VirginiaTech
Invent the Future®

Virginia Tech Global Qualified Server Certification Authority Certification Practice Statement

Identification: Virginia Polytechnic Institute and State University; VPI&SU; Virginia Tech
Data Universal Number System: 003137015

Object Identifier: 1.3.6.1.4.1.6760.5.2.3.5.1

Date: August 20, 2015

Version: 0.10

Table of Contents

Document History

Version	Release Date	Author	Status + Description
0.10	8/20/2015	VTPKI PMA	Draft

Detailed History of Changes

Changes in version 0.10 (publication date: 8/20/2015) with respect to new SHA-256 CA

- **1.0 Introduction** – Change to version 1.3.0 of the Baseline Requirements
- **1.1.1 Certificate Naming** – Add the new SHA-256 Virginia Tech Global Qualified Server CA serial number
- **6.1.5 Key Sizes** – Add SHA-256
- **7.1.3 Algorithm Object Identifiers** – Add SHA256WithRSAEncryption

Changes in xxxx (publication date : xxxx) with respect to xxxx

- Details

Acknowledgments

This Virginia Tech Global Qualified Server CA CPS endorses in whole or in part the following industry standards:

- ETSI TS 102 042 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- ISO 21188:2006, Public key infrastructure for financial services -- Practices and policy framework.
- RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.
- WebTrust, WebTrust Program for Certification Authorities Version 2.0, AICPA/CICA, available at http://www.webtrust.org/homepage-documents/item49945.aspxRFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.
- RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.
- RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers, et al, June 1999.
- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
- RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.
- RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.
- RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.ETSI TS 101 042: Policy requirements for certification authorities issuing public key certificates (Normalised level only).
- The ISO 1-7799 standard on security and infrastructure
- FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.
- X509v3, ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

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.
- CABForum 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 the Virginia Tech Global Qualified Server Certification Authority (hereinafter referred to as the GQSCA) applies to the products and services of the Virginia Polytechnic Institute and State University (“Virginia Tech”), including the GQSCA. Primarily this pertains to the issuance and lifecycle management of Digital 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 policy according to the structure of RFC 3647, the topic may not necessarily apply to Services of Virginia Tech Global Qualified Server CA. These sections have *‘No stipulation’* appended. 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 on the 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 GQSCA during the complete life cycle of certificates issued by the GQSCA.

The GQSCA operates within the scope of activities of Virginia Tech and its affiliates. This CPS addresses the requirements of the CA that issues certificates of various types under the Certificate Policy of GlobalSign nv-sa and its TrustedRoot 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.

The GQSCA conforms to version 1.3.0 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document to the extent allowable by law.

For Subscribers this CPS becomes effective and binding by accepting a Subscriber Agreement or Terms of Use Agreement. For Relying Parties this CPS becomes binding by relying upon a certificate issued under this CPS. In addition, Subscribers are bound 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 GQSCA. 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 digital certificates according to GQSCA’s own and industry requirements pursuant to the standards set out above. This CPS aims at facilitating the GQSCA in delivering certification services and managing the certificate lifecycle of and issued client, server and other-purpose end entity certificates. The certificate types addressed in this CPS are the following:

SSL/TLS	A certificate to authenticate web servers

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

GQSCA certificates:

- Can be used to authenticate web resources, such as servers and other devices.

This CPS identifies the roles, responsibilities and practices of all entities involved in the life cycle, use, reliance upon and management of GQSCA certificates. The provisions of this CPS with regard to practices, level of services, responsibilities and liability bind all parties involved, including GQSCA, 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 aligning to 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 GQSCA uses in creating and maintaining the certificates that it manages. In addition to this CPS GQSCA maintains a range of adjacent documented polices which include but are not limited to addressing such issues as:

- Business Continuity and Disaster Recovery
- Security Policy
- Personnel Policies
- Key management Policies
- Registration Procedures

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

A subscriber or relying party of a certificate must refer to this CPS in order to establish trust in a certificate issued by GQSCA as well as for notices with regard to the prevailing practices thereof. It is also essential to establish the trustworthiness of the entire certificate chain of the hierarchy. This includes the Root CA as well as any operational certificates. This can be established on the basis of the assertions within this CPS.

1.1.1 Certificate Naming

The exact names of the GQSCA certificates that make use of this CPS are:

- Virginia Tech Global Qualified Server CA with serial number 22:AA:72:7F:F6:28:1A:0B:C7:73:C1:E2:0C:0C:40:23:CA
- Virginia Tech Global Qualified Server CA with serial number 45:E6:BB:58:86:C0:8C:6E:93:DF:13:EA:C8:88

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

1.2 Document Name and Identification

This document is the Virginia Tech Global Qualified Server Certification Authority Certification Practice Statement.

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

1.3.6.1.4.1.6760.5.2.3.5.1	SSL/TLS Policy

The OID for GlobalSign nv-sa (GlobalSign CA) is a 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 (Which may be updated from time to time) as follows:

1.3.6.1.4.1.4146.1.60	CA Chaining Policy – TrustedRoot™

In addition to these identifiers, all certificates that comply with the CABForum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates will include the additional identifiers as follows:

2.23.140.1.2.2	Organization Validation Certificates Policy

1.3 PKI participants

The GQSCA does not issue a PKC to any entity that is not within the scope of Virginia Tech or its affiliated entities

1.3.1 Certification Authorities

GQSCA is a Certification Authority (CA) that issues high quality and highly trusted certificates in accordance with this CPS. As a Certification Authority, GQSCA performs functions related to PKI certificate life cycle management such as subscriber registration, certificate issuance, certificate renewal, certificate distribution and certificate revocation. GQSCA also provides Certificate status information using an online repository in the form of a CRL (Certificate Revocation List) distribution point and/or OCSP (Online Certificate Status Protocol) responder.

GQSCA 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 GQSCA does not have the authority to issue subordinate CA PKCs.

1.3.2 Registration Authorities

A Registration Authority (RA) is an entity that identifies and authenticates applicants for certificates. An RA may also initiate or pass along revocation requests for certificates and requests for re-issuance and renewal (sometimes referred to as rekey) of certificates. Virginia Tech Identity Management Services (IMS) will act as a Registration Authority for certificates the GQSCA issues. IMS is responsible for:

- Accepting, evaluating, approving or rejecting the registration of certificate applications.
- Registering subscribers for certification services.
- Providing systems to facilitate the identification of subscribers (according to the type of certificate requested).
- Using officially notarized or otherwise authorized documents or sources of information to evaluate and authenticate a subscriber’s application.
- Following approval of an application requesting issuance of a certificate via a multifactor authentication process.
- Initiating the process to revoke a certificate from the applicable GlobalSign subordinate issuing CA.

1.3.3 Subscribers

Subscribers to GQSCA are either legal entities or natural persons that successfully apply for and receive a certificate to support their use in transactions, communications and the application of digital signatures.
The *Subject* of a certificate is the party named in the certificate. A *Subscriber*, as used herein, refers to both the subject of the certificate and the entity that contracted with the GQSCA 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 on the online process for the application for a certificate.

1.3.4 Relying Parties

Relying parties are natural persons or legal entities that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber’s certificate.

To verify the validity of a digital certificate, relying parties must always refer to GQSCA’s revocation information either in the form of a Certificate Revocation List (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 GQSCA.

1.3.5 Other Participants

GQSCA is cross signed by GlobalSign nv-sa via its TrustedRoot Program as detailed within the GlobalSign CP on https://www.globalsign.com/respository.

1.4 Certificate Usage

A digital certificate is a specifically formatted data object that cryptographically binds an identified subscriber with a Public Key (supporting either RSA or ECC). A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital 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 GQSCA 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.
- **Confidentiality:** The assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended.
- **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.

Authentication (Devices and objects): Device authentication certificates can be used for specific electronic authentication transactions that support the identifying of web sites and other on line resources, such as software objects etc. The authentication function of a digital certificate can be ascertained in any transaction context with the purpose of authenticating a device that the subscriber seeks to secure through a digital certificate. To describe the function of authentication, the term digital signature is often used.

- SSL/TLS: authentication of a remote domain name and associated organizational context and webservice and encryption of the communication channel

- **Assurance levels:** Subscribers should choose an appropriate level of assurance to which relying parties will confidently transact.

Assurance Level OID	Applicability
Test 1.3.6.1.4.1.6760.5.2.2.1.1	This level is not currently used.
Rudimentary 1.3.6.1.4.1.6760.5.2.2.2.1	This level is not currently used.
Basic 1.3.6.1.4.1.6760.5.2.2.3.1	This level provides a sufficient level of assurance relevant to production environments where there are risks and consequences of data compromise. PKCs issued at this assurance level require the approval and signature of the subscriber's dean, director, department head, or designee. This guarantees that the subject entry named in the PKC is a member of the SCA communities.
Medium 1.3.6.1.4.1.6760.5.2.2.4.1	This level is reserved for future use when stricter identity verification mechanisms are available and in use.
High 1.3.6.1.4.1.6760.5.2.2.5.1	This level is reserved for future use when stricter identity verification mechanisms are available and in use.

Confidentiality: All certificate types can be used to ensure the confidentiality of communications effected by means of digital certificates. Confidentiality may apply to business and personal communications as well as personal data protection and privacy.

Any other use of a digital certificate is not supported by this CPS. When using a digital certificate the functions of electronic signature (non repudiation) and authentication (digital signature) 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;
- where prohibited by law.

1.4.2.1 Certificate extensions

Certificate extensions comply to X.509 v.3 standards. EKU = Enhanced or Extended Key usage

• SSL/TLS:	Client and Server Authentication EKU

1.4.2.2 Critical Extensions

GQSCA 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.
- To show the number of levels in the hierarchy under a CA certificate.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

Identity Management Services

1.5.2 Contact Person

Director, Identity Management Services
Virginia Tech
1700 Pratt Drive
Blacksburg, VA 24061

1.5.3 Person Determining CPS Suitability for the Policy

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

Chair, VTPKI PMA
Virginia Tech
314 Burruss Hall
Blacksburg, VA 24061

1.5.4 CPS Approval Procedures

The GQSCA 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 duty 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 Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

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 the Acknowledgements.

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.

Certificate: An electronic document that uses a digital signature to bind a public key and an identity.

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 time-stamped 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.

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).

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.

HSM: Hardware Security Module: A 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.

Independent Audit: An audit that is performed by a Qualified Auditor and that determines an entity’s compliance with these Requirements and one or more of the audit schemes listed in the Acknowledgements.

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: 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: 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 17.6 (Auditor Qualifications).

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

Registration Authority: 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.

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 or Terms of Use Agreement.

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

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

Trusted Platform Module: 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 these 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 digital 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
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
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RAA	Registration Authority Administrator
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

GQSCA publishes all CA certificates revocation data for issued certificates, CPS, and any Relying Party Agreements or Subscriber Agreements in online repositories. GQSCA 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 down-time that does not exceed 0.5% annually.

GQSCA may publish submitted information on publicly accessible directories for the provision of certificate status information.

GQSCA refrains from making publicly available certain elements of documentation including security controls, procedures, internal security polices etc. However elements may be disclosed in audits associated with formal accreditation schemes such as WebTrust 2.0.

2.2 Publication of Certificate Information

GQSCA publishes its CPS, Subscriber Agreements, Relying Party Agreements on the following URL http://www.pki.vt.edu. CRLs are published in online repositories. The CRLs contain entries for all revoked un-expired certificates and are valid, depending on certificate type.

2.3 Time or Frequency of Publication

CRLs for end-user certificates are issued at least every 24 hours. Each CRL includes a monotonically increasing sequence number for each CRL issued.

New or modified versions of this CPS, Subscriber Agreements, or Relying Party Warranties are published within seven days of approval by the VTPKI PMA.

2.4 Access control on repositories

Access to repositories is limited to Certification Authority Administrators (CAA) appointed by the Office of the Vice President for Information Technology.

3.0 Identification and Authentication

Virginia Tech operates an RA that verifies and authenticates the identity and/or other attributes of an applicant applying for a certificate and that the Applicant is associated with either Virginia Tech or one of its affiliated entities.

Certificate 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

GQSCA 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.

Non wildcard SSL Certificates are issued with a Fully Qualified Domain Name (FQDN) name.

Wildcard SSL Certificates include a wildcard asterisk character. Before issuing a certificate with a wildcard character (*) GQSCA follows best practices to determine if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix”. (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation.) and if it does, it will reject the request as the domain space must be owned or controlled by the subscriber. e.g. *.globalsign.com.

In the case of SSL certificates, while the FQDN or authenticated domain name is placed in the Common Name (CN) attribute of the Subject field, it may also be duplicated into the Subject Alternative Name extension along with a www version of the DNS-ID. Subject Alternative Names are marked non-critical in line with RFC5280.

3.1.2 Need for Names to be Meaningful

Where possible, GQSCA uses distinguished names to identify both the subject and the Issuing CA of a certificate. In cases where a GQSCA product allows the use of role or departmental name then additional unique elements may be added to the DN within the OU field to allow differentiation by relying parties.

3.1.3 Anonymity or Pseudonymity of Subscribers

GQSCA 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. GQSCA reserves the right to disclose the identity of the subscriber if required by law or following a reasoned and legitimate request.

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

GQSCA enforces the uniqueness of each subject name in a certificate as follows:

• SSL/TLS:	A domain name within the Common Name attribute as approved as unique by ICANN, the Internet Corporation for Assigned names and Numbers.

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. Unless otherwise specifically stated, GQSCA does not require that an Applicant’s right to use a trademark be verified. GQSCA has the right to revoke any certificate that is part of a dispute.

3.2 Initial Identity Validation

GQSCA may perform identification of the applicant for a certificate using any legal means of communication or investigation necessary to identify the legal person or individual.

3.2.1 Method to Prove Possession of Private Key

Subscribers must prove possession of the private key corresponding to the public key being registered either as a CSR (Certificate Signing Request) in PKCS#10 format.

3.2.2 Authentication of Organization Identity

No stipulation.

3.2.2.1 Role Based Certificate Authentication

No stipulation.

3.2.3 Authentication of Individual identity

Identity Management Services Requirements

Initial registration requires:

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

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

3.2.4 Non Verified Subscriber Information

GQSCA validates all information to be included within the Subject DN of a certificate.

3.2.5 Validation of Authority

- **SSL/TLS** Verification through a reliable means of communication with the organization or individual applicant together with verification that the applicant has ownership or control of the domain name by either a challenge response mechanism or direct confirmation with the contact listed with the Domain Name Registrar or WHOIS. Domain names are constrained by the list of DNS name listed within the Name Constraints attribute of the GQSCA certificate.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

No stipulation.

3.3.1 Identification and Authentication for Re-key After Revocation

No stipulation

3.4 Identification and Authentication for Revocation Request

The GQSCA will accept an authorized revocation request sent as an email which specifies the certificate common name and serial number of the PKC to be revoked. In addition, the reason for revocation must be explained**.** IMS will confirm the identity of the applicant sending the revocation request.

4.0 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

GQSCA maintains its own whitelists of individuals from whom and entities from which it will accept certificate applications.
GQSCA does not issue certificates to entities that reside in countries where the laws of a GQSCA office location prohibit doing business.

Applications are accepted as follows:

- **On-line:** Via a web interface over a https session. A certificate applicant must submit an application via a secure ordering process according to a procedure maintained by GQSCA.

4.1.2 Enrollment Process and Responsibilities

GQSCA maintains systems and processes that sufficiently authenticate the applicants identity for all certificate types that present the identity to relying parties. Applicants must submit sufficient information to allow GQSCA's RA to successfully perform the required verification. GQSCA shall protect all communications and securely store all 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 keys 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 applicable Terms and Conditions.
- Paying any Applicable Fees.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

GQSCA maintains systems and processes that sufficiently authenticate the applicants identity in line with the applicable statements made in this CPS. Initial identity vetting will be performed by GQSCA in line with section 3.2.

4.2.2 Approval or Rejection of Certificate Applications

GQSCA shall reject requests for certificates where validation of all items cannot successfully be completed. GQSCA may also reject requests based on potential brand damage to GQSCA in accepting the request. GQSCA may also reject requests for certificates from applicants who have previously been rejected or have previously violated a stipulation within their Subscriber Agreement or Terms of Use Agreement.

Assuming all validation steps can be completed successfully following the procedures within this CPS then GQSCA shall approve the certificate request.

GQSCA is under no obligation to provide a reason to an applicant on why a request has been rejected.

4.2.3 Time to Process Certificate Applications

GQSCA shall ensure that all reasonable methods are used in order to evaluate and process certificate applications. Where issues occur which are outside of the control of GQSCA, then GQSCA shall strive to keep the applicant duly informed.

The following approximations are given for processing and issuance.

- **SSL/TLS -** Approximately 2 business days.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

GQSCA shall ensure it communicates with any RA accounts capable of causing certificate issuance using multifactor authentication. This includes RAs directly operated by GQSCA or RAs contracted by GQSCA. RAs shall perform validation of all information sent to the CA and ensure that any database used to store any information is suitably protected from unauthorized modification or tampering.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

GQSCA shall inform the subscriber of the issuance of a certificate to an e-mail address which was supplied by the subscriber during the enrollment process or by any other equivalent method. The e-mail may contain the certificate itself or a link to download depending upon the workflow of the certificate requested.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Digital Certificate is deemed accepted upon issuance.

4.4.2 Publication of the Certificate by the CA

GQSCA publishes the certificate by delivering it to the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs, Local RA or partners/resellers or GQSCA may be informed of the issuance if they were involved in the initial enrollment.

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. GQSCA provides a suitable Subscriber Terms of Use 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 digital certificate. Where it is possible to make a back-up of a private key, Subscribers must use the same level of care and protection attributed to the live private key. At the end of the useful life of a Key, Subscribers must securely delete the key and any fragments that it has been split into for the purposes of backup.

4.5.2 Relying Party Public Key and Certificate Usage

Within this CPS GQSCA provides the conditions under which digital certificates may be relied upon by relying parties, including the appropriate certificate services to verify certificate validity, such as CRL and/or OCSP. GQSCA provides a Relying Party agreement to Subscribers the content of which should be presented to the Relying Party prior to reliance upon a digital certificate from the GQSCA. 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

Subscribers may renew certificates issued by the GQSCA by submitting a CSR using the existing private/public key pair of the certificate to be renewed.

4.6.2 Who May Request Renewal

As per 4.1

4.6.3 Processing Certificate Renewal Requests

As per 4.2

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As per 4.4.3

4.7 Certificate Re-Key

4.7.1 Circumstances for Re-Key

GQSCA PKCs can be rekeyed. Rekeying a PKC means that a new PKC is created that has the same characteristics and level of assurance as the old one, except that the new PKC has a new, different public key (corresponding to a new, different private key), and a different serial number.

4.7.2 Who May Request Certification of a New Public Key

As per 4.1

4.7.3 Processing Certificate Re-Keying Requests

As per 4.2

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

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 the details which differ from a previously issued certificate. The new modified certificate may or may not have a new public key and may or may not have a new ‘Not After’ date.

- GQSCA treats Modification the same as ‘New’ issuance.

4.8.2 Who May Request Certificate Modification

As per 4.1

4.8.3 Processing Certificate Modification Requests

As per 4.2

4.8.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

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

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 CRL (Certificate Revocation List). The CRL itself will then be digitally signed with the same key material, which originally signed the certificate to be revoked. Adding a serial number allows relying parties to establish that the lifecycle of a digital certificate has ended. GQSCA may remove serial numbers when revoked certificates pass their expiration date to promote more efficient CRL file size management. Prior to performing a revocation GQSCA will verify the authenticity of the revocation request. Revocation may be performed under the following circumstances:

- The Subscriber requests revocation through an authenticated request to GQSCA's Support team or GQSCA's Registration Authority,
- GQSCA obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has been compromised, created using a weak algorithm, or that the Digital Certificate has otherwise been misused,
- GQSCA receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement or Terms of Use Agreement,
- GQSCA receives notice or otherwise becomes aware that a Subscriber uses the certificate for criminal activities such as phishing attacks, fraud, certifying or signing malware etc.,
- GQSCA receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use any of the elements within the 'Subject' or 'Subject Alternative Name' of the Digital Certificate, or that the Subscriber has failed to renew or maintain control of any of those elements,
- GQSCA receives notice or otherwise becomes aware of a material change in the information contained in the Digital Certificate,
- A determination, in GQSCA's sole discretion, that the Digital Certificate was not issued according to best practice or any of GQSCA's own published policies,
- If GQSCA determines that any of the information appearing in the Digital Certificate is not accurate,
- GQSCA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Digital Certificate,
- GQSCA's right to issue Digital Certificates expires or is revoked or terminated,
- GQSCA's Private Key for the relevant issuing CA Certificate is compromised,
- GQSCA receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of GQSCA's jurisdiction of operation,
- The continued use of the certificate is harmful to the business of GQSCA and relying parties,
- The subscriber suspects the loss of a pass phrase to any hardware token which therefore leads to the loss of control of the private key on the token,
- Any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of the certificate or the GQSCA.

When considering whether certificate usage is harmful to GQSCA then GQSCA considers, among other things, the following:

- The nature and number of complaints received,
- The identity of the complainant(s),
- Relevant legislation in force, and
- Responses to the alleged harmful use from the Subscriber.

4.9.2 Who Can Request Revocation

GQSCA and RAs shall accept authenticated requests for revocation. GQSCA may also at its own discretion revoke certificates.

Certificate Revocation Requests are accepted from:

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

4.9.3 Procedure for Revocation Request

A Certificate Revocation Request (CRR) is initiated through:

- An eligible requestor sends an email to IMScerts@vt.edu. The requestor will include the certificate common name and serial number in the revocation request.

- The GQSCA RAA will review the CRR. Upon validation, the certificate will be revoked within the parameters set in 4.9.7 and 4.9.12.

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

No stipulation

4.9.5 Time Within Which CA Must Process the Revocation Request

GQSCA will begin investigation procedures for a suspected key compromise or misuse of a certificate within one business day after receipt of the report.

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 as well as ensuring 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). GQSCA will include all applicable URIs within the certificate to aid relying parties perform the revocation checking process such as:

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

4.9.7 CRL Issuance Frequency

The GQSCA revocation list is published at least once a day.

4.9.8 Maximum Latency for CRLs

GQSCA ensures that online CA CRLs are published daily.

4.9.9 On-Line Revocation/Status Checking Availability

GQSCA 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

GQSCA 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 GQSCA at its own discretion decides that evidence suggests a possible key compromise has taken place. Where key compromise is not disputed, GQSCA shall revoke Subscriber End Entity certificates within 24 hours and publish online an updated CRL within 60 minutes of the update.

4.9.13 Circumstances for Suspension

GQSCA 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

GQSCA 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 Digital Certificate and may refer to any of the following URLs

- http://crl.globalsign.com/gs/
- http://ocsp2.globalsign.com

- http://www.pki.vt.edu/globalqualifiedserver/crl/cacrl.crl
- http://vtca-p.eprov.seti.vt.edu:8080/ejbca/publicweb/status/ocsp

4.10.2 Service Availability

GQSCA 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

CA private keys are never escrowed. GQSCA does not offer Key Escrow Services to Subscribers.

4.11.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5.0 Facility, Management, and Operational Controls

5.1 Physical Controls

GQSCA 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, etc.

5.1.1 Site Location and Construction

GQSCA 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

GQSCA ensures that the facilities used for certificate life cycle 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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

5.1.6 Media Storage

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

5.1.7 Waste Disposal

GQSCA 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

GQSCA 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.

5.2 Procedural Controls

5.2.1 Trusted Roles

GQSCA ensures that all operators and administrators including vetting agents are acting in the capacity of a Trusted Role. Trusted Roles are such that no conflict of interest is possible and the roles are distributed such that no single person can circumvent the security of the CA system.

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 IMS. The RAA’s responsibilities are:

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

5.2.2 Number of Persons Required per Task

GQSCA requires at least 2 people for key generation and certificate generation. The goal is to guarantee the trust for these CA services so that any malicious activity would require collusion. Revocation only requires a single RAA. All participants shall serve in a Trusted Role as defined in section 5.2.1 above.

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a Trusted Role, Virginia Tech 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

GQSCA enforces role separation either by the CA equipment or procedurally or by both means.
Individual CA personnel are specifically designated to the roles defined in section 5.2.1 above. It is forbidden to own at the same time the following roles:

- CAA and RAA

No individual shall be assigned more than one identity.

5.3 Personnel Controls

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

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

5.3.1 Qualifications, Experience, and Clearance Requirements

Virginia Tech 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. GQSCA personnel fulfill 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 5.2.1 are documented in job descriptions. GQSCA 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. GQSCA 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 GQSCA personnel in Trusted Roles are free from conflicting interests that might prejudice the impartiality of the CA operations. GQSCA does not appoint to a Trusted Roles or management any person who is known to have a conviction for a serious crime or another offence, which affects his/her suitability for the position. Personnel do not have access to the trusted functions until any necessary checks are completed. GQSCA requires candidates to provide past convictions and turns down an application in case of refusal. All persons filling Trusted Roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

5.3.3 Training Requirements

GQSCA 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;
- Disaster recovery and business continuity procedures.

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

5.3.4 Retraining Frequency and Requirements

Individuals responsible for Trusted Roles are aware of changes in the GQSCA 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

GQSCA 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 GQSCA operations are subjected to the same process, procedures, assessment, security controls and training as permanent CA personnel.

5.3.8 Documentation Supplied to Personnel

GQSCA 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.

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 collected. 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.
GQSCA ensures all events relating to the life cycle 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,

5.4.2 Frequency of Processing Log

Audit logs are reviewed periodically and reasonably 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 providing 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.

The GQSCA retains audit logs for at least one year.

5.4.4 Protection of Audit Log

The events are logged in a manner to ensure that only authorized trusted access is 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 in 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 realization.

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, 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 invoked 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 then GQSCA determines whether to suspend GQSCA operations until the problem is solved, duly informing the impacted asset owners.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

GQSCA performs regular vulnerability assessments covering all GQSCA 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:

GQSCA key lifecycle management events, including:

- Key generation, backup, storage, recovery, archival, and destruction;
- Cryptographic device lifecycle management events; and

- CA System equipment configuration.

GQSCA 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 keys.

GQSCA 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 GQSCA and compliance auditors;
- Certificate Policy and previous versions;
- Certification Practice Statement and previous versions; and
- Certificate Application Forms and Subscriber Agreement between Subscribers and the GQSCA

Time stamping:

- Clock synchronization.

Miscellaneous

- Violations of the CP or this CPS

5.5.2 Retention Period for Archive

The archives are retained according to the Virginia Tech records management policy 2000.

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 archives for the GQSCA application.

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

The archive collection system respects the security requirements defined in section 5.3.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized GQSCA equipment, Trusted Role and other authorized persons are allowed to access the archive. Requests to obtain and verify archive information are coordinated by IMS.

5.6 Key Changeover

GQSCA may periodically change over Key Material for issuing CAs in line with section 6.3.2. Certificate subject information may also be modified and certificate profiles may be altered to highlight 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 GQSCA 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 in the scope of the audit process as described in section 8 to validate what are the operations that are first maintained after a disaster and the recovery plan.

GQSCA personnel that own a Trusted Role and operational role are specially trained to operate according to procedures defined in the Disaster Recovery plan for the most sensitive activities.

If GQSCA 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 GQSCA 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, however the signature keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate certificates status information according to GQSCAs disaster recovery plan.

5.7.3 Entity Private Key Compromise Procedures

In case a GQSCA signature key is compromised, lost, destroyed or suspected to be compromised:

- GQSCA, after investigation of the problem decides whether the GQSCA certificate should be revoked. If so then:
    - All the Subscribers who have been issued a certificate will be notified at the earliest feasible opportunity;
    - A new GQSCA 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 GQSCA Termination

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

- Stops delivering certificates according to and referring to this CPS
- Archive all audit logs and other records prior to termination;
- Destroys all private keys upon termination;
- Ensures archive records are transferred to VTPKI PMA.
- Use secure means to notify customers and software platform providers to delete all trust anchors.

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

GQSCA generates all issuing key pairs in a physically secure environment by personnel in Trusted Roles under, at least, dual control. GQSCA 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 Subscriber and thus does not need to be delivered.

6.1.3 Public Key Delivery to GQSCA

GQSCA shall only accept Public keys from Subscribers in line with section 3.2.1 of this CPS.

6.1.4 CA Public Key Delivery to Relying Parties

GQSCA 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

GQSCA follows NIST recommended timelines and best practice in the choice of size of its Keys for Root CAs, Issuing CAs and only signs end entity certificates following best practice.

The following Key sizes and hashing algorithms are used for Root Certificates, Issuing Certificates and End Entity Certificates and CRL/OCSP certificate status responders in line with CABForum Base Requirements:

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

GQSCA generates keys in accordance with FIPS 140-2 Lvl 3 and uses reasonable techniques to validate the suitability of 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)

GQSCA 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

GQSCA 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

GQSCA activates Private Keys for cryptographic operations with multi-token control (using CA activation data) by people performing duties associated with their trusted roles. The Trusted Roles permitted to participate in this private key multi-token controls are strongly authenticated (i.e. Token with PIN code).

6.2.3 Private Key Escrow

GQSCA does not escrow Subscriber Private Keys for any reason.

6.2.4 Private Key Backup

The GQSCA maintains a backup copy of its private key in order to re-establish functionality in case of destruction of the key.

6.2.5 Private Key Archival

GQSCA does not archive Subscriber Private Keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

GQSCA Private Keys are generated, activated and stored in Hardware Security Modules. Private Keys never exist in plain text outside of a cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

GQSCA 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 line with the obligations that are presented in the form of a Subscriber Agreement or Terms of use Agreement.

6.2.9 Method of Deactivating Private Key

GQSCA ensures that Hardware Security Modules that have been activated are not left unattended or otherwise available to unauthorized access. During the time a GQSCA's Cryptographic 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, its Private Keys are removed from the Hardware Security Module.

6.2.10 Method of Destroying Private Key

GQSCA 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 GQSCA 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

GQSCA archives Public Keys from certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

GQSCA certificates have a maximum validity period of:

Type	Private Key Usage	Certificate Term.
• **SSL/TLS Certificates -**	No stipulation	2 years

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of GQSCA activation data used to activate GQSCA 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 person in a Trusted Role. The delivery method maintains the confidentiality and the integrity of the *activation data.*

6.4.2 Activation Data Protection

Issue CA activation data is protected from disclosure through a combination of cryptographic and physical access control mechanisms. GQSCA activation data is stored on tokens.

6.4.3 Other Aspects of Activation Data

GQSCA activation data may only be held by GQSCA 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 GQSCA PKI components must include the following functions:

- Require authenticated logins for Trusted Role;
- Provide discrete 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;
- Provide protection for the operating system.

6.5.2 Computer Security Rating

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

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the GQSCA 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);
- Software is developed in a controlled environment, and the development processes are defined and documented. This requirement does not apply to commercial off-the-shelf 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 is 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 are obtained from sources authorized by local policy. GQSCA hardware and software are scanned for malicious code on first use and periodically thereafter;
- Hardware and software updates are purchased or developed in the same manner as original equipment; and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the GQSCA system as well as any modifications and upgrades are documented and controlled by the GQSCA administrators. There is a mechanism for detecting unauthorized modification to the GQSCA software or configuration. A formal configuration management methodology is used for installation and on-going maintenance of the GQSCA system. The GQSCA 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 Life Cycle Security Controls

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

6.7 Network Security Controls

GQSCA PKI components implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of 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 GQSCA components are regularly synchronized with a reliable time service. GQSCA 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)

GQSCA issues digital certificates in compliance with X.509 Version 3.

7.1.2 Certificate Extensions

GQSCA issues digital 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

GQSCA issues digital certificates with Algorithms indicated by the following OIDs;

• **SHA1WithRSAEncryption**	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
• **SHA256WithRSAEncryption**	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}

7.1.4 Name Forms

GQSCA issues digital certificates with Name Forms compliant to RFC 5280. Within the domain of each Issuing CA, GQSCA 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

GQSCA issues digital certificates with a Policy Qualifier and suitable text to aid relying parties to determine applicability.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

7.2.1 Version Number(s)

GQSCA issues Version 2 CRLs in compliance with RFC 5280. CRLs have the following fields:

• **Issuing CA**	GQSCA
• **Effective date**	Date and Time
• **Next update**	Date and Time
• **Signature Algorithm**	sha1RSA
• **Signature Hash Algorithm**	SHA-1
• **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

GQSCA operates an Online Certificate Status Profile (OCSP) responder in compliance with RFC 2560 or RFC5019.

7.3.1 Version Number(s)

GQSCA 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. GQSCA 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 GQSCA are assessed on an annual basis by GlobalSign nv-sa or an affiliated GlobalSign company as part of the contractual obligation in using TrustedRoot chaining services. The assessment covers all CA related activities as recommended by the CABForum 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 CABForum Baseline requirements are maintained using suitably qualified and trained GlobalSign staff members.

8.3 Assessor's Relationship to Assessed Entity

GQSCA is a cross signed entity under contract with GlobalSign nv-sa or an affiliated company under the TrustedRoot program.

8.4 Topics Covered by Assessment

The Audit meets the requirements of the CABForum Baseline Requirements.

8.5 Actions Taken as a Result of Deficiency

GQSCA follows the same process if presented with a material non-compliance by GlobalSign nv-sa or an affiliated company. GQSCA 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 highlighted to the GlobalSign Policy Authority for discussion and resolution.

8.6 Communications of Results

Results of the Audit are reported to VTPKI PMA 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

GQSCA 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 classed as being Confidential Information and therefore are subject to reasonable care and attention by GQSCA staff including Administrators.

- Personal Information as detailed in section 9.4
- Audit Logs from CA and RA systems
- Activation Data used to activate CA private keys as detailed in section 6.4
- Internal Virginia Tech business process documentation including Disaster Recovery Plans (DRP), Business Continuity Plans (BCP)
- Audit reports from an independent auditor as detailed in section 8.0

9.3.2 Information Not Within the Scope of Confidential Information

Any GQSCA information not defined as confidential within this CPS shall be deemed public. Certificate status information and certificates themselves are deemed public.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

GQSCA protects personal Information in line with legal requirements where GQSCA operates through internal policy.

9.4.2 Information Treated as Private

GQSCA treats all information received from Applicants that will not ordinarily be placed into a certificate in accordance with university policy, state law, and federal law and regulations. This applies both to those Applicants who are successful in being issued a digital certificate and those who are unsuccessful and rejected. GQSCA periodically trains all RA 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, in accordance with university policy, state law, and federal law and regulations and in accordance with 9.4.5.

9.4.4 Responsibility to Protect Private Information

GQSCA protects personal Information in line with legal requirements where GQSCA operates.

9.4.5 Notice and Consent to Use Private Information

By the act of applying, Applicants consent to make public information that will be placed into a certificate. Additional information is treated in accordance with university policy, state law, and federal law and regulations. GQSCA incorporates the relevant provisions within an appropriate Subscriber Agreement including any additional information obtained from third parties that may be applicable to the validation process for the product or service being offered by GQSCA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

GQSCA may disclose private Information without notice to Applicants or Subscribers where required to do so by law, regulation or Virginia Tech policy.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property rights

GQSCA does not knowingly violate the Intellectual Property Rights of third parties. Public and Private keys remain the property of Subscribers who legitimately hold them. GQSCA 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

GQSCA uses this CPS and applicable Subscriber Agreements to convey legal conditions of usage of issued certificates to Subscribers and Relying Parties. All parties including the GQSCA, any RAs and subscribers warrant the integrity of their respective private key(s). If any such party suspects that a private key has been compromised they will immediately notify the appropriate RA.

GQSCA represents and warrants to Certificate Beneficiaries:

- The Subscriber that is a party to the Subscriber or Terms of Use Agreement for the Certificate;
- All Relying Parties who reasonably rely on a Valid Certificate.

that, during the period when the Certificate is valid, GQSCA 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, GQSCA (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 GQSCA's Certification Practice Statement (See section 3.2);
- **Authorization for Certificate:** That, at the time of issuance, GQSCA (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 GQSCA's Certification Practice Statement (See section 3.2.5);
- **Accuracy of Information:** That, at the time of issuance, GQSCA (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 GQSCA's Certification Practice Statement (See sections 3.2.3, 3.2.3, 3.2.4);
- **No Misleading Information:** That, at the time of issuance, GQSCA (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 GQSCA's 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 GQSCA's Certification Practice Statement (See sections 3.2.3, 3.2.3, 3.2.4);

- **Subscriber Agreement:** That GQSCA and Subscriber are Affiliated; therefore, the Applicant representative acknowledged and accepted the Terms of Use (See section 4.5.1);
- **Status:** That GQSCA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- **Revocation:** That GQSCA 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 GQSCA does not contain any misleading or false information
- All translated material provided by the RA is accurate

9.6.3 Subscriber Representations and Warranties

Unless otherwise stated in this 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 GQSCA's certificate promises to:

- Have the technical capability to use digital certificates.

- Receive notice of the GQSCA and associated conditions for relying parties.
- Validate a GQSCA's certificate by using certificate status information (e.g. a CRL or OCSP) published by the GQSCA in accordance with the proper certificate path validation procedure.
- Trust a GQSCA'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 GQSCA's certificate, only as it may be reasonable under the circumstances.
- 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.
- Take any other precautions prescribed in the GQSCA'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

GQSCA 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 GQSCA

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 GQSCA, GlobalSign nv-sa and any related entity providing services to GQSCA, 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 notice of the opposite is communicated by the GQSCA on its web site or repository.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

GQSCA will communicate the conditions and effect of this CPS termination via their appropriate repository.

9.11 Individual Notices and Communications with Participants

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

9.12.2 Notification Mechanism and Period

GQSCA 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

GQSCA 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

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

9.16 Miscellaneous Provisions

9.16.1 Compelled Attacks

GQSCA is subject to the Commonwealth of Virginia jurisdiction and regulatory framework. GQSCA 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

GQSCA 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 GQSCA.

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

GQSCA’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.

Mary B. Dunker

Digitally signed by Mary B Dunker
DN: 0.9.2342.19200300.100.1.1=819647, cn=Mary B Dunker, o=Virginia Polytechnic Institute and State University, dc=vt, dc=edu, c=US
Date: 2015.08.24 19:57:19 -04'00'

John D Krallman

Digitally signed by John D Krallman
DN: 0.9.2342.19200300.100.1.1=808013, cn=John D Krallman, o=Virginia Polytechnic Institute and State University, dc=vt, dc=edu, c=US
Date: 2015.08.25 07:37:41 -04'00'