an OCSP service, either hosted locally or provided by an Authorized Responder, MUST provide for the inclusion of a value for a uniform Resource Indicator (URI) access Location and the OID value id-ad-ocsp for the access Method in the Access Description SEQUENCE of the Authority Info Access extension.

7.1.3 Algorithm Object Identifiers

PKCs issued under this CP MUST use FIPS-140 approved asymmetric encryption for signatures. PKCs under this CP MUST use the standard OIDs for both the signatures and subject keys corresponding to the type of asymmetric encryption used.

7.1.4 Name Forms

Where required as set forth above, the subject and issuer fields of the base PKC SHALL be populated with an X.500 Distinguished Name as documented in the CPS, with the attribute type as further constrained by [RFC2459]. DC components MUST be included.

7.1.5 Name Constraints

Subject and Issuer Distinguished Names MUST be present in all certificates.

7.1.6 Certificate Policy Object Identifier

PKCs issued under this CP SHALL assert in the CertPolicyId field the OID appropriate to the Level of Assurance with which it was issued as provided in Section 1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

The CPSuri policy qualifier SHALL contain a pointer to an online, digitally signed copy of the CPS under which the PKC was issued. The CPS SHALL include a URI reference to this CP as specified in Section 1.2.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

No stipulation.

7.1.10 Certificate Serial Numbers

Each PKC signed by a VTCA SHALL include an integer serial number unique among all PKCs issued by that VTCA. A given serial number SHALL NOT be reused even if an otherwise identical PKC is reissued.

7.2 CARL/CRL PROFILE

7.2.1 Version Numbers

A VTCA SHALL issue X.509 version 2 (or higher) CARLs/CRLs.

7.2.2 CARL and CRL Entry Extensions

Detailed CARL/CRL profiles addressing the use of each extension SHALL be defined by a VTCA in corresponding CPS(s).

7.2.3 OCSP Services

OCSP MUST be supported by a VTCA. The CPS MUST document the OCSP services provided, the message formats supported, and define the timeliness of the certificate status data returned.

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

This policy SHALL be reviewed in its entirety every year. Errors, updates, or suggested changes to this document SHALL be communicated to every VTCA and SHALL be available in the Repository to Subscribers. Such communication MUST include a description of the change, a change justification, and contact information for the person requesting the change. All policy changes under consideration by the PMA SHALL be published in the Repository for a period of at least one month. The PMA SHALL accept, accept with modifications, or reject the proposed change after completion of the review period.

8.2 PUBLICATION AND NOTIFICATION POLICIES

The PMA SHALL see that a list of VTCAs asserting this policy is maintained. Proposed changes to the policy and policy updates SHALL be sent to those VTCAs. Each VTCA SHALL notify its subscribers of any changes to the certificate policy via a mechanism described in its CPS.

8.2.1 Amendments Generally

The PMA shall be entitled to amend this CP prospectively but not retroactively.

8.2.2 Urgent Amendments Exception

An amendment SHALL be deemed "urgent" and become effective immediately. "Urgent" SHALL be designated if, in the sole discretion of the PMA, failure to make the amendment may result in a compromise of a VTCA or the VTPKI infrastructure generally.

8.2.3 Assent to Amendments

In the case of an amendment that is not deemed "urgent," a Subscriber's decision not to request revocation of a PKC prior to the effective date of an amendment SHALL constitute agreement to

the amendment. In the case of an amendment that is deemed "urgent," a Subscriber's decision not to request revocation upon notification SHALL constitute agreement to the amendment.

8.2.4 Maintenance of Prior Versions

No stipulation.

8.3 CPS APPROVAL PROCEDURES

VTCAs MUST comply with the procedures of the PMA. Where a CPS contains information relevant to the security of a VTCA, all or part of the CPS need not be made publicly available.

8.4 WAIVERS

No stipulation.

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 Material	Random numbers, pseudo random numbers, and cryptographic 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 collectively to the Self Signed Root and Global Virginia Tech Root CAs and all of the Subordinate CAs within each 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.