Virginia Tech Global Software Token User Certification Authority Certification Practice Statement

Object Identifier 1.3.6.1.4.1.6760.5.2.3.6.1

Date: 7/24/17

Version: 1.1

Table of Contents

Document History

Version	Release Date	Author	Status + Description
1.1	7/24/17	Karen Herrington	Draft
1.2	3/26/17	Karen Herrington	Final version

Detailed History of Changes

Acknowledgments

This Virginia Tech Global Software Token User Certification Authority CPS endorses in whole or in part the following industry standards:

- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

This CPS is created according to the requirements of the following schemes and endorses these in whole or in part:

- AICPA/CICA, WebTrust 2.0 Program for Certification Authorities.
- AICPA/CICA, WebTrust For Certification Authorities – Extended Validation Audit Criteria.
- CA/B Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates

GlobalSign® and the GlobalSign Logo are registered trademarks of GMO GlobalSign K.K.

1.0 Introduction

This Certification Practice Statement (CPS) of Virginia Tech Global Software Token User Certification Authority (herein after referred to as GSTUCA) applies to the products and services of Virginia Polytechnic Institute and State University (Virginia Tech). Primarily this pertains to the issuance and lifecycle management of Certificates including validity checking services. This CPS may be updated from time to time as outlined in Section 1.5 *Policy Administration*. The latest version may be found on the following URL http://www.pki.vt.edu.

A CPS highlights the *"procedures under which a Digital Certificate is issued to a particular community and/or class of application with common security requirements"*. This CPS meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format *(RFC 3647 obsoletes RFC 2527).* An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of electronic signatures and Certificate management. While certain section titles are included in this CP according to the structure of RFC 3647, the topic may not necessarily apply to Services of GSTUCA. These sections state *'No stipulation'*. Where necessary additional information is presented in subsections to the standard structure. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability with other third party CAs and provides Relying Parties with advance notice of GSTUCA practices and procedures. Additional assertions on standards used in this CPS can be found under section *"Acknowledgements"* on the previous page.

This CPS is final and binding between Virginia Tech, a state agency and public educational institution,

and

the Subscriber and/or Relying Party, who uses, relies upon or attempts to rely upon certification services made available by the Certification Authority referring to this CPS.

This CPS addresses the technical, procedural and personnel policies and practices of the GSTUCA during the complete life cycle of Certificates issued by the GSTUCA.

The GSTUCA operates within the scope of activities of Virginia Tech. This CPS addresses the requirements of the CA that issues Certificates of various types under the Certificate Policy of GlobalSign nv-sa and its Trusted Root Program. The chaining to any particular Issuing CA may well vary depending on the choice of intermediate Certificate and/or Cross Certificate used or provided by a platform or client.

For Subscribers, this CPS becomes effective and binding by accepting a Subscriber Agreement or Terms of Use. For Relying Parties, this CPS becomes binding by relying upon a Certificate issued under this CPS. In addition, Subscribers are required by the Subscriber Agreement to inform their Relying Parties that the CPS is itself binding toward those Relying Parties.

1.1 Overview

This CPS applies to the complete hierarchy of Certificates issued by GSTUCA. The purpose of this CPS is to present the practices and procedures in managing Certificates and to demonstrate compliance with requirements pertaining to the issuance of Certificates according to GSTUCA's own and industry requirements pursuant to the standards set out above. This CPS aims at facilitating the GSTUCA in delivering certification services and managing the Certificate lifecycle of any issued client, server and other-purpose end entity Certificates. The Certificate types addressed in this CPS are the following:

1.1.1.1.1 SMIME/Client Authentication	A personal certificate of medium assurance with reference to professional context

These Certificates shall be issued and managed in accordance with CA/Browser Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (the "Baseline Requirements"). An indication of compatibility is the inclusion of CA/Browser Forum Policy OIDs as detailed in Section 1.2.

GSTUCA Certificates:

- Can be used for digital signatures in order to replace handwritten signatures
- May be used for encryption of data
- Can be used to authenticate clients in SSL/TLS connections,

This CPS identifies the roles, responsibilities and practices of all entities involved in the lifecycle, use, reliance upon and management of GSTUCA Certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved, including GSTUCA, their nominated RA, Subscribers and Relying Parties. Certain provisions might also apply to other entities such as the certification service provider, application provider etc.

A GlobalSign Certificate Policy (CP) complements this CPS. The purpose of the GlobalSign CP is to state the *"what is to be adhered to"* and, therefore, set out an operational rule framework for the broad range of GlobalSign products and services. The latest version of the CP governing this CPS can be found on https://www.globalsign.com/repository

This CPS states *"how the Certification Authority adheres to the Certificate Policy".* In doing so, this CPS features a greater amount of detail and provides the end user with an overview of the processes, procedures and conditions that the GSTUCA uses in creating and maintaining the Certificates that it manages. In addition to this CPS GSTUCA maintains additional documented polices addressing such issues as:

- Business continuity and disaster recovery
- Security policy
- Personnel policies
- Key management policies
- Registration procedures

A digitally signed copy of the GSTUCA CPS (Certification Practice Statement) is available at http://www.pki.vt.edu/gstuca/cps.

A Subscriber or Relying Party of a Certificate must refer to this CPS in order to establish trust in a Certificate issued by GSTUCA as well as for information about the prevailing practices of GSTUCA. It is also essential to establish the trustworthiness of the entire Certificate chain of the hierarchy. This includes the Root CA Certificate as well as any operational Certificates. This can be established on the basis of the assertions within this CPS.

1.1.2 Certificate Naming

The exact names of the GSTUCA Certificates that make use of this CPS are:

- Virginia Tech Global Software Token User CA with serial number 48:CA:81:80:1B:C2:51:28:37:D8:3E:C4:DD:AB

Certificates allow entities that participate in an electronic transaction to prove their identity to other participants, sign data digitally or encrypt data. By means of a Certificate, GSTUCA provides confirmation of the relationship between a named entity (Subscriber) and its Public Key. The process to obtain a Certificate includes the identification, naming, authentication and registration of the Subscriber as well as aspects of Certificate management such as the issuance, revocation and expiration of the Certificate. By means of this procedure to issue Certificates, GSTUCA provides adequate and positive confirmation about the identity of the user of a Certificate and a positive link to the Public Key that the Subscriber uses. GSTUCA makes available Certificates that can be used for non-repudiation, encryption and authentication.

1.2 Document Name and Identification

This document is the Virginia Tech Global Software Token User Certification Authority Certification Practice Statement.

The Virginia Tech GSTUCA organizes its OID arcs for the various certificates and documents described in this CPS (Which may be updated from time to time) as follows:

1.3.6.1.4.1.6760.5.2.3.6.1 Software Token Personal Digital Certificate Policy

The OID for GlobalSign nv-sa (GlobalSign CA) is an iso (1) identified-organization (3) dod (6) internet (1) private (4) enterprise (1) GlobalSign nv-sa (4146). GlobalSign CA organizes its OID arcs for the various Certificates and documents described in its CP as follows:

1.3.6.1.4.1.4146.1.60 CA Chaining Policy – Trusted Root

In addition to these identifiers, all Certificates that comply with the Baseline Requirements will include the following additional identifiers:-

2.23.140.1.2.2 Organization Validation Certificates Policy

1.3 PKI participants

This CPS serves the communities defined below.

- VT-ACTIVE-MEMBER - An active student or employee at Virginia Tech.

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

1.3.1 Certification Authorities

GSTUCA is a Certification Authority (CA) that issues trusted Certificates in accordance with this CPS. As a Certification Authority, GSTUCA performs functions related to Certificate lifecycle management such as Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation. GSTUCA also provides Certificate status information using an online repository in the form of a Certificate Revocation List (CRL) distribution point and/or Online Certificate Status Protocol (OCSP) responder.

GSTUCA ensures the availability of all services pertaining to the management of Certificates, including without limitation the issuing, revocation and status verification of a Certificate, as they may become available or required in specific applications. The GSTUCA does not have the authority to issue subordinate CA PKCs.

1.3.2 Registration Authorities

GSTUCA issues certificates in a self-service mode using a Certificate Manager application. The Certificate Manager application performs the registration functions of identifying and authenticating subscribers who apply for certificates or make revocation, reissuance or renewal requests.

Offices designated by the Vice President for Information Technology or designee may also act as Registration Authorities for Certificates GSTUCA issues, particularly pertaining to revocation or key recovery requests made by someone other than the Subscriber.

1.3.3 Subscribers

Subscribers to GSTUCA are natural persons that successfully apply for and receive a Certificate to support their use in transactions, communications and the application of Digital Signatures.

A *Subscriber*, as used herein, refers to both the Subject of the Certificate and the entity that contracted with the GSTUCA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

For all categories of Subscribers, additional credentials are required as explained in the online process for the application for a Certificate.

1.3.4 Relying Parties

To verify the validity of a Certificate, Relying Parties must always refer to GSTUCA's revocation information either in the form of a CRL distribution point or an OCSP responder.

Only Relying Parties that accept this CPS in its entirety without any limitations (financial or otherwise) can make appropriate use of a PKC issued by the GSTUCA.

1.3.5 Other Participants

GSTUCA is cross signed by GlobalSign nv-sa via its Trusted Root program as detailed within the GlobalSign CP on https://www.globalsign.com/respository

1.4 Certificate Usage

A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1 Appropriate certificate usage

End entity Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Certificates issued by GSTUCA can be used for public domain transactions that require:

- **Non-repudiation:** A party cannot deny having engaged in the transaction or having sent the electronic message.
- **Authentication:** The assurance to one entity that another entity is who he/she/it claims to be.
- **Integrity:** The assurance to an entity that data has not been altered intentionally or unintentionally) from sender to recipient and from time of transmission to time of receipt.

Digital signature: Digital (Electronic) signature can only be used for specific transactions that support digital signing of electronic forms, electronic documents, or electronic mail. The Certificate is only warranted to produce Digital Signatures in the context of applications that support Certificates. Certificates that are appropriate for Digital Signatures are the following:

- SMIME/Client Authentication**:** authentication of a natural person (medium bronze level assurance)

Assurance levels: Subscribers should choose an appropriate level of assurance to which Relying Parties will confidently transact.

Assurance Level	Applicability

Test 1.3.6.1.4.1.6760.5.2.2.1.1	This level is not used.
Rudimentary 1.3.6.1.4.1.6760.5.2.2.2.1	This level is not used.
Basic 1.3.6.1.4.1.6760.5.2.2.3.1	This level is not used.
Medium Bronze 1.3.6.1.4.1.6760.5.2.2.4.1	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud. Refer to the InCommon Assurance Program for details on the Bronze profile.
Medium Silver 1.3.6.1.4.1.6760.5.2.2.5.1	This level is reserved for future use, where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud. Refer to the InCommon Assurance Program for details on the Silver profile.
High 1.3.6.1.4.1.6760.5.2.2.6.1	This level is reserved for future use, where threats to data are high, or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

Any other use of a Certificate is not supported by this CPS. When using a Certificate the functions of electronic signature (non-repudiation), authentication (Digital Signature) and encryption are permitted together within the same Certificate. The different terms relate to different terminologies used by IETF and the vocabulary adopted within the legal framework of the European Union Directive 1999/93/EC (a community framework on electronic signatures).

1.4.2 Prohibited certificate usage

Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Any usage of the Certificate inconsistent with these extensions is not authorized.

Certificates issued under this CPS do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment into which the Certificate has been installed is not free from defect, malware or virus.

Certificates issued under this CPS may not be used:-

- for any application requiring fail safe performance such as
  - the operation of nuclear power facilities
  - air traffic control systems
  - aircraft navigation systems
  - weapons control systems
  - any other system whose failure could lead to injury, death or environmental damage; or
- where prohibited by law.

1.4.2.1 Certificate extensions

Certificate extensions comply with X.509 v.3 standards.

- SMIME/Client Authentication: Client Authentication and Email Protection EKU
- Smart Card Logon EKU

1.4.2.2 Critical Extensions

GSTUCA also uses certain critical extensions in the Certificates it issues such as:

- A basic constraint in the key usage to show whether a Certificate is meant as a CA or not;
- To show the intended usage of the key; and
- To show the number of levels in the hierarchy under a CA Certificate.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Requests for information on the compliance of Issuing CAs with accreditation schemes as well as any other inquiry associated with this CPS should be addressed to:

Virginia Tech Public Key Infrastructure Policy Management Authority (VTPKI PMA).

1.5.2 Contact Person

Chair, VTPKI PMA
314 Burruss Hall
800 Drillfield Dr.
Blacksburg, VA 24060

1.5.3 Person Determining CPS Suitability for the Policy

Concerns about possible abuse of this CPS, should be directed in writing to the VTPKI PMA.

1.5.4 Procedures

The GSTUCA complies with the procedures of the VTPKI PMA, published at www.pki.vt.edu.

1.5.4.1 Changes with notification

Updated versions of this CPS are provided to parties that have a legal right to receive such updates.

1.5.4.2 Version management and denoting changes

Changes are denoted through new version numbers for the CPS. New versions are indicated with an integer number followed by one decimal that is zero. Minor changes are indicated through one decimal number that is larger than zero. Minor changes include:

- Minor editorial corrections
- Changes to contact details

1.6 Definitions and acronyms

Activation Data: Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

Applicant Representative: A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a Certificate Request on behalf of the Applicant, and/or (ii) who signs and submits a

Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA.

Application Software Supplier: A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.

Archive: Long term, physically separate storage.

Attestation Letter: A letter attesting that Subject Identity Information is correct.

Audit Criteria: The requirements described in this document and any requirements that an entity must follow in order to satisfy the audit scheme selected under section 16.1.

Audit Report: A statement, report, or letter issued by a Qualified Auditor stating a CA's or RA's compliance with these Requirements.

Authenticate: To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to possible unauthorized modification in an automated information system, or establish the validity of a transmitted message.

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.

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.

Backup: Copy of files and programs made to facilitate recovery if necessary.

Binding: A statement by an RA of the relationship between a named entity and its public key.

CDS (Certified Document Services): A document signing architecture created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 6.0.

Certificate: An electronic document that uses a Digital Signature to bind a Public Key and an identity.

Certificate Beneficiaries: The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom GlobalSign CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier, and all Relying Parties who reasonably rely on a Valid Certificate.

Certificate Data: Certificate Requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Request: Communications described in Section 10 requesting the issuance of a Certificate.

Certificate Revocation List: A regularly updated timestamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Client: 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: A violation of a security policy that results in loss of control over sensitive information.

Confidentiality: Assurance that information is not disclosed to unauthorized entities or processes.

Country: Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations.

CPSuri: A PKC standard extension that provides a URI pointing to an online copy of the CA's CPS.

Cross Certificate: A certificate that is used to establish a trust relationship between two Root 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]

Data Integrity: Assurance that the data are unchanged from creation to reception.

Delegated Third Party: A natural person or Legal Entity that is not the CA but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Digital Signature: To encode a message by using an asymmetric cryptosystem and a Hash function such that a person having the initial message and the signer's Public Key can accurately determine whether the transformation was created using the Private Key that corresponds to the signer's Public Key and whether the initial message has been altered since the transformation was made.

Distinguished Name: Same as Subject Name.

Domain Authorization: Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a certificate for a specific Domain Namespace.

Domain Authorization Document: Documentation provided by, or a CA's documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of Applicant to request a Certificate for a specific Domain Namespace.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Domain Name System: An Internet service that translates Domain Names into IP addresses.

Effective Date: The date, as determined by the eligible audit schemes, on which Requirements come into force.

End Entity: Relying Parties and Subscribers.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

Expiry Date: The "Not After" date in a certificate that defines a Certificate's validity period.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a Country, or political subdivision within such Country (such as a state, province, city, county, etc.).

Hash (e.g. SHA1 or SHA256): An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other

fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or Google Safe Browsing list, or names the CA identifies using its own risk-mitigation criteria.

Hardware Security Module (HSM): An HSM is type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.

Integrity: Protection against unauthorized modification or destruction of information. . 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.

Internal Server Name: A server name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

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.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Incorporate by Reference: To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message. Such an incorporated message shall have the same effect as if it had been fully stated in the message.

Independent Audit: An audit that is performed by a Qualified Auditor and that determines an entity's compliance with the Baseline Requirements and one or more of the audit schemes listed in Section 17.1 of the Baseline Requirements

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

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

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a Country's legal system.

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.

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. 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 alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate. See also OCSP Responder.

Public Key Certificate: As used in this CPS, refers to an object conforming to X.509v3 or higher.

Policy Management Authority: 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: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure (PKI): A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2 (Identity/ Qualifications of Assessor).

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Rekey: 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

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such supplier merely displays information relating to a Certificate.

Renew: The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Requirements: This document.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:

http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Root Key Generation Script: A documented plan of procedures for the generation of the Root CA Key Pair**.**

Server: A system entity that provides a service in response to requests from clients.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the commonName field.

Subject Name: The relevant attributes included under Subject in the certificate profile.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA.

Trusted Platform Module (TPM): A hardware cryptographic device which is defined by the Trusted Computing Group. https://www.trustedcomputinggroup.org/specs/TPM.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered Domain Name: A Domain Name that is not a Registered Domain Name.

Uniform Resource Identifier: 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.

Uniform Resource Locator: Refers to the subset of URI that identify resources via a representation of their primary access mechanism (e.g., their network "location"), rather than identifying the resource by name or by some other attribute(s) of that resource. See RFC1738 and RFC1808.

Uniform Resource Name: 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.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists: Someone who performs the information verification duties specified by the Baselines Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

Virginia Tech Certification Authority: Collectively, the Self Signed Virginia Tech Root CA, its subordinates, and CAs implemented under GlobalSign's Trusted Root Program.

WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

X.509: The standard of the ITU-T (International Telecommunications Union-T) for Certificates.

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CAA	Certification Authority Administrator
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
ETSI	European Telecommunications Standards Institute
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
GSCA	GlobalSign Certification Authority
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISO	International Standards organization
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LOA	Level of Assurance
LRA	Local Registration Authority
NAESB	North American Energy Standards Board
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure

PMA	Policy Management Authority
RA	Registration Authority
RAA	Registration Authority AdministratorRFC
RFC	Request for Comments
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
TPM	Trusted Platform Module
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
VAT	Value Added Tax
VOIP	Voice Over Internet Protocol
VTCA	Virginia Tech Certification Authority
VTPKI	Virginia Tech Public Key Infrastructure

2.0 Publication and Repository Responsibilities

2.1 Repositories

GSTUCA publishes all CA Certificates revocation data for issued Certificates, CPS, and any Relying Party agreements or Subscriber Agreements in Repositories. GSTUCA ensures that revocation data for issued Certificates is available through a Repository 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0.5% annually.

GSTUCA may publish submitted information on publicly accessible directories for the provision of Certificate status information.

GSTUCA refrains from making publicly available sensitive and/or confidential documentation including security controls, operating procedures, and internal security policies. These documents are, however, made available to Qualified Auditors as required during any WebTrust or ETSI audit performed on GlobalSign CA.

2.2 Publication of Certificate Information

GSTUCA publishes its CPS, Subscriber Agreements, Relying Party agreements on the following URL http://www.pki.vt.edu. CRLs are published in Repositories. The CRLs contain entries for all revoked un-expired Certificates with a validity period that depends on Certificate type and/or position of the Certificate within the Certificate chain.

2.3 Time or Frequency of Publication

CRLs for end user Certificates are issued at least every 24 hours. CRLs for CA Certificates are issued at least every 6 months and within 24 hours if a CA Certificate is revoked. Each CRL includes a monotonically increasing sequence number for each CRL issued.

New or modified versions of this CPS, Subscriber Agreements, or Relying Party agreements are published within seven days of approval by the VTPKI PMA. Previous versions remain available online 365 days beyond the latest expiration date of any PKC that references this CPS. Archived copies of all CPSs under which the UCA has ever issued a PCA are kept in accordance with the Virginia Record retention policy.

2.4 Access control on repositories

There are no limitations on access to this CPS and CRLs. PKCs are published at the discretion of the Subscriber.

3.0 Identification and Authentication

Virginia Tech acts as an RA that verifies and authenticates the identity and/or other attributes of an Applicant and that the Applicant is associated with either Virginia Tech or one of its affiliated entities.

Applicants are prohibited from using names in their Certificate that infringe upon the intellectual property rights of others.

Virginia Tech RAs authenticate the requests of parties wishing to revoke Certificates.

3.1 Naming

3.1.1 Types of Names

GSTUCA Certificates are issued with subject DNs (Distinguished Names) which meet the requirements of X.500 naming, RFC-822 naming and X.400 naming. CNs (Common Names) respect name space uniqueness and are not misleading.

3.1.2 Need for Names to be Meaningful

- SMIME/Client Authentication: The CN component of a Subject name in a PKC issued by the GSTUCA is the name of the Subscriber to which the PKC is issued. First name, middle initial and last name (Banner name per ED-ID) will be used in the Subject name.

Where possible, GSTUCA uses distinguished names to identify both the Subject and the Issuing CA of a Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers

GSTUCAs may issue end entity anonymous or pseudonymous Certificates provided that such Certificates are not prohibited by applicable policy and where possible name space uniqueness is preserved. GSTUCA reserves the right to disclose the identity of the Subscriber if required by law.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished names in Certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

GSTUCA enforces the uniqueness of each Subject name in a Certificate as follows.

- SMIME/Client Authentication: A Distinguished Name that includes a unique identifier, the organization's name, and the Subject's name.

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers may not request Certificates with any content that infringes the intellectual property rights of another entity. GSTUCA does not require that an Applicant's right to use a trademark be verified. GSTUCA reserves the right to revoke any Certificate that is part of a dispute.

3.2 Initial Identity Validation

GSTUCA may perform identification of the Applicant using any legal means of communication or investigation necessary to identify the Legal Entity or individual.

3.2.1 Method to Prove Possession of Private Key

No stipulation.

3.2.2 Authentication of Organization Identity

Organizational details are replicated from the DirectoryName Name constraints within the Trusted Root CA provided by GlobalSign which have been vetted in accordance with section 3.2.2 of the GlobalSign CPS.

3.2.2.1 Role Based Certificate Authentication

No stipulation.

3.2.3 Authentication of Individual identity

GSTUCA authenticates individuals depending upon the class of Certificate as indicated below.

3.2.3.1 Class 1

Class 1 Certificates are not supported.

3.2.3.2 Class 2 (SMIME/Client Authentication)

Subscriber authenticates with a PID and password plus a second factor.

3.2.4 Non-Verified Subscriber Information

GSTUCA validates all information to be included within the Subject DN of a Certificate.

3.2.5 Validation of Authority

- SMIME/Client Authentication **-** Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over the email address to be listed within the Certificate.

3.2.6 Criteria for Interoperation

Not applicable

3.3 Identification and Authentication for Re-key Requests

The certificates are being issued for a period of two years. The Subscriber must be a member of an approved community at the time of re-keying. Re-keying a PKC means that a new PKC is created using a new, different public key (corresponding to a new, different private key), and a different serial number. If any of the Subject's information from ED-ID has changed, the new information will be used to determine eligibility and attributes for the new PKC.

3.3.1 Identification and Authentication for Re-key After Revocation

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

3.4 Identification and Authentication for Revocation Request

Revocation requests are accepted. The revocation request must identify the certificate to be revoked and explain the reason. See Section 4.9

4.0 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

GSTUCA does not issue Certificates to entities that reside in Countries where the laws of a GSTUCA office location prohibit doing business.

4.1.2 Enrollment Process and Responsibilities

GSTUCA maintains systems and processes that sufficiently authenticate the Applicant's identity for all Certificate types that present the identity to Relying Parties. Applicants must submit sufficient information to allow GSTUCA's RA to successfully perform the required verification. GSTUCA shall protect communications and securely store information presented by the Applicant during the application process.

Generally, the application process includes the following steps (but not necessarily in this order as some workflow processes generate Key Pairs after the validation has been completed):-

- Generating a suitable Key Pair using a suitably secure platform;
- Generating a Certificate Signing Request (CSR) using an appropriately secure tool;
- Submitting a request for a Certificate type and appropriate information;
- Agreeing to a Subscriber Agreement or other applicable terms and conditions; and
- Paying any applicable fees.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

GSTUCA maintains systems and processes to sufficiently authenticate the Applicant's identity in compliance with this CPS. Initial identity vetting will be performed by GSTUCA in line with section 3.2.

4.2.2 Approval or Rejection of Certificate Applications

GSTUCA shall reject requests for Certificates where validation of all items cannot successfully be completed. GSTUCA may also reject requests based on potential brand damage to GSTUCA in accepting the request. GSTUCA may also reject applications for Certificates from Applicants who have previously been rejected or have previously violated a provision of their Subscriber Agreement.

Assuming all validation steps can be completed successfully following the procedures within this CPS then GSTUCA shall approve the Certificate Request.

GSTUCA is under no obligation to provide a reason to an Applicant for rejection of a Certificate Request.

4.2.3 Time to Process Certificate Applications

GSTUCA shall ensure that all reasonable methods are used in order to evaluate and process Certificate applications. Where issues outside of the control of GSTUCA occur, GSTUCA shall strive to keep the Applicant duly informed.

The following approximations are given for processing and issuance.

- **SMIME/Client Authentication -** Approximately 5 minutes.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

The private key is generated by the GSTUCA on the server and issued to the subscriber in a password protected PKCS#12 formatted file. The private key should remain protected by a password and stored in a secure location. A copy of the private key will also be stored encrypted by the GSTUCA public key.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

A confirmation email will be sent to the subscriber's email address of record.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

During the issuance process, the subscriber agrees to the terms of the Subscriber Agreement.

4.4.2 Publication of the Certificate by the CA

GSTUCA will publish the Certificate. The Subscriber will be given the option to suppress visibility. Data on the certificate includes the UID, email address (pid@vt.edu and alias's@vt.edu), and display name (preferred first name + last name).

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

GSTUCA does not notify other entities.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must protect their Private Key taking care to avoid disclosure to third parties. GSTUCA provides a suitable Subscriber Agreement, which highlights the obligations of the Subscriber with respect to Private Key protection. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate.

4.5.2 Relying Party Public Key and Certificate Usage

This GSTUCA CPS provides the conditions under which Certificates may be relied upon by Relying Parties, including the appropriate Certificate services to verify Certificate validity, such as CRL and/or OCSP. Relying Parties should use the information to make a risk assessment and as such are solely responsible for performing the risk assessment prior to relying on the Certificate or any assurances made.

Software used by Relying Parties should be fully compliant with X.509 standards including best practice for chaining decisions around policies and key usage.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Certificates may be renewed upon expiration of the existing certificate.

4.6.2 Who May Request Renewal

Any Subscriber may request renewal of a certificate which he/she owns.

4.6.3 Processing Certificate Renewal Requests

A renewal will consist of the generation of a new certificate with an existing key pair.

4.6.4 Notification of New Certificate Issuance to Subscriber

A notification email will be sent to the Subscriber upon issuance of a new certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2. The new certificate will replace the previous certificate.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3.

4.7 Certificate Re-Key

The certificates are being issued for a period of two years. The Subscriber must be a member of an approved community at the time of re-keying. Re-keying a PKC means that a new PKC is created using a new, different public key (corresponding to a new, different private key), a different serial number and a new expiration date. If any of the Subject's information from ED-ID has changed, the new information will be used to determine eligibility and attributes for the new PKC.

4.7.1 Circumstances for Certificate Re-Key

Certificates may be re-keyed at valid subscriber request.

4.7.2 Who May Request Certification of a New Public Key

As per 4.1.1.

4.7.3 Processing Certificate Re-Keying Requests

As per 4.3.1. A re-key includes revocation of the original certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per 4.4.2. The new certificate will replace the previous certificate.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification is defined as the production of a new Certificate that has details which differ from a previously issued Certificate. The new modified Certificate will have a new Public Key and will have a new ‘Not After’ date.

- GSTUCA treats modification the same as Renewal.

4.8.2 Who May Request Certificate Modification

As per 4.6.2.

4.8.3 Processing Certificate Modification Requests

As per 4.6.3.

4.8.4 Notification of New Certificate Issuance to Subscriber

As per 4.6.4.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As per 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

As per 4.4.2. The new certificate will replace the previous certificate.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificate revocation is a process whereby the serial number of a Certificate is effectively blacklisted by adding the serial number and the date of the revocation to a Certificate Revocation List (CRL). The CRL itself will then be digitally signed with the same Private Key, which originally signed the Certificate to be revoked. Adding a serial number allows Relying Parties to establish that the lifecycle of a Certificate has ended. GSTUCA may remove serial numbers when revoked Certificates pass their expiration date to promote more efficient CRL file size management. Prior to performing a revocation GSTUCA will verify the authenticity of the revocation request. Revocation of a Subscriber Certificate shall be performed under the following circumstances:

- The Subscriber wishes to revoke the Certificate;
- GSTUCA obtains reasonable evidence that the Subscriber's Private Key has been Compromised, no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, or that the Certificate has otherwise been misused;
- GSTUCA receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under the Subscriber Agreement;
- GSTUCA receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
- GSTUCA is made aware that the Certificate was not issued in accordance with this CPS;
- If GSTUCA determines that any of the information appearing in the Certificate is not accurate or is misleading;
- GSTUCA ceases operations for any reason and has not arranged to provide revocation support for the Certificate;
- GSTUCA's right to issue Certificates expires or is revoked or terminated, unless GSTUCA has made arrangements to continue maintaining the CRL/OCSP Repository;
- GSTUCA is made aware of a possible Compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
- Revocation is required by GSTUCA's CP and/or CPS;
- The technical content of format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time);

4.9.2 Who Can Request Revocation

GSTUCA and RAs shall accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber named in the Certificate. GSTUCA may also at its own discretion revoke Certificates.

4.9.3 Procedure for Revocation Request

The Subscriber requests revocation through use of the self-service tool. Once revoked, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs are published according to this CPS.

4.9.4 Revocation Request Grace Period

The 'revocation request grace period' is the time available for a Subscriber to take any necessary actions to respond to a revocation requested by an authorized party. Subscribers are given 72 hours to take appropriate actions otherwise GSTUCA may revoke the Certificate.

4.9.5 Time Within Which CA Must Process the Revocation Request

GSTUCA will begin investigation procedures for a suspected Key Compromise or misuse of a Certificate within 1 business day of receipt of the report.

All revocation requests for end entity Certificates, both those generated automatically via user accounts and those initiated by GSTUCA itself must be processed within a maximum of 5 minutes of receipt.

4.9.6 Revocation Checking Requirements for Relying Parties

Prior to relying upon a Certificate, Relying Parties must validate the suitability of the Certificate to the purpose intended and ensure the Certificate is valid. Relying Parties will need to consult CRL or OCSP information for each Certificate in the chain as well as validating that the Certificate chain itself is complete and follows IETF PKIX standards. This may include the validation of Authority Key Identifier (AKI) and Subject Key Identifier (SKI). GSTUCA will include all applicable URIs within the Certificate to aid Relying Parties in performing the revocation checking process such as:-

- http://crl.globalsign.com/gs/
- http://ocsp2.globalsign.com
- http://vtca.pki.vt.edu:8080/ejbca/publicweb/status/ocsp
- http://www.pki.vt.edu/vtgstuca/crl/cacrl.crl

4.9.7 CRL Issuance Frequency

CRLs will be issued every 12 hours.

4.9.8 Maximum Latency for CRLs

GSTUCA ensures that online CA CRLs are published every 12 hours. A request for revocation received from GSTUCA's RA system during the 12 hour period prior to the next scheduled CRL is included within the CRL if received up to 30 minutes prior.

4.9.9 On-Line Revocation/Status Checking Availability

GSTUCA supports OCSP responses in addition to CRLs. Response times are no longer than 10 seconds under normal network operating conditions.

4.9.10 On-Line Revocation Checking Requirements

Relying Parties must confirm revocation information.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements Related to Key Compromise

GSTUCA and any of its Registration Authorities shall use commercially reasonable methods to inform Subscribers that their Private Key may have been compromised. This includes cases where new vulnerabilities have been discovered or where GSTUCA at its own discretion decides that evidence suggests a possible Key Compromise has taken place. Where Key Compromise is not disputed, GSTUCA shall revoke Subscriber end entity Certificates within 2 business days and publish online CRLs within 30 minutes of creation.

4.9.13 Circumstances for Suspension

GSTUCA does not support suspension.

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

4.10.1 Operational Characteristics

GSTUCA provides a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both. These services are presented to Relying Parties within the Certificate and may refer to any of the following URLs

- http://crl.globalsign.com/gs/
- http://ocsp2.globalsign.com
- http://vtca.pki.vt.edu:8080/ejbca/publicweb/status/ocsp
- http://www.pki.vt.edu/vtgstuca/crl/cacrl.crl

4.10.2 Service Availability

GSTUCA maintains 24x7 availability of Certificate status services and may use additional content distribution network cloud-based mechanisms to aid service availability of cacheable results.

4.10.3 Operational Features

No stipulation

4.10.4 End of Subscription

Subscribers may end their subscription to Certificate services by having their Certificate revoked or naturally letting it expire.

4.11 Key Escrow and Recovery

4.11.1 Key Escrow and Recovery Policy and Practices

GSTUCA escrows the private keys of Subscribers.

Certificates will be retained for 10 years or until the Certificate Authority is phased out, whichever comes first.

The subscriber may click a "Recover" button/link in the VTCA Certificate Manager application and be issued the same key pair and a new certificate. The existing certificate must first be revoked.

The subscriber's private key can be recovered for the subscriber or for a third party, as stipulated in University policy #7035 "Privacy Policy for Employees Electronic Communications". Recovery of a subscriber's private key will be available for 10 years after issuance or until the Certificate Authority is phased out, whichever comes first.

The following parties may request recovery of a subscriber's private key:

- The subscriber
- The appropriate Business Unit supervision (ie. Dept. Head, Dean) of a subscriber
- Virginia Tech Legal Counsel
- The Executor of an Estate / Legal Power of Attorney for a subscriber

Requests for key recovery by anyone other than the subscriber should be directed to 4Help@vt.edu.

1) Request will be made through either Service Now or other method.
2) Request must designate individual who will be receiving the electronic data.
3) Request must be approved by IT leadership.
4) IMCS will extract the data and place it on an external device.
5) Designated recipient will receive external device from IMCS and sign for receipt of keys (Chain of Custody).

4.11.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5.0 Facility, Management, and Operational Controls

5.1 Physical Controls

GSTUCA maintains physical and environmental security policies for systems used for Certificate issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery.

5.1.1 Site Location and Construction

GSTUCA ensures that critical and sensitive information processing facilities are housed in secure areas with appropriate security barriers and entry controls. These are physically protected from unauthorized access, damage and interference and the protections provided are commensurate with the identified risks in risk analysis plans.

5.1.2 Physical Access

GSTUCA ensures that the facilities used for Certificate lifecycle management are operated in an environment that physically protects the services from Compromise through unauthorized access to systems or data. An authorized employee will always accompany any unauthorized person entering a physically secured area. Physical protections are achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the systems hosting the CA operations. No parts of the CA premises are shared with other organizations within this perimeter.

5.1.3 Power and Air Conditioning

GSTUCA ensures that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water Exposures

GSTUCA ensures that the CA systems are protected from water exposure.

5.1.5 Fire Prevention and Protection

GSTUCA ensures that the CA system is protected with a fire suppression system.

5.1.6 Media Storage

GSTUCA ensures that any media used is securely handled to protect it from damage, theft and unauthorized access.

5.1.7 Waste Disposal

GSTUCA ensures that all media used for the storage of information is declassified or destroyed in a generally accepted manner before being released for disposal.

5.1.8 Off-Site Backup

GSTUCA ensures that a full system backup of the Certificate issuance system is sufficient to recover from system failures and is made on a regular basis. Back-up copies of essential business information and software are also taken on a regular basis. Backups are stored on disk in Cassell and on tape in Andrews Information Systems Building.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted roles include but are not limited to the following:

Certification Authority Administrator

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

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

- Startup/Shutdown of the VTCA

Registration Authority Administrator (RAA)

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

- Verify correct third-party authorization for a recovery request
- Extract the data for key recovery and place it on an external device.
- Retrieve the signature of the designated recipient of the keys during the key recovery process.

5.2.2 Number of Persons Required per Task

Key pair and certificate generation under GSTUCA operates in a self-service mode.

Key recovery will require that at least two Administrators from IMCS be involved in the process.

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a trusted role, GSTUCA performs a background check. Each role described above is identified and authenticated in a manner to guarantee that the right person has the right role to support the CA.

5.2.4 Roles Requiring Separation of Duties

No stipulation.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

GSTUCA employs a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function. GSTUCA personnel fulfil the requirement through *expert knowledge, experience and qualifications* with formal training and education, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in Section 5.2.1, are documented in job descriptions. GSTUCA personnel (both temporary and permanent) have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. GSTUCA personnel are formally appointed to trusted roles by senior management responsible for security.

The job descriptions include skills and experience requirements. Managerial personnel are employed who possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

5.3.2 Background Check Procedures

All GSTUCA personnel in trusted roles are free from conflicting interests that might prejudice the impartiality of the CA operations. GSTUCA does not appoint to a trusted role or management position any person who is known to have a conviction for a serious crime or another offence, if such conviction affects his/her suitability for the position. Personnel do not have access to the trusted functions until any necessary checks are completed and results analyzed. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

Any use of information revealed by background checks by GSTUCA shall be in compliance with applicable laws.

5.3.3 Training Requirements

GSTUCA ensures that all personnel performing duties with respect to the operation of the CA receive comprehensive training in:

- CA/RA security principles and mechanisms;
- Software versions in use on the CA system;
- Duties they are expected to perform; and
- Disaster recovery and business continuity procedures.

GSTUCA and RA personnel are retrained when changes occur in GSTUCA or RA systems. Refresher training is conducted as required and GSTUCA shall review refresher training requirements at least once per year.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for trusted roles are aware of changes in the GSTUCA or RA operations, as applicable. Any significant change to the operations has a training (awareness) plan, and the execution of such plan is documented.

5.3.5 Job Rotation Frequency and Sequence

GSTUCA ensures that any change in the staff will not affect the operational effectiveness of the service or the security of the system.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary sanctions are applied to personnel violating provisions and policies within this CPS or CA related operational procedures.

5.3.7 Independent Contractor Requirements

Contractor personnel employed for GSTUCA operations are subject to the same process, procedures, assessment, security control and training as permanent CA personnel.

5.3.8 Documentation Supplied to Personnel

GSTUCA makes available to its personnel this CPS, any corresponding CP and any relevant statutes, policies or contracts. Other technical, operational and administrative documents (e.g., administrator manuals, user manuals, etc.) are provided in order for the trusted personnel to perform their duties.
Documentation is maintained identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files shall be generated for all events relating to the security and services of the CA. Where possible, the security audit logs shall be automatically generated. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non- electronic, shall be retained and made available during compliance audits.

GSTUCA ensures all events relating to the lifecycle of Certificates are logged in a manner to ensure the traceability to a person in a trusted role for any action required for CA services. At a minimum, each audit record includes the following (either recorded automatically or manually) elements:

- The type of event;
- The date and time the event occurred;
- Success or failure where appropriate;
- The identity of the entity and/or operator that caused the event;
- The identity to which the event was targeted; and
- The cause of the event.

5.4.2 Frequency of Processing Log

Audit logs are reviewed periodically for any evidence of malicious activity and following each important operation.

5.4.3 Retention Period for Audit Log

Audit log records are held for a period of time as appropriate to provide necessary legal evidence in accordance with any applicable legislation. Records may be required at least as long as any transaction relying on a Valid Certificate can be questioned.

5.4.4 Protection of Audit Log

The events are logged in a way that they cannot be deleted or destroyed (except for transfer to long term media) for any period of time that they are retained.

The events are logged in a manner to ensure that only individuals with authorized trusted access are able to perform any operations regarding their profile without modifying integrity, authenticity and confidentiality of the data.

The events are protected in a manner to keep them readable during the time of their storage.

The events are date stamped in a secure manner that guarantees, from the date of creation of the record to the end of the archive period that there is a trusted link between the event and the time of its realisation.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries are backed-up in a secure location (for example, a fire proof safe), under the control of an authorized trusted role, and separated from their component source generation. Audit log backup is protected to the same degree as originals.

5.4.6 Audit Collection System (Internal vs. External)

Audit processes are initiated at system start up and finish only at system shutdown. The audit collection system ensures the integrity and availability of the data collected. If necessary, the audit collection system protects the data confidentiality. In the case of a problem occurring during the process of the audit collection GSTUCA determines whether to suspend GSTUCA operations until the problem is resolved, duly informing the GSTUCA impacted asset owners.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

GSTUCA performs regular vulnerability assessments covering all GSTUCA assets related to Certificate issuance, products and services. Assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration or destruction of the Certificate issuance process.

5.5 Records Archival

5.5.1 Types of Records Archived

CAs and RAs archive records with enough detail to establish the validity of a signature and of the proper operation of the CA system. At a minimum, the following data is archived:

GSTUCA key lifecycle management events, including:-

- Key generation, backup, storage, recovery, archival, and destruction;
- Cryptographic device lifecycle management events; and
- CA system equipment configuration.

GSTUCA issuance system management events including:-

- System start-up and shutdown actions;
- Attempts to create, remove, or set passwords or change the system; and
- Changes to Issuing CA Private Keys.

GSTUCA and Subscriber Certificate lifecycle management events, including:-

- Certificate requests, renewal, and re-key requests, and revocation for both successful and unsuccessful attempts;
- All verification activities stipulated in this CPS;
- Acceptance and rejection of Certificate requests;
- Issuance of Certificates; and
- Generation of Certificate Revocation Lists and OCSP entries including failed read-and-write operations on the Certificate and CRL directory.

Security events, including:-

- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- System crashes, hardware failures, and other anomalies;
- Firewall and router activities; and
- Entries to and exits from the CA facility.

Documentation and Auditing:-

- Audit documentation including all work related communications to or from GSTUCA and compliance auditors;
- Certificate Policy and previous versions;
- Certification Practice Statement and previous versions; and
- Subscriber agreements between Subscribers and GSTUCA

Time stamping:-

- Clock synchronization.

Miscellaneous

- Violations of the CP or this CPS

5.5.2 Retention Period for Archive

The minimum retention period for archive data is 5 years.

5.5.3 Protection of Archive

Archive protections ensure that only authorized trusted access is able to make operations without modifying integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.4 Archive Backup Procedures

Daily backups created using the network backup service provided by Network Infrastructure and Services, a unit of Information Technology, serve as backups for the GSTUCA system.

5.5.5 Requirements for Timestamping of Records

If a timestamping service is used to date the records, then it has to respect with the requirements defined in Section 6.8. Irrespective of timestamping methods, all logs must have data indicating the time at which the event occurred.

5.5.6 Archive Collection System (Internal or External)

The archive collection system complies with the security requirements defined in Section 5.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized GSTUCA equipment, trusted role and other authorized persons are allowed to access the archive. Requests to obtain and verify archive information are co-ordinated by operators in trusted roles.

5.6 Key Changeover

GSTUCA may periodically change over key material for Issuing CAs in accordance with Section 6.3.2. Certificate Subject information may also be modified and Certificate profiles may be altered to adhere to new best practices. Keys used to sign previous Subscriber Certificates are maintained until such time as all Subscriber Certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Virginia Tech establishes business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or Compromise the GSTUCA services. Virginia Tech carries out risk assessments to evaluate business risk and determine the necessary security requirements and operational procedures to be taken as a consequence of its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary *(threat evolution, vulnerability evolution, etc.).* This business continuity is included in the scope of the audit process as described in Section 8 to validate which operations should first be restored after a disaster and the recovery plan.

GSTUCA personnel that serve in a trusted role and operational role are specially trained to operate according to procedures defined in the disaster recovery plan for business critical operations.

If GSTUCA detects a potential hacking attempt or another form of Compromise, it contacts the Information Technology Security Office to perform an investigation in order to determine the nature and the degree of damage. With the Information Technology Security Office, the GSTUCA assesses the scope of potential damage in order to determine whether the CA or RA system needs to be rebuilt, whether only some Certificates need to be revoked, and/or whether a CA hierarchy needs to be declared as Compromised. The CA disaster recovery plan highlights which services should be maintained.

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

If any equipment is damaged or rendered inoperative but the Private Keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate Certificate status information according to GSTUCA's disaster recovery plan.

5.7.3 Entity Private Key Compromise Procedures

In the event a GSTUCA Private Key is Compromised, lost, destroyed or suspected to be Compromised:

- GSTUCA, after investigation of the problem, shall decide if the GSTUCA Certificate should be revoked. If so then:-
    - All the Subscribers who have been issued a Certificate will be notified at the earliest feasible opportunity; and
    - A new GSTUCA Key Pair shall be generated or an alternative existing CA hierarchy shall be used to create new Subscriber Certificates;

5.7.4 Business Continuity Capabilities After a Disaster

The disaster recovery plan deals with the business continuity as described in Section 5.7.1. Certificate status information systems should be deployed so as to provide 24 hours per day, 365 days per year availability (with a rate of 99.95% availability excluding planned maintenance operations).

5.8 GSTUCA Termination

In the event of termination, GSTUCA provides notice to all customers prior to the termination and:

- Stops delivering Certificates according to and referring to this CPS;
- Archives all audit logs and other records prior to termination;
- Destroys all Private Keys upon termination;
- Ensures archive records are transferred to an appropriate authority such as another GSTUCA that delivers identical services; and
- Uses secure means to notify customers and Application Software Suppliers to delete all trust anchors.

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

GSTUCA generates all issuing Key Pairs in a physically secure environment. GSTUCA key generation is carried out within a device which is at least certified to FIPS 140-2 level 3 or above.

6.1.2 Private Key Delivery to Subscriber

The private key is generated by the CA and issued to the subscriber in a password protected PKCS #12 formatted file bundled with its public key. Although it is possible to extract the keys out of the PKCS #12 formatted file, the keys should stay in the file and a password should not be removed from the file.

.

6.1.3 Public Key Delivery to Certificate GSTUCA

GSTUCA only accepts Public Keys from RAs that have been protected during transit and have had the authenticity and integrity of their origin from the RA suitably verified. RA's shall only accept Public Keys from Subscribers in accordance with Section 3.2.3 of this CPS.

6.1.4 CA Public Key Delivery to Relying Parties

GSTUCA relies on the processes of GlobalSign nv-sa (the Root Authority) to deliver Root Certificates to Relying Parties, and upon chain verification mechanisms within the Relying Parties' software platform to establish the chain of trust for the Relying Party.

6.1.5 Key Sizes

GSTUCA follows NIST recommended timelines and best practice in the choice of size of its Key Pairs for Root CAs and Issuing CAs and only signs end entity Certificates following best practices.

The following key sizes and Hashes are used for Root Certificates, Issuing CA Certificates and end entity Certificates and CRL/OCSP Certificate status responders in accordance with the Baseline Requirements:-

- 2048 bit RSA key with Secure Hash Algorithm 1 (SHA-1)
- 2048 bit RSA key with Secure Hash Algorithm 2 (SHA-256)

Where possible, the entire Certificate chain and any Certificate status responses use the same level of security and cryptography. Exceptions due to cross-certified Certificates are acceptable.

Existing Certificates with an unsuitable cryptographic strength are replaced in sufficient time as to protect Relying parties, Subscribers and Issuing CAs.

6.1.6 Public Key Parameters Generation and Quality Checking

GSTUCA generates Key Pairs in accordance with FIPS 186 and uses reasonable techniques to validate the suitability of Public Keys presented by Subscribers. Known weak keys shall be tested for and rejected at the point of submission.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

GSTUCA sets key usage of Certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 v3 (see Section 7.1).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

GSTUCA ensures that all systems signing Certificates and CRLs or generating OCSP responses use FIPS 140-2 level 3 as the minimum level of cryptographic protection.

6.2.2 Private Key (n out of m) Multi-Person Control

GSTUCA activates Private Keys for cryptographic operations with multi-person control (using CA activation data) performing duties associated with their trusted roles. The trusted roles permitted to participate in this Private Key multi-person controls are strongly authenticated (i.e. token with PIN code).

6.2.3 Private Key Escrow

GSTUCA generates and escrows all private keys issued to a Subscriber. The escrowed keys are recoverable by the subscriber and are encrypted in the GSTUCA database by the GSTUCA private key.

Certificates will be retained for 10 years or until the Certificate Authority is phased out, whichever comes first.

6.2.4 Private Key Backup

The encrypted escrowed key is backed up as a part of the regular nightly database backups.

6.2.5 Private Key Archival

GSTUCA archives private keys in the sense that each escrowed key is never deleted.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

GSTUCA Private Keys are generated, activated and stored in Hardware Security Modules. When Private Keys are outside of a Hardware Security Module (either for storage or transfer), they are encrypted. Private Keys never exist in plain text outside of a cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

GSTUCA stores Private Keys on at least a FIPS 140-2 level 3 device.

6.2.8 Method of Activating Private Key

GSTUCA is responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the Hardware Security Module. Subscribers are responsible for protecting Private Keys in accordance with the obligations that are presented in the form of a Subscriber Agreement or Terms of Use.

6.2.9 Method of Deactivating Private Key

GSTUCA ensures that Hardware Security Modules that have been activated are not left unattended or otherwise available to unauthorized access. During the time a GSTUCA's Hardware Security Module is on-line and operational, it is only used to sign Certificates and CRL/OCSPs from an authenticated RA. When a CA is no longer operational, Private Keys are removed from the Hardware Security Module.

6.2.10 Method of Destroying Private Key

GSTUCA Private Keys are destroyed when they are no longer needed or when the Certificates to which they correspond have expired or have been revoked. Destroying Private Keys means that GSTUCA destroys all

associated CA secret activation data in such a manner that no information can be used to deduce any part of the Private Key.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

GSTUCA archives Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

GSTUCA Certificates have a maximum validity period of 2 years. GSTUCA complies with the Baseline Requirements with respect to the maximum Validity Period. In some cases, the maximum Validity Period may not be realized by the Subscriber in the event the current or future Baseline Requirements impose requirements on Certification Authorities relative to Certificate issuance that were not in place at the time the Certificate was originally issued, particularly in the case of a request for reissuance, e.g., additional requirements are included for identification and authentication for certain Certificate type, or maximum Validity Period is decreased.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of GSTUCA activation data used to activate GSTUCA Private Keys are made during a key ceremony (Refer to Section 6.1.1). Activation data is either generated automatically by the appropriate HSM or in such a way that meets the same needs. It is then delivered to a holder of a share of the key who is a person in trusted role. The delivery method maintains the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

Issuing CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. GSTUCA activation data is stored on smart cards.

6.4.3 Other Aspects of Activation Data

GSTUCA activation data may only be held by GSTUCA personnel in trusted roles.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. The GSTUCA PKI components must include the following functions:

- Require authenticated logins for trusted role;
- Provide discretionary access control;
- Provide security audit capability (protected in integrity);
- Prohibit object re-use;
- Require use of cryptography for session communication;
- Require trusted path for identification and authentication;
- Provide domain isolation for process; and
- Provide self-protection for the operating system.

When GSTUCA PKI equipment is hosted on an evaluated platform in support of computer security assurance requirements then the system (hardware, software, operating system), when possible, operates in an elevated configuration. At a minimum, such platforms use the same version of the computer operating system as that which received the evaluation rating. The computer systems are configured with minimum of the required accounts, network services, and no remote login.

6.5.2 Computer Security Rating

All the GSTUCA PKI component software is compliant with the requirements of the protection profile from a suitable entity.

6.6 Lifecycle Technical Controls

6.6.1 System Development Controls

The system development controls for the GSTUCA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology;
- Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
- Hardware and software are developed in a controlled environment, and the development processes are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location;
- The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation;
- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the CA operations installed on the equipment and are obtained from sources authorized by local policy. GSTUCA hardware and software are scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates are purchased or developed in the same manner as original equipment and are installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the GSTUCA system as well as any modifications and upgrades are documented and controlled by the GSTUCA management. There is a mechanism for detecting unauthorized modification to the GSTUCA software or configuration. A formal configuration management methodology is used for installation and on-going maintenance of the GSTUCA system. The GSTUCA software, when first loaded, is checked as being that supplied from the vendor, with no modifications, and is the version intended for use.

6.6.3 Lifecycle Security Controls

GSTUCA maintains a maintenance scheme to ensure the level of trust of software and hardware that are evaluated and certified.

6.7 Network Security Controls

GSTUCA PKI components implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of security guards, firewalls and filtering routers. Unused network ports and services are turned off. Any boundary control devices used to protect the network on which PKI equipment are hosted deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Time Stamping

All GSTUCA components are regularly synchronized with a reliable time service. GSTUCA uses Network Time Protocol to establish the correct time:
• Initial validity time of a CA Certificate;
• Revocation of a CA Certificate;
• Posting of CRL updates;
• Issuance of Subscriber End Entity certificates.
Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

7.0 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

GSTUCA issues Certificates in compliance with X.509 Version 3.

7.1.2 Certificate Extensions

GSTUCA issues Certificates in compliance with RFC 5280 and applicable best practice. Criticality also follows best practice to prevent unnecessary risks to Relying Parties when applied to name constraints.

7.1.3 Algorithm Object Identifiers

GSTUCA issues Certificates with algorithms indicated by the following OIDs
- SHA256WithRSAEncryption {iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}

7.1.4 Name Forms

GSTUCA issues Certificates with name forms compliant to RFC 5280. Within the domain of each Issuing CA, GSTUCA includes a unique non-sequential Certificate serial number that exhibits at least 20 bits of entropy.

7.1.5 Name Constraints

GQSCA complies with the Name Constraint requirements of the GlobalSign Trusted Root program.

7.1.6 Certificate Policy Object Identifier

No stipulation

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

GSTUCA issues Certificates with a policy qualifier and suitable text to aid Relying Parties in determining applicability.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.2 CRL Profile

7.2.1 Version Number(s)

GSTUCA issues Version 2 CRLs in compliance with RFC 5280. CRLs have the following fields:-
- Issuer GSTUCA
- Effective date Date and Time
- Next update Date and Time
- Signature Algorithm sha1RSA
- Signature Hash Algorithm sha1
- Serial Number(s) List of revoked serial numbers
- Revocation Date Date of Revocation

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:
• CRL Number Sequentially assigned natural number
• Authority Key Identifier AKI of the issuing CA for chaining/validation requirements
• Issuing Distribution Point URL of the Certificate Revocation List

7.3 OCSP Profile

GSTUCA operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 2560 or RFC5019 and highlights this within the AIA extension via an OCSP responder URI.

7.3.1 Version Number(s)

GSTUCA issues Version 1 OCSP responses.

7.3.2 OCSP Extensions

No stipulation

8.0 Compliance Audit and Other Assessments

The procedures within this CPS encompass all relevant portions of currently applicable PKI standards. GSTUCA is constrained by GlobalSign nv-sa using dNSNameConstraints and therefore external independent auditing is not applicable.

8.1 Frequency and Circumstances of Assessment

The Certificates issued by GSTUCA are assessed on an annual basis by GlobalSign nv-sa or an affiliated GlobalSign company as part of the contractual obligation in using Trusted Root chaining services. The assessment covers all CA related activities as recommended by the Baseline Requirements.

8.2 Identity/Qualifications of Assessor

GlobalSign nv-sa or an affiliated GlobalSign company determines through an annual assessment that the provisions of the contract and adherence to the Baseline Requirements are maintained using suitably qualified and trained GlobalSign staff members.

8.3 Assessor's Relationship to Assessed Entity

GSTUCA is a cross-signed entity under contract with GlobalSign nv-sa or an affiliated company under the Trusted Root program.

8.4 Topics Covered by Assessment

The audit meets the requirements of the Baseline Requirements.

8.5 Actions Taken as a Result of Deficiency

GSTUCA follows the same process if presented with a material non-compliance by GlobalSign nv-sa or an affiliated company. GSTUCA creates a suitable corrective action plan to remove the deficiency. Corrective action plans which directly affect policy and procedure as dictated by GlobalSign's CP and this CPS are referred to the GlobalSign Policy Authority for discussion and resolution.

Communications of Results
Results of the audit are reported to GSTUCA for analysis and resolution of any deficiency through a subsequent corrective action plan.

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

GSTUCA may charge fees for Certificate issuance.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Customer shall maintain the following insurance, which may be through a self-insurance policy, related to their respective performance and obligations:

- Commercial General Liability insurance (occurrence form) with policy limits of at least 1 million US dollars in coverage; and

- Professional Liability/Errors and Omissions insurance, with policy limits of at least 1 million US dollars in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing digital Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following items are classified as being confidential information and therefore are subject to reasonable care and attention by GSTUCA staff including vetting agents and administrators.

- Personal information as detailed in Section 9.4;
- Audit logs from CA and RA systems;
- Activation data used to active CA Private Keys as detailed in Section 6.4;
- Internal GlobalSign business process documentation including Disaster Recovery Plans (DRP) and Business Continuity Plans (BCP); and
- Audit reports from an independent auditor as detailed in Section 8.0.

9.3.2 Information Not Within the Scope of Confidential Information

Any information not defined as confidential within this CPS shall be deemed public. Certificate status information is deemed public.

9.3.3 Responsibility to Protect Confidential Information

GSTUCA protects confidential information through training and enforcement with employees, agents and contractors.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

GSTUCA protects personal information through internal policy in accordance with legal requirements where GSTUCA operates.

9.4.2 Information Treated as Private

GSTUCA treats all information received from Applicants that will not ordinarily be placed into a Certificate as private. This applies both to those Applicants who are successful in being issued a Certificate and those who are unsuccessful and rejected. GSTUCA periodically trains all RA and vetting staff as well as anyone who has access to the information about due care and attention that must be applied.

9.4.3 Information Not Deemed Private

Certificate status information and any Certificate content is deemed not private.

9.4.4 Responsibility to Protect Private Information

GSTUCA protects personal information in accordance with legal requirements where GSTUCA operates.

9.4.5 Notice and Consent to Use Private Information

Personal Information obtained from Applicants during the application and enrollment process is deemed private and permission is required from the Applicant to allow the use of such information. GSTUCA includes any required consents in the Subscriber Agreement including any permission required for additional information to be obtained from third parties that may be applicable to the validation process for the product or service being offered by GSTUCA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

GSTUCA may disclose private information without notice to Applicants or Subscribers where required to do so by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property rights

GSTUCA does not knowingly violate the intellectual property rights of third parties. Public and Private Keys remain the property of Subscribers who legitimately hold them. GSTUCA retains ownership of Certificates; however, it grants permission to reproduce and distribute Certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

GlobalSign and the GlobalSign logo are the registered trademarks of GMO GlobalSign K.K.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

GSTUCA uses this CPS and applicable Subscriber Agreements to convey legal conditions of usage of issued Certificates to Subscribers and Relying Parties. All parties warrant the integrity of their respective Private Key(s).

GSTUCA represents and warrants to Certificate Beneficiaries that, during the period when the Certificate is valid, GSTUCA has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate - including:

- **Right to Use Domain Name or IP Address**: That, at the time of issuance, GSTUCA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's Subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GSTUCA's Certificate Policy and/or Certification Practice Statement (see Section 3.2);
- **Authorization for Certificate:** That, at the time of issuance, GSTUCA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GSTUCA's Certificate Policy and/or Certification Practice Statement (see Section 3.2.5);
- **Accuracy of Information:** That, at the time of issuance, GSTUCA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GSTUCA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **No Misleading Information:** That, at the time of issuance, GSTUCA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GSTUCA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in GSTUCA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.3, 3.2.3, 3.2.4);
- **Subscriber Agreement:** That GSTUCA and Subscriber are affiliated; therefore, the Applicant Representative acknowledged and accepted the Terms of Use (see Section 4.5.1);
- **Status:** That GSTUCA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- **Revocation:** That GSTUCA will revoke the Certificate for any of the reasons specified in the CABForum Baseline Requirements (see Section 4.9.1).

9.6.2 RA Representations and Warranties

RAs warrant that:-

- Issuance processes are in compliance with this CPS and the relevant GlobalSign CP;
- All information provided to GSTUCA does not contain any misleading or false information; and
- All translated material provided by the RA is accurate.

9.6.3 Subscriber Representations and Warranties

- Unless otherwise stated in the CPS, Subscribers are responsible for:
- Having knowledge and, if necessary, seeking training on using digital certificates.

- Generating securely their private-public key pair, using a trustworthy system.
- Providing correct and accurate information in their communications with GQSCA.
- Ensuring that the public key submitted to the GQSCA correctly corresponds to the private key used.
- Accepting the Terms of Use, GlobalSign CP and associated policies published in the GQSCA repository.
- Refraining from tampering with an issued certificate.
- Using certificates only for legal and authorized purposes in accordance with this CPS.
- Notifying the GQSCA or RA of any changes in the information submitted.
- Ceasing to use a certificate if any featured information becomes invalid.
- Ceasing to use a certificate when it becomes invalid.
- Removing a certificate when invalid from any applications and/or devices on which they have been installed.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorized use of their private key.
- For any acts and omissions of partners and agents subscribers use to generate, retain, escrow, or destroy any private keys.
- Refraining from submitting any material that contains statements that violate any law or the rights of any party.
- Requesting the revocation of a certificate in case of an occurrence that materially affects the integrity of a certificate.
- Notifying the appropriate RA immediately, if a Subscriber becomes aware of or suspects the compromise of a private key.
- Submit accurate and complete information to GQSCA in accordance with the requirements of this CPS particularly with regards to registration.
- Only use the key pair in accordance with any other limitations notified to the Subscriber according to this CPS or any Trusted Root CA Chaining agreement.
- Exercise absolute care to avoid unauthorized use of its private key.
- Use a key length and algorithm as indicated in this CPS.
- Notify GQSCAs without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
    - The Subscriber's private key has been lost, stolen, potentially compromised; or
    - Control over the Subscribers private key has been lost due compromise of activation data (e.g. PIN code or Pass Phrase) or
    - Inaccuracy or changes to the certificate content, as notified to the Subscriber.

The Subscriber is ultimately liable for the choices he or she makes when applying for a certificate. The applicant and GQSCA must designate the usage of a trustworthy device as well as the choice of organizational context.

9.6.4 Relying Party Representations and Warranties

A party relying on a GSTUCA's Certificate warrants to:

- Have the technical capability to use digital certificates;
- Receive notice of the GSTUCA and associated conditions for Relying Parties;
- Validate a GSTUCA's Certificate by using Certificate status information (e.g. a CRL or OCSP) published by the GSTUCA in accordance with the proper Certificate path validation procedure;
- Trust a GSTUCA's Certificate only if all information featured on such Certificate can be verified via such a validation procedure as being correct and up to date;
- Rely on a GSTUCA's Certificate, only as it may be reasonable under the circumstances; and
- Notify the appropriate RA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised.

The obligations of the Relying Party, if it is to reasonably rely on a Certificate, are to:

- Verify the validity or revocation of the CA Certificate using current revocation status information as indicated to the Relying Party;
- Take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or this CPS; and
- Take any other precautions prescribed in the GSTUCA's Certificate as well as any other policies or terms and conditions made available in the application context a Certificate might be used.

Relying Parties must at all times establish that it is reasonable to rely on a Certificate under the circumstances taking into account circumstances such as the specific application context a Certificate is used in.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

GSTUCA does not warrant that:

- The accuracy of any unverifiable piece of information contained in certificates except as it may be stated in the relevant product description below in this CPS and in a Warranty Policy, if available.
- The accuracy, authenticity, completeness or fitness of any information contained in, free, test or demo certificates.

9.8 Limitations of Liability

IN NO EVENT SHALL GQSCA BE LIABLE FOR ANY INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR FOR ANY LOSS OF PROFITS, LOSS OF DATA OR OTHER INDIRECT, INCIDENTAL, CONSEQUENTIAL 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.

9.9 Indemnities

9.9.1 Indemnification by GSTUCA

No stipulation.

9.9.2 Indemnification by Subscribers

No stipulation.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify GSTUCA, GlobalSign nv-sa and any related entity providing services to GSTUCA, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End User License Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10 Term and Termination

9.10.1 Term

This CPS remains in force until such time as communicated otherwise by GSTUCA on its web site or Repository.

9.10.2 Termination

Notified changes are appropriately marked by an indicated version. Following publication, changes become applicable 30 days thereafter.

9.10.3 Effect of Termination and Survival

GSTUCA will communicate the conditions and effect of this CPS termination via the appropriate Repository.

9.11 Individual Notices and Communications with Participants

GSTUCA notifies subscriber representatives via email prior to certificate expiration with sufficient notice to allow for continuity of service.

9.12 Amendments

9.12.1 Procedure for Amendment

Changes to this CPS are indicated by appropriate numbering. The GSTUCA complies with procedures of the VTPKI PMA published at www.pki.vt.edu.

9.12.2 Notification Mechanism and Period

GSTUCA will post appropriate notice on www.pki.vt.edu of any major or significant changes to this CPS as well as any appropriate period by when the revised CPS is deemed to be accepted.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation

9.13 Dispute Resolution Provisions

GSTUCA complies with the procedures of the VTPKI PMA published at www.pki.vt.edu/rootca/pma/index.html.

9.14 Governing Law

This CPS is governed, construed and interpreted in accordance with the laws of the Commonwealth of Virginia.

9.15 Compliance with Applicable Law

GSTUCA complies with applicable laws of the Commonwealth of Virginia. Export of certain types of software used in certain GSTUCA public Certificate management products and services may require the approval of appropriate public or private authorities. Parties (including GSTUCA, Subscribers and Relying Parties) agree to conform to applicable export laws and regulations as pertaining to the United States.

9.16 Miscellaneous Provisions

9.16.1 Compelled Attacks

GSTUCA is subject to the Commonwealth of Virginia jurisdiction and regulatory framework. GSTUCA will use all reasonable legal defense against being compelled by a third party to issue Certificates in violation of this CPS.

9.16.2 Survival

The obligations and restrictions contained under section “Legal Conditions” survive the termination of this CPS.

9.16.3 Entire Agreement

GSTUCA will contractually obligate every RA involved with Certificate issuance to comply with this CPS and all applicable industry guidelines. No third party may rely on or bring action to enforce any such agreement.

9.16.4 Assignment

Entities operating under this CPS cannot assign their rights or obligations without the prior written consent of GSTUCA

9.16.5 Severability

If any provision of this CPS, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CPS will be interpreted in such manner as to effect the original intention of the parties.

9.16.6 Enforcement

GSTUCA’s failure to enforce a provision of this CPS does not waive GQSCA’s right to enforce the same provisions later or right to enforce any other provisions of this CPS.

9.17 Other Provisions

No Stipulation