Scientific Software and Systems (SSS) Public Key Infrastructure Certificate Policy (CP) and Certificate Practice Statement (CPS)

December 2022

Document History

Version	Date	Author	Change Comment
0.1	March 2022	Brett Moses	Original Draft
0.2	May 2022	Brett Moses	Added OID section 1.2
1.0	November 2022	Brett Moses	Final version
1.1	December 2022	Brett Moses	Updated section 1
1.2	December 2022	Brett Moses	Added and updated references.

Scope and Applicability

This document constitutes the Certificate Policy (CP) and Certificate Practice Statement (CPS) for the SSS PKI Certification Authorities (CAs). SSS IT Security Specialists is responsible for the operation of the SSS OKI Root and Policy CAs as well as for the SSS Issuing CAs. The purpose of this document is to publicly disclose to Subjects and Relying Parties the business policies and practices under which the SSS CAs operate.

Digital certificates, containing a public key, identify the entity who is the holder of the associated private key used to digitally sign an electronic transaction. This forms the basis of positive identity, message integrity, and non-repudiation when conducting business electronically. Private keys may also be used to achieve confidentiality.

This SSS Certificate Policy introduces the rules that SSS IT Security Specialists requires adherence to ensure a high level of trust in the digital certificates issued by the SSS Issuing CA. Digital certificates, properly issued, are an effective risk management tool used address the business need for positive identity, privacy and non-repudiation.

The management of the resources required to operate the SSS Root, Policy, and Issuing CAs is in accordance with the provisions is contained in this policy document. These resources include registration authorities, personnel, network infrastructure, IT systems, cryptographic material, physical locales, and information assets.

Document References

[CAB_Forum] Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates; CA / Browser Forum; http://www.cabforum.org

[ETSI TS 102042] Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates (Feb. 2013)

[ISO27001] Information technology - Security techniques - Information security management systems – Requirements (March 2015)

[RFC3647] Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Network Working Group: S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu (November 2003).

[RFC5280] Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile, Network Working Group: R. Housley, W. Polk, W. Ford, D. Solo (May 2008)

ETSI EN 319 401 V2.1.1: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

ETSI EN 319 411-1 V1.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

2nd Draft NISTIR 7924: Reference Certificate Policy, Computer Security Division Information Technology Laboratory : Harold Booth, Andrew Regenscheid (May 2014)

[RFC 7382] “Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI)”. S. Kent, D. Kong, K. Seo

RFC 2822 “Internet Message Format”, Network Working Group: P. Resnick, Editor

[FIPS 140-2] Federal Information Processing Standards (FIPS) 140-2

[RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Network Working Group: D. Cooper

Table of Contents

1. Introduction

This document is structured according to RFC 3647 “Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework” [RFC3647], and RFC 7382 “Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI)”.

1.1. Overview

This document describes the Certificate Policy (CP) and Certificate Practice Statement (CPS) of the SSS Public Key Infrastructure (PKI) CAs. It describes the services provided by the SSS PKI as well as the binding requirements that must be fulfilled by service providers and other PKI participants. This policy document:

- defines the certification process and the cooperation, duties and rights of the PKI participants.
- describes the business, technical and procedural requirements to govern the use of SSS Certificates by participants in the SSS PKI.
- provides the framework and context within which certificates are requested, created, issued, renewed, managed, revoked and/or used by participants of the SSS PKI.

The SSS PKI issues certificates for use in conjunction with various SSS IT Security Specialists products and services. These certificates are used to authenticate the participating entities in an online transaction, to provide confidentiality for the data being communicated, the context within which certificates are requested, created, issued, renewed, managed, revoked and/or used by participants of the SSS PKI and to provide message integrity of transactions.

Based on the recommendations of the Internet Engineering Task Force for Public Key Infrastructure, RFC 3647 and RFC 7382, this CP \ CPS establishes the Policy for deploying Certificates to protect the integrity and confidentiality of Subscriber information within the SSS PKI. Where a heading of RFC 3647 \ RFC 7382 does not apply to the SSS PKI the statement “Not applicable” or “No stipulation” is made.

1.1.1 PKI hierarchy

The structure of the SSS PKI hierarchy is shown in Figure 1.

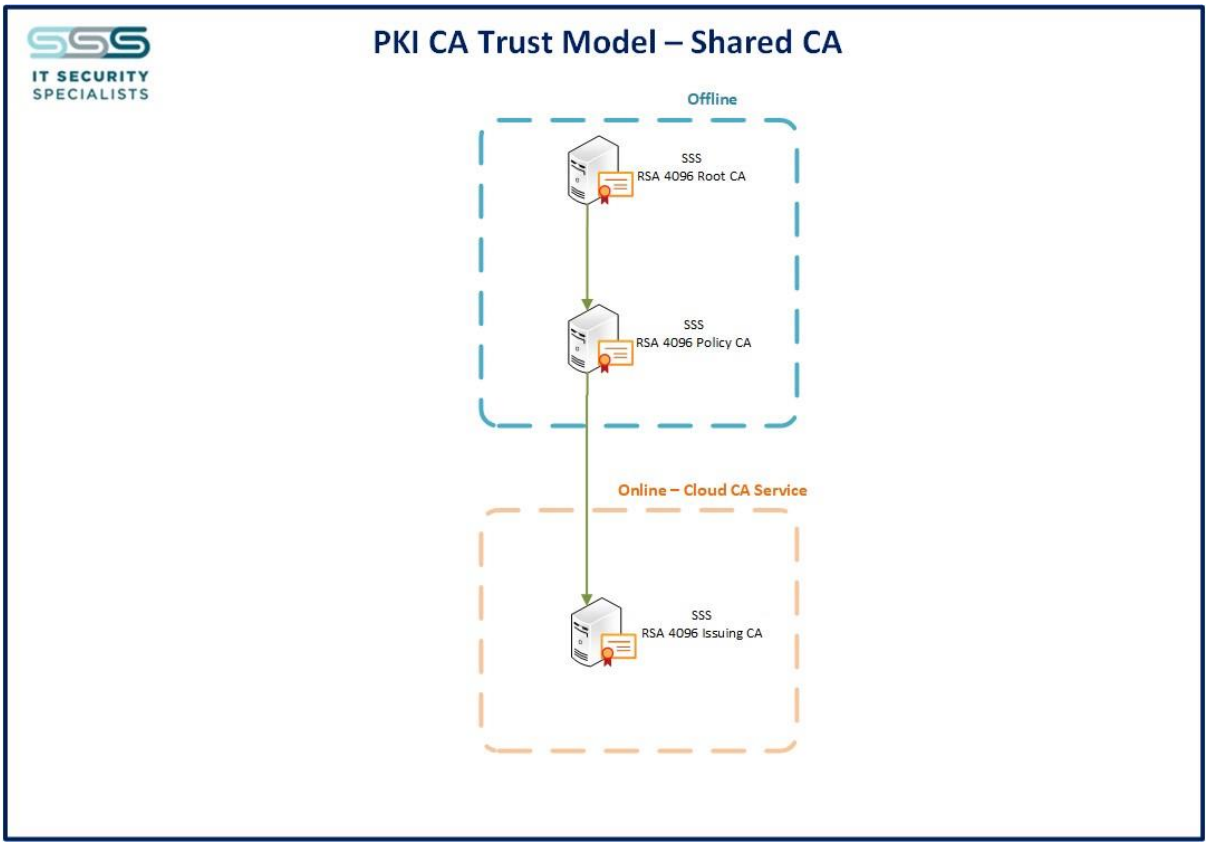

Figure 1: SSS PKI Hierarchy

In compliance with the business requirement, the PKI will consist of a:

a. Production Root CA
b. Production Policy SubCA
c. Production Issuing CA

This infrastructure will be duplicated across the datacentres for disaster recovery and business continuity purposes

1.1.2 SSS Root CA

The SSS PKI architecture is based on a three-tier CA structure. This Root CA is stored off-line. The Root CA performs the signing, issuance, and revocation of certificates used to establish and authenticate the Policy CA. The Root CA only issues Subordinate CA Certificates. The Root CA is also used for signing it's CRL file.

1.1.3 SSS Policy CA

The Policy CA is a subordinate CA undersigned by the Root CA and is stored off-line. The Policy CA performs the signing, issuance, and revocation of certificates used to establish and authenticate the Issuing CA. The Policy CA only issues Issuing CA certificates. The role of this Policy CA would be to provide different certificate policies and constraints, such as naming, application, key usages that the Issuing CA can issue certificates, etc. for the Issuing CAs. The Policy CA is also used for signing it's CRL file.

1.1.4 SSS Issuing CA

The SSS Issuing CA is online and issues Certificates to End Entities and manages and revokes End Entity Certificates.

1.2 Document Name and Identification

This CP \ CPS is referred to as the SSS Certificate Policy and Certificate Practice Statement.

Title: Scientific Software and Systems (SSS) Public Key Infrastructure Certificate Policy (CP) and Certificate Practice Statement (CPS)

OID: 1.3.6.1.4.1.58631.1.4.1

Expiration: This version of the document is the most current one until a subsequent release is approved and published

1.3 PKI Participants

PKI Participants are classified as the SSS Certification Authorities, Registration Authorities, Subjects, and Relying Parties.

1.3.1 Certification Authorities

The SSS PKI Hierarchy is depicted in Figure 1 above.

1.3.1.1 Root CA

The Root CA issues, manages, and revokes X.509v3 Certificates used by the corresponding Policy CAs. This includes the following activities:

- Generating Root CA Key Pairs
- Generating Certificates for the Policy CAs
- Recertification of existing Subordinate CA keys
- Revoking Policy CA Certificates; and
- Maintaining a Revocation List of Subordinate CA Certificates.

1.3.1.2 Policy CA

The Policy CA issues, manages, and revokes X.509v3 Certificates used by the corresponding Policy CAs. This includes the following activities:

- Generating Certificates for the Issuing CAs
- Recertification of existing Issuing CA keys
- Revoking Issuing CA Certificates; and
- Maintaining a Revocation List of Issuing CA Certificates.

1.3.1.3 Issuing CAs

The Issuing CAs together with PKI Participants (such as Registration Authorities) issue, manage or revoke X.509v3 Public Key Certificates used for securing business processes either internally (e.g. domain computer certificates) or externally (e.g. web server certificates). The services offered include:

- Generating Certificates for the end entities
- Revoking End-Entity Certificates
- Maintaining a Revocation List for End-Entity Certificates

1.3.2 Registration Authorities

The client or organisation that subscribes to the SSS PKI, shall be Registration Authority (RA) entity that collects and verifies each End Entity's identity and information to be entered into the End Entity's public key certificate. While the RA enables the process for End Entities to enrol for certificates from the Issuing CA, it does not sign or issue certificates. The RA shall perform its functions in accordance with this CP \ CPS. The RA shall be responsible for:

- Developing and maintaining control over the registration process; and
- Developing and maintaining the identification and authentication process.

Automation to facilitate these RA activities is allowed where possible to meet these requirements, and where the users have access to this automation service.

The RA shall only perform the functionality delegated by the CA.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the CP \ CPS asserted in the certificate, and who does not issue certificates. CAs can be considered "Subscribers" in a PKI. However, the term "Subscriber" as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

The Subscriber's responsibilities include the:

a. Provision of complete, accurate and truthful information in a certificate application;
b. Request to revoke the subject's certificate when the certificate contains incorrect information or Subscriber's Private Key or the Activation Data controlling its access has been lost or when Subscriber has reason to believe that the Private Key has been accessed by another individual or otherwise compromised; and
c. Acknowledgement of receipt or assent to Subscriber responsibilities.

1.3.4 Designated Certificate Holder

Under certain circumstances, automation may require a device to hold a certificate. In these situations, an individual user shall take ownership responsibility for these certificates and the associated security.

1.3.5 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party shall be responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information.

The Relying Party may use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A

Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

Relying Party responsibilities include:

a. perform cryptographic operations properly: verification of Digital Signatures by referring to Subject's Public Key listed in a valid Certificate and verification whether there is a Certificate Path to a trusted CA;
b. check the status of Certificates before relying on it, including the revocation status in the Certificate Revocation List ("CRL") or by the use of the Online Certificate Status Protocol ("OCSP");
c. assent to the terms of an applicable agreement required as a condition to relying on the Certificate.

1.3.6 Other participants

1.3.6.1 Policy Authority

The Policy Authority (PA) shall be responsible for:

- Reviewing, approving, and maintaining this CP \ CPS
- Reviewing and approving the CP \ CPS for any CA that issues certificates asserting policy OIDs defined in this document
- Reviewing and accepting applications from other PKI Domains desiring to interoperate with the SSS PKI and
- Reviewing and approving any audit reports for CAs that issue certificates asserting policy OIDs defined in this document.

1.3.6.2 Operational Authority

Within SSS, the Operational Authority (OA) shall be an employee of SSS. The OA shall be tasked with the operation of one or more Certification Authority servers. These servers issue and manage Public Key Certificates and certificate revocation lists issued in accordance with this CP \ CPS. The OA shall be responsible for:

- Developing, and submitting to the PA for review and approval, a CP \ CPS for each CA that is participating in the SSS PKI
- Responsible for all equipment and software required to operate the SSS PKI, as well as maintaining an inventory list of physical assets; and
- Ensuring that the Certificate Authority, Repository, Registration System, Smartcard Management System and other PKI-related components are operational in accordance with this policy.

1.4 Certificate Usage

1.4.1 Appropriate Certificate uses

The certificates signed by the SSS Root CA are approved for the following usages:

Certificate	Use
Root CA Certificate	This certificate is signed by the Root CA itself and only approved for signing the CA Certificates of the Policy CA, and the Root CA´s CRL. The SSS CA may issue certificates to enable Server Authentication, Client Authentication, Device Authentication, IKE, Code Signing, and Encryption
Policy CA Certificate	This certificate is signed by the Root CA and only approved for signing the CA Certificates of the Issuing CA, and the Policy CA´s CRL. The SSS CA may issue certificates to enable Server Authentication, Client Authentication, Device Authentication, IKE, Code Signing, and Encryption.
Issuing CA Certificates	These certificates are approved only for the signing of the end-entity certificates, the Issuing CA´s CRL, and OCSP signer certificates. The SSS CA may issue certificates to enable Server Authentication, Client Authentication, Device Authentication, IKE, Document Signing, Encryption, Code Signing, OCSP signing, IP Sec tunnelling, Secure email, EFS

Table 1: Certificate Usage

1.4.2 Prohibited Certificate uses

All certificate usages not listed in 1.4.1 are prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The SSS PA is responsible for all aspects relating to the update and amendment of this CP \ CPS.

1.5.2 Contact Person

Questions, comments and suggestions regarding this CP \ CPS can be directed to:

Brett Moses

SSS – IT Security Specialists, Level 8

25 Victoria Street

Petone

Lower Hutt

5012

New Zealand

Website : https://www.sss.co.nz

Email: brett.moses@sss.co.nz

1.5.3 Person Determining CP and CPS Suitability for the Policy

The SSS PA shall approve the CP \ CPS for each CA that issues certificates under this policy.

1.5.4 CP and CPS approval procedures

The PA shall review this CP \ CPS annually. The PA may amend this CP \ CPS, or any part thereof, at any time at its discretion. All policy changes under consideration by the PA shall be disseminated to interested parties. All interested parties shall provide their comments to the PA in a fashion to be prescribed by the PA. Distribution of potential policy changes to relying party and subscriber end entities is not the responsibility of the PA. The PA will make a reasonable effort to ensure that such information is accessible to those communities through normal distribution channels.

The OA shall determine if a CP \ CPS sets out in a satisfactory manner how the CA will implement the requirements of this policy, and recommend approval when appropriate to the PA. The PA shall approve the Certification Practice Statement and any amendments thereto. Any modifications to this CP shall be subject to inspection and review by the external auditor during the normal compliance audit period.

1.6 Definitions and Acronyms

1.6.1 List of Definitions

Access: Ability to make use of any information system (IS) resource.

Access Control: Process of granting access to information system resources only to authorized users, programs, processes, or other systems.

Accreditation: Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

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

Anonymous: Having an unknown name.

Applicant: The subscriber is called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.

Application: A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.

Archive: Long-term, physically separate storage.

Attribute Authority: An entity, recognized as having the authority to verify the association of attributes to an identity.

Audit: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009]

Audit Data: Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]

Authenticate: To confirm the identity of an entity when that identity is presented.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Authorized Organizational Representative (AOR): A person (potentially among several) within an organization who is authorized to vouch for non-person identities. Any particular AOR is not permanently linked to any particular non-person identity; the CA must only ascertain that the AOR is legitimately associated with the organization, and that the AOR is identified as having authority for the identity in question.

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

Bastion Host: A special purpose computer on a network specifically designed and configured to withstand attacks.

Binding: Process of associating two related elements of information.

Biometric: A physical or behavioural characteristic of a human being.

Certificate: A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. As used in this CP, the term “certificate” refers to X.509 certificates that expressly reference the OID of this CP in the certificate policies extension.

Certification Authority (CA): n authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.

CA Facility: The collection of equipment, personnel, procedures and structures that are used by a certification authority to perform certificate issuance and revocation.

CA Operating Staff: CA components are operated and managed by individuals holding trusted, sensitive roles.

Certificate Policy (CP): A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of public key certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certification Practice Statement (CPS): A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

CPS Summary: A publicly releasable version of the CPS.

Certificate-Related Information: Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.

Certificate Revocation List (CRL): A list maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date.

Certificate Status Server (CSS): A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status and may also provide additional attribute information for the subject certificate.

Compromise: Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Computer Security Objects Registry (CSOR): Computer Security Objects Registry operated by the National Institute of Standards and Technology.

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

Cross-Certificate: A certificate used to establish a trust relationship between two certification authorities.

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. [FIPS 140]

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

Digital Signature: The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.

End Entity Certificate: A certificate in which the subject is not a CA..

Firewall: Gateway that limits access between networks in accordance with local security policy.

Integrity: Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.

Intellectual Property: Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.

Intermediate CA: A CA that is subordinate to another CA and has a CA subordinate to itself.

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 Exchange: The process of exchanging public keys in order to establish secure communications.

Key Management Key: Key exchange, key agreement, key transport

Key Pair: Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (2) even knowing the public key, it is computationally infeasible to discover the private key.

Key Rollover Certificate: The certificate that is created when a CA signs a new public key for itself with its old private key, and vice versa

Modification (of a certificate): The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.

Mutual Authentication: Occurs when parties at both ends of a communication activity authenticate each other (see authentication).

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.

Object Identifier (OID): A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Federal PKI, OIDS are used to uniquely identify certificate policies and cryptographic algorithms.

Online Certificate Status Protocol: Protocol which provides on-line revocation status information for certificates.

Operations Zone (OZ): Network area containing systems for routine business operations.

Out-of-Band: Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring on-line).

Policy Authority (PA): 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.

Privacy: Restricting access to subscriber or relying party information in accordance with Federal law.

Private Key: (1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Pseudonym: A subscriber name that has been chosen by the subscriber that is not verified as meaningful by identity proofing.

Public Key: (1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital certificate.

Public Key Infrastructure (PKI): A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Public Zone (PZ): Network area that is not behind a protective boundary controlled by the organization.

Registration Authority (RA): An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA).

Re-key (a certificate): To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.

Relying Party: A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate and is in a position to rely on them.

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

Repository: A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.

Restricted Zone (RZ): Controlled network area for sensitive data processing and storage

Revoke a Certificate: To prematurely end the operational period of a certificate effective at a specific date and time.

Risk: An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Root CA: In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Security Auditor: An individual (e.g. employee, contractor, consultant, 3rd party) who is responsible for auditing the security of CAs or Registration Authorities (RAs), including reviewing, maintaining, and archiving audit logs; and performing or overseeing internal audits of CAs or RAs. A single individual may audit both CAs and RAs. Security Auditor is an internal role that is designated as trusted.

Server: A system entity that provides a service in response to requests from the SSS PKI CAs.

Signature Certificate: A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.

Special Access Zone (SAZ): Highly controlled network area for processing and storage of especially high value data.

Subordinate CA: In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).

Subscriber: A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device.

Subscriber Certificate: A certificate in which has been issued to a subscriber from the SSS PKI Issuing CAs.

Superior CA: In a hierarchical PKI, a CA that has certified the certificate signature key of another CA, and that constrains the activities of that CA. (See subordinate CA).

Threat: Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]

Trust List: Collection of Trusted Certificates used by relying parties to authenticate other certificates.

Trust Zone: The level of security controls in a network segment.

Trusted Agent: Entity authorized to act as a representative of a CA in confirming subscriber identification during the registration process. Trusted agents do not have automated interfaces with certification authorities.

Trust Anchor Manager: Authorities who manage a repository of trusted Root CA Certificates. They act on behalf of relying parties, basing their decisions on which CAs to trust on the results of compliance audits. A TAM sets requirement for inclusion of a CA's root public key in their store. These requirements are based

on both security and business needs. The TAM has a duty to enforce compliance with these requirements, for example, requirements around the supply of audit results, on initial acceptance of a root, and on an ongoing basis. TAMs will follow their normal practice of requiring CAs to submit an annual audit report.

Trusted Certificate: A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

Two-Person Control: Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.

Zeroize: A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140]

Zone Boundary: The limit of authority over the security of the data processed within the boundary.

1.6.2 List of Acronyms

ARL	Authority Revocation List
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DNS	Domain Name System
EFS	Encrypted File System
ELB	Elastic Load-balanced
FIPS	Federal Information Processing Standard
IKE	Internet Key Exchange
IP Sec	Internet Protocol Security
LDAP	Lightweight Directory Application Protocol
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure, also known as PKS
PKS	Public Key Services, also known as PKI
PSS	Probabilistic Signature Scheme

RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request for Comment
RSA	Rivest Shamir Adelman
SPSE	Secure Personal Security Environment
TA	Trusted Agent
URL	Uniform Resource Locator

2 Publication and Repository Responsibilities

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. CAs may optionally post subscriber certificates in this repository, unless specifically prohibited within the CP. To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

2.1 Repositories

SSS IT Security Specialists' CA Repositories are operated by the SSS IT Security Specialists. The Repository responsibilities include:

a. accurately publishing information;
b. publishing and archiving Certificates;
c. publishing the status of Certificates;
d. availability to the CAs, RAs, Subjects and Relying Parties during the period of availability specified in SSS PKI documentation;
e. promptness or frequency of publication; and
f. security of the Repository and controlling access to information published on the Repository to prevent unauthorized access and tampering.

Relying Parties have access to:

- Certificate Revocation List (CRL) via:
  - HTTP: http://mpki.sss.co.nz
- Online certificate status information via:
  - HTTP: http://mpki.sss.co.nz/ocsp

2.2 Publication of Certification Information

The SSS CA publishes the publicly available information at http://mpki.sss.co.nz

At a minimum the following information is published:

- all required Certificates to trust the Root CAs;
- all Issuing CA Certificates;
- revocation information for Root CA and Issuing CA certificates and for end entity certificates; and

The CP shall be publicly available. The CPS of the CA is not required to be published. However, a summary or redacted CPS shall either be publicly available or available upon request to relying parties.

2.3 Time or Frequency of Publication

An updated version of the policy document will be made publicly available within thirty days of the incorporation of changes.

2.4 Access Controls on Repositories

The CA shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be publicly available through the Internet. Direct and/or remote access to other information in the CA repositories shall be determined by the Policy Authority. The CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under what conditions the restricted information may be made available.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

All CAs operating under this policy shall generate, sign, and process certificates that contain an X.501 Distinguished Name (DN) that clearly and distinguishingly identifies the issuer and the subject of the certificate. Geopolitical or Domain Component naming elements may be used exclusive to each other. Other name forms may appear in the certificate's subject alternative name extension. For device certificates, the fully distinguished domain name of the subscribing end entity shall be incorporated in the subject name.

3.1.2 Need of Names to be Meaningful

Names used in certificates must represent an unambiguous identifier for the subject. Names shall be meaningful enough for a human to identify the named entity, irrespective of whether the entity is a person, machine, or process. Interpreting the name semantic may require a reference database (e.g., human resources directory or inventory catalogue) external to the PKI.

While the issuer name in CA certificates is not generally interpreted by relying parties, this CP still requires use of meaningful names by CAs issuing under this policy. CA certificates that assert this policy shall not include a personal name, but rather shall identify the subject as a CA and include the namespace for which the CA is authoritative.

Certificate Description	Name Meanings
CA Digital Signature Certificates	CAs shall implement a name that is descriptive to the purpose of the CA.
SSL Certificates	The authenticated FQDN shall be included in a SAN. The subject DN common name may also contain the authenticated registered domain name of the Agency Application server.

Table 2: Naming Conventions

3.1.2.1 CA Names

The CN must be stated as the full name of the CA. A CA name indicates its purpose.

3.1.2.2 End Entity (EE) Names

EE Certificates must contain commonly understood names permitting the determination of the identity of the entity.

3.1.3 Anonymity or Pseudonymity of subscribers

The CA shall not issue anonymous certificates. Pseudonymous certificates, if issued shall be identified as such. CAs issuing pseudonymous certificates shall maintain a mapping of identity to pseudonym.

3.1.4 Rules for Interpreting Various Name Forms

Name forms shall comply with RFC 2822 and X.500 standards for name forms.

3.1.5 Uniqueness of Names

Each CA must ensure that each of its subscribers is identifiable by a unique name. Each X.500 name assigned to a subscriber by a CA (i.e., in that CA's namespace) must identify that subscriber uniquely. When other name forms are used, they too must be allocated such that each name identifies only one subscriber of that CA. Name uniqueness is not violated when multiple certificates are issued to the same entity. For certificates that assert names that do not identify individual people, an Authorized Organisational Representative (AOR) shall be identified as having responsibility for the certificate subject. The CPS shall identify the method for the assignment of unique subject names.

3.1.6 Recognition, Authentication, and Roles of Trademarks

CAs operating under this policy shall not issue a certificate knowing that it infringes on the trademark of another. The PA shall resolve disputes involving names and trademarks.

3.2 Initial Identity Validation

A Certificate shall be issued to a Subject only when the Subject has submitted a Certificate Request and is able to prove to the RA possession of the corresponding Private Key.

3.2.1 Method to Prove Possession of Private Key

In all cases where the subject named in a certificate generates its own keys, that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request. Proof of possession must be commensurate with the level of assurance being requested in the subsequent certificate. Cryptographic proof using the generated keys or in person proof using validated software and hardware are two examples of meeting this stipulation.

3.2.2 Authentication of Organization Identity

Requests for CA certificates shall include the CA name, address, and documentation of the existence of the CA. Before issuing CA certificates, an authority for the issuing CA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the CA.

For subscriber organization certificates, the CA shall verify the existence of the organization by verifying the identity and address of the organization and that the address is the subscriber's address of existence or operation.

3.2.3 Authentication of Individual Identity

For all End Entity Certificates, SSS CA shall cause the respective RA to confirm that:

- the Certificate Applicant is the person identified in the Certificate Application.
- the Certificate Applicant rightfully holds the Private Key corresponding to the Public Key to be listed in the Certificate; and
- the information to be included in the Certificate is accurate, except for non-verified Subject information.

To make this confirmation, RAs use information in the subscriber's organisation human resources databases to approve or reject Certificate Applications. Prior to issuance of a Certificate, Certificate Applicants shall either be:

- personally present before an authorized RA or its designated representative to check the identity of the Certificate Applicant against a well-recognized form of government-issued or corporate identification (e.g., a passport, driver's license, or corporate identity card).
- electronic form-based process used by the RA.

3.2.3.1 Authentication of Human Subscribers

The identity proofing requirements for individuals will vary based on local laws and the level of assurance the PKI is seeking to attain.

The RA shall ensure that the subscriber's identity information is verified. Identity shall be verified no more than 30 days before initial certificate issuance. At a minimum, authentication procedures for human subscribers must include the following steps:

1) Verify that a request for certificate issuance to the applicant was submitted by the organization.
2) Verify Subscriber's organizational membership through use of official organization records.
3) Establish subscriber's identity by in-person proofing before the registration authority, based on the following process:

   a) The subscriber presents an official form of identification (e.g., an organization ID badge, a passport, or driver's license) as proof of identity

   b) The RA examines the presented credential that can be linked to the subscriber (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and

   c) The credential presented above shall be verified by the RA for currency and legitimacy (e.g., the organization ID is verified as valid).

4) Verify information to be included in the certificate (e.g., e-mail address, subject alternative pseudonymous names).
5) Record and maintain records of the applicant by the RA or CA. This information is archived to help establish an audit trail for dispute resolution.

3.2.3.2 Authentication of Devices

This applies to identities assigned to hardware devices, not the software or applications that run on them.

Some computing and communications devices (routers, firewalls, etc.) will be named as certificate subjects. In such cases, an Authorized Organizational Representative (AOR), or in certain cases the device itself, must provide identifying information for the device. The AOR/device is responsible for providing registration information which may include:

- Equipment identification (e.g., serial number)
- Equipment certificate signing request CSR
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the AOR when required.

The registration information provided by the AOR/device shall be verified. If the device itself provides this information, the identity of the device shall be authenticated. If the information is provided by an AOR for a single device or batch of devices, the AOR shall be authenticated.

3.2.3.3 Authentication of Applications or Services

This applies to identities assigned to the services offered via a network, irrespective of the hardware running the software that implements the service. This enables services to be replaced from backup in the event of a hardware failure, without re-provisioning keys. (The hardware may have its own certificate, as described in Section 3.2.3.2 above.)

Some software applications or services will be named as certificate subjects. In such cases, an Authorized Organizational Representative (AOR) must provide identifying information for the device. The AOR is responsible for providing registration information which may include:

- Unique software application or service name (e.g. DNS name)
- Software application or service certificate signing request CSR
- Software application or service authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the AOR when required.

The registration information provided by the AOR shall be verified. The CA shall validate that the AOR is authorized to request a certificate for the application or service. An automated RA process using certificate lifecycle automation with configured policy is able to process certificate requests on behalf of an RA provided sufficient logging is enabled.

Auto-enrolment of devices through an Active Directory Domain policy is allowed provided the device is trusted in the domain.

3.2.3.5 Authentication for Code Signing Certificates

Code signing indicates to the recipient of the code that the code comes from an authorized source, and that the integrity of the source has been protected during distribution (i.e., that the code hasn't been modified). A code signing certificate identifies the person or organization authorized to make those claims to the code recipient.

The procedures for issuing code signing certificates shall comply with all other stipulations of this CP (e.g., subscriber identity proofing, validation of organization affiliation, key generation, private key protection, and Subscriber obligations). One or more AORs shall be assigned to act on behalf of the code signing certificate subscriber for certificate management activities such as issuance, renewal, re-key, modification, and revocation.

The CA or the RA shall record the information identified in Section 3.2.3.1 for an AOR associated with the code signing certificate. The CA or RA shall verify the identity of the AOR using an individual certificate issued by a CA with equivalent assurance as the code signing certificate, or other commensurate methods. AORs shall be responsible for:

- Authorizing subscribers for a code signing certificate
- Revocation of subscriber's code signing certificates
- Always maintaining a current up-to-date list of subscribers who are authorized to hold code signing certificates and their associated private keys.

3.2.3.6 Domain Names

All the domains requested in a certificate must be owned and managed by the subscriber's organisation or the domains must be owned by sub entities. Domains which do not meet these criteria will not be issued a certificate from the certificate authority and must use a third-party supplier.

The procedures for Certificates that will include the domain name of a server include the following:

- Verify that the domain name is registered with a domain name server (DNS) managed by the subscriber's organisation or one of its sub entities. Subdomains must be for a domain appropriately registered in DNS.
- Verify that the entity to be named as the Subject in the Certificate is aware of its registration of the domain name.

3.2.4 Non-verified Subscriber Information

Information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

Before issuing CA certificates or signature certificates that assert organizational authority, the CA shall validate the subscriber's authority to act in the name of the organization.

3.2.6 Criteria for Interoperation

The SSS PA shall determine the interoperability criteria for CAs operating under the SSS CP.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

RAs SHALL treat certificate re-key requests identical to applications for new certificates and perform the same identity-proofing processes as described in Section 3.2.2. Routine re-key of the SSS PKI CA Certificates SHALL be performed in accordance with the established Key Generation process in Section 6.1 of this policy.

For re-key of any subscriber certificate issued under this certificate policy, identity may be established through use of current signature key, except that identity shall be established following the same procedures as the initial registration at least once every 1 years from the time of original registration.

Automated Routine Re-key

Routine re-Key may be performed through use of the current signature key as long as the Key has not exceeded its validity period and the associated certificate is not revoked. Requests for all re-Keys shall be recorded in a log, with the status of the request.

Manual Re-Key Requests

Only the individual or Authorised representative of an entity may request a re-Key transaction. The entity or individual requesting re-Key may authenticate using their valid Digital Signature Key pair. Routine re-Key authentication may use a secret question and answer established by the subscriber during the initial registration process.

3.3.2 Identification and Authentication for Re-key after Revocation

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.2 above.

3.4 Identification and Authentication for Revocation Requests

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether the associated private key has been compromised. If the Private Key is not available for signing a revocation request, the Subscriber may submit a written revocation request (email is acceptable).

4. Certificate Life-Cycle Operational Requirements

This section addresses the administration of SSS Root CA's and Issuing CAs' Key Pairs throughout the operational life cycle of the Root CA and the Issuing CAs, including how

- the Public and Private Keys are generated and/or re-generated (i.e. re-keying)
- the Private Key(s) are stored, protected and eventually destroyed
- the Public Key(s) are distributed and archived.

This policy does not allow a certificate to be issued to multiple entities or to contain a public key whose associated private key is shared. Wildcard Certificates will only be permitted with special dispensation after the risk has been assessed. In the case of services such as Elastic Load-balanced (ELB) services Subject Alternative Names (SANs) should be used.

Application for Certificates issued under this policy may be submitted in person or via electronic means, as long as the identification and authentication requirements applicable to the assurance level of the certificates being requested are satisfied.

Bulk applications for Certificates issued under this policy are permitted, as long as the identification and authentication requirements applicable to the assurance level of the certificates being requested are satisfied.

4.1 Certificate Application

The Certificate application process must provide sufficient information to:

- Establish the applicant's authorization (by the employing or sponsoring organization) to obtain a certificate. (per Section 3.2.3)
- Establish and record identity of the applicant. (per Section 3.2.3)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required. (per Section 3.2.1)
- Verify any role or authorization information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for the CA and applicants that does not compromise security, but all must be completed before certificate issuance.

4.1.1 Who Can Submit a Certificate Application

A certificate application shall be submitted to the CA by the Subscriber, AOR, or an RA on behalf of the Subscriber. Multiple certificate requests from one RA or AOR may be submitted as a batch.

4.1.2 Enrolment Process and Responsibilities

All communications among PKI Authorities supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

Subscribers are responsible for providing accurate information on their certificate applications.

4.2 Certificate Application Processing

Information in certificate applications must be verified as accurate before certificates are issued. Procedures to verify information in certificate applications shall be specified in this policy.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the subscriber shall meet the requirements specified for subscriber authentication as specified in Sections 3.2 and 3.3.

4.2.2 Approval or Rejection of Certificate Applications

Any certificate application that is received by a CA under this policy, for which the identity and authorization of the applicant has been validated, will be duly processed. However, the CA shall reject any application for which such validation cannot be completed, or when the CA has cause to lack confidence in the application or certification process.

4.2.3 Time to Process Certificate Applications

The RA shall process certificate applications within 30 days of identity verification, after which the applicant shall be required to re-perform identity verification.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon receiving the application, the CAs/RAs shall:

- Verify the identity of the applicant as specified in Section 3.2.
- Verify the authority of the requester and the integrity of the information in the certificate request as specified in Section 4.1.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).
- Make the certificate available to the subscriber after confirming that the subscriber has formally acknowledged their obligations as described in Section 9.6.3.

The certificate request may already contain a to-be-signed certificate built by either the RA or the subscriber. This certificate shall not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction.

All authorization and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this policy shall inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber. For device certificates, the CA shall issue the certificate according to the certificate requesting protocol used by the device (this may be automated) and, if the protocol does not provide inherent notification, also notify the authorized organizational representative of the issuance (this may be in batch).

4.4 Certificate Acceptance

Before a subscriber can make effective use of its private key, the CA shall explain to the subscriber its responsibilities and obtain the subscriber's acknowledgement, as defined in Section 9.6.3.

4.4.1 Conduct Constituting Certificate Acceptance

Failure to object to the certificate or its contents shall constitute acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

Whether or not subscriber certificates are published to the publicly accessible Shadow Directory will be at the discretion of the customer Organisation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

PKI Authorities must be notified whenever a CA operating under this policy issues a CA certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key shall be specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Certificates may specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy shall issue CRLs specifying the current status of all unexpired certificates except for OCSP responder certificates. It is recommended that relying parties process and comply with this information whenever using certificates in a transaction.

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name and other information as the old one, but with a new key and extended validity period and a new serial number. Renewal of a certificate does not require a change to the *subjectName* and does not violate the requirement for name uniqueness.

An old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.1 Circumstance for Certificate Renewal

Any certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been revoked or compromised, and the Subscriber name and attributes are unchanged.

In addition, the validity period of the certificate must not exceed the remaining lifetime of the private key, as specified in Section 5.6. The identity proofing requirements listed in Section 3.3.1 shall also be met.

CA Certificates and OCSP responder certificates may be renewed as long as the aggregated lifetime of the public key does not exceed the certificate lifetime specified in Section 6.3.2.

The CA may renew previously-issued certificates during recovery from CA key compromise without subject request or approval as long as the CA is confident of the accuracy of information to be included in the certificates.

4.6.2 Who May Request Renewal

For all CAs and OCSP responders operating under this policy, the corresponding operating authority may request renewal of its own certificate. The Subscriber, RA, or AOR may request the renewal of a Subscriber certificate.

4.6.3 Processing Certificate Renewal Requests

Digital signatures on subscriber renewal requests shall be validated before electronic renewal requests are processed per Section 3.3. Alternatively, subscriber renewal requests may be processed using the same process used for initial certificate issuance.

4.6.4 Notification of New Certificate Issuance to Subscriber

The CA may inform the subscriber of the re-key of his or her certificates and contents of the certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.6.6 Publication of the Renewal Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate Re-key

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified. Subscribers shall identify themselves for the purpose of re-keying as required in section 3.3.

4.7.1 Circumstance for Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes its identity. A Certificate shall be re-Keyed prior to reaching the end of its validity period. Other examples of circumstances requiring certificate re-key include: suspected or actual loss / compromise, or upgrade of assurance level..

4.7.2 Who May Request Certification of a New Public Key

Requests for certification of a new public key shall be considered as follows:

- Subscribers with a currently valid certificate may request certification of a new public key.
- CAs and RAs may request certification of a new public key on behalf of a subscriber.

- For device, application/service, or role certificates, an AOR that owns or controls the device may request re-key.

4.7.3 Processing Certificate Re-keying Requests

Digital signatures on subscriber re-key requests shall be validated before electronic re-key requests are processed. Alternatively, subscriber re-key requests may be processed using the same process used for initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

The CA may inform the subscriber of the re-key of his or her certificates and contents of the certificate.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate.

4.7.6 Publication of the Rey-keyed Certificate by the CA

As specified in Section 2, all CA certificates shall be published in repositories. This policy makes no stipulation regarding publication of subscriber certificates.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Certificate modification means creating a new certificate that has the same key and a different serial number, and that it differs in one or more other fields, from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

4.8.1 Circumstance for Certificate Modification

A CA operating under this policy may modify a CA or OCSP responder certificate whose characteristics have changed (e.g. assert new policy OID). A CA may perform certificate modification for a subscriber whose characteristics have changed (e.g., name change due to marriage, or reorganisation resulting in a modified distinguished name).

4.8.2 Who May Request Certification Modification

Requests for certification of a new public key shall be considered as follows:

- Subscribers with a currently valid certificate may request certificate modification.
- CAs and RAs may request certificate modification on behalf of a subscriber.
- For device certificates, the Designated Certificate Holder of the device may request certificate modification.

4.8.3 Processing Certificate Modification Requests

A certificate modification shall be achieved using one of the following processes:

- Initial registration process as described in Section 3.2
- Identification & Authentication using a subscriber-signed certificate modification request, as described in Section 4.8.3. In addition, the validation of the changed subject information shall be in accordance with the initial identity-proofing process as described in Section 3.2

The RA shall complete all required re-verification prior to issuing the modified certificate

4.8.4 Notification of New Certificate Issuance to Subscriber

The CA may inform the subscriber of the re-key of his or her certificates and contents of the certificate.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

Failure to object to the certificate or its contents constitutes acceptance of the certificate

4.8.6 Publication of the Modified Certificate by the CA

As specified in Section 2, all CA certificates shall be published in repositories. This policy makes no stipulation regarding publication of subscriber certificates.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

CAs operating under this policy shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance and shall be readily available to any potential relying party.

Revocation requests must be authenticated.

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised. Certificate suspension for CA certificates is not allowed by this policy. However, the use of certificate suspension for end entity certificates is allowed.

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key contained within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding include:

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Any information in the certificate becomes invalid.
- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- There is reason to believe the private key has been compromised.
- The original certificate request was not authorized.
- The subscriber or other authorized party (as defined in this policy) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information at least until the certificates expire.

4.9.2 Who can Request Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation should subsequently be provided to the subscriber. The RA can request the revocation of a subscriber's certificate on behalf of any authorized party as specified in this policy. A subscriber may request that its own certificate be revoked. The AOR of the organization that owns or controls a device can request the revocation of the device's certificate. Other authorized individuals of the organization may request revocation as described in this policy.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). Only the PA may direct the OA to revoke certificates issued by the Root CA..

4.9.4 Revocation Request Grace Period

There is no grace period for certificate revocation under this Policy. The CA shall revoke certificates upon request as quickly as is practical upon receipt of a valid revocation request.

4.9.5 Time within which CA must Process the Revocation Request

CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published.

4.9.6 Revocation Checking Requirement for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the relying party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuing Frequency

CRLs shall be issued on a scheduled basis, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below. Certificate status information shall be published no later than the next scheduled update specified in the *nextUpdate* field of the previously issued CRL for same scope.

For SSS PKI Issuing CA , the CRL issuance frequency shall be at least once every 7 days.

CRLs for SSS PKI Root and Policy CA Certificates SHALL be updated and issued at least once every twelve (12) months.

4.9.8 Maximum Latency for CRLs

CRLs shall be published within 4 hours of generation.

4.9.9 On-line Revocation/Status Checking Availability

Where on-line status checking is supported, status information must be updated within 24 hours of certificate revocation. Since some relying parties cannot accommodate on-line communications, all CAs will be required to support CRLs.

4.9.10 On-line Revocation Checking Requirements

The SSS PKI Issuing CA SHALL support an OCSP capability using the GET method for certificates issued in accordance with RFC 6960.

For the status of Subscriber Certificates: The SSS PKI Issuing CA SHALL update information via OCSP at least every seven (7) days and the responses from this service MUST have a maximum expiration time of ten (10) days.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements re: Key Compromise

In the event of a CA private key compromise, the CA will follow the procedures outlined in Section 5.7.3.

4.9.13 Circumstances for Suspension

Not applicable. 4.9.14 Who Can Request Suspension

The SSS PA, SSS OA, or RA may request suspension of any Subscriber certificate issued by the CA. A Subscriber may request suspension of a certificate in which they are listed as the certificate subject.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

No applicable.

4.10 Certificate Status Services

4.10.1 Operational characteristics

The SSS Root CA shall issue direct, full and complete CRLs. Every CRL contains the serial numbers of all non-expired revoked certificates issued by the CA.

4.10.2 Service availability

The CRL shall be available for download 24x7 in an online repository that software applications can use to automatically check the current status of all unexpired certificates issued by the CA.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

Subscription is synonymous with the certificate validity period. The subscription ends when the certificate is revoked or expired. The Subscriber shall have a mechanism for notifying the CA to end subscription of their CA services. This shall follow the process for Key revocation outlined above in Section 4.9.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

Physical security controls shall be implemented that protect the PKI from unauthorised physical access to equipment, facilities, key material, information, and documents, and to safeguard them against espionage, sabotage, damage, tampering, theft, and other covert or overt acts. Physical security requirements imposed on CAs are likewise imposed on any RAs to the extent of their responsibilities and the level of sensitivity of the information they maintain.

5.1.1 Site Location and Construction

The location and construction of the facility housing the CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorised access to the CA equipment and records.

5.1.2 Physical Access

The CA equipment shall always be protected from unauthorised access, and especially while the cryptographic module is installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

Physical access controls and procedures shall be implemented to:

- Ensure that no unauthorized access to the hardware is permitted
- Manual or electronical monitoring for unauthorized intrusion at all times
- Ensure an access log is maintained and available for inspection
- Mandate at least two-person access requirements. Both people must hold trusted roles and at least one individual shall be a member of the CA Operations Staff. Technical or mechanical mechanisms (e.g., dual locks) shall be used to enforce the two-person physical access control
- Ensure that other individuals shall be escorted by two persons. This includes maintenance personnel. All individuals shall be recorded in the access log
- Ensure access to sensitive physical areas is denied Upon the permanent departure of trusted personnel

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules and CA equipment shall be placed in secure containers.

Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module and shall not be stored with the cryptographic module.

A security check of the facility housing the CA equipment shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation;
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorised access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last Authorised person to depart shall perform the

check and shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Power and air conditioning

The CA shall have backup power capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

5.1.4 Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water.

5.1.5 Fire Prevention and Protection

An automatic fire extinguishing system shall be installed in accordance with local policy and code.

5.1.6 Media Storage

CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit, archive, or backup information shall be duplicated and stored in a location separate from the CA.

5.1.7 Waste Disposal

Waste containing sensitive information shall be destroyed, such that the information is unrecoverable, prior to disposal. Media used to store sensitive data shall be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-Site Backup

Alternate facilities have been established for the storage and retention of PKI systems/data backups. The facilities are accessible by authorized personnel with physical security and environmental controls.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. Trusted role operations include:

- The validation, authentication, and handling of information in Certificate Applications
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrolment information
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository
- Access to safe combinations and/or keys to security containers that contain materials supporting production services
- Access to hardware security modules (HSMs), their associated keying material, and the secret share splits of the PINs that protect access to the HSMs
- Installation, configuration, and maintenance of the CA
- Access to restricted portions of the certificate repository
- The ability to grant physical and/or logical access to the CA equipment

Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. At a minimum the following roles will be used:

- **System Administrator** – Authorised to install, configure, and maintain the server operating system and other non-CA software packages; configure and maintain the networking operations; establish and maintain system accounts; and configure OS audit parameters.
- **Security Officer** – Authorised to configure the CA policies; configure audit parameters; and perform certificate lifecycle operations for Registration Authorities. Security Officers do not issue certificates to End User Subscribers.
- **Security Compliance Auditor** – Authorised to view, but not modify, audit logs, reports, the Security Policy, and user properties.
- **Master User** – Authorised to perform initial configuration of the CA; start and stop the CA services; and verify and backup the CA's database.
- **Registration Authorities** – Authorised to request or approve certificates or certificate revocations.
- **Compliance Auditors –** Authorised to audit the operational management and functions of the OA and RAs against this policy.

Multiple people may hold the same trusted role, with collective privileges sufficient to fill the role. CAs may use different titles to describe these roles, or break out the duties in different ways, as long as the requirements for separation duties are met (see Sections 5.2.2 and 5.2.4). Other trusted roles may be defined by the Organizational administering the PKI, in which case they will be described as additional subsections. The policy may further define these roles, as well as define additional Trusted Roles to provide further role separation, or to include repository responsibilities.

5.2.2 Number of Persons Required Per Task

Two or more persons are required for the following tasks:

- Generation, activation, and backup of CA keys
- Performance of CA administration or maintenance tasks
- Archiving or deleting CA audit logs. At least one of the participants shall serve in a Security Auditor role.
- Physical access to CA equipment
- Access to any copy of the CA cryptographic module
- Processing of third party key recovery requests

Where multiparty control is required, at least one of the participants shall be a System Administrator. All participants must serve in a trusted role as defined in section 5.2.1. Multiparty control shall not be achieved using personnel that serve in the Security Compliance Auditor trusted role.

5.2.3 Identification and Authentication for Each Role

An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Roles Requiring Separation of Duties

Individuals serving as Security Auditors shall not perform or hold any other trusted role. Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require multi-person control.

An individual that performs any trusted role shall only have one identity when accessing CA equipment.

5.3 Personnel Controls

Personnel Security plays a critical role in the CA facility's overall security system. Personnel Security shall be designed to prevent both unauthorized access to the CA facility and CA systems and compromise of sensitive CA operations by CA personnel.

Inadequate personnel security procedures or negligent enforcement of personnel security policies can pose potentially devastating threats to security. These threats can include unauthorized access, data loss and corruption, denial of service, and even facility sabotage and terrorism. Such events can erode or destroy customer confidence in the CA.

5.3.1 Qualifications, Experience, and Clearance Requirements

All persons filling Trusted Roles shall be selected on the basis of loyalty, trustworthiness, and integrity. Any personnel occupying a Trusted Role, as defined in 5.2.1, must possess suitable experience and be deemed qualified.

5.3.2 Background Check Procedures

On entering employment, a SSS employee must submit a background check which is to be renewed and resubmitted every two years. Persons external to the SSS may only enter CA service premises when accompanied by at least one authorized SSS employee. Background checks on persons external to SSS are the responsibility of the organizations employing them.

A background investigation shall cover the following areas:

- Employment;
- Education;

- Place of residence;
- Law Enforcement; and
- References.

If the trustworthiness of an individual filling a Trusted Role is questioned, the individual shall be removed from the sensitive position while the problem is being investigated. Based on the outcome of the investigation, the SSS OA may re-instate the individual in the Trusted Role or permanently remove them from their Trusted Role.

5.3.3 Training Requirements

All personnel performing duties with respect to the operation of the CA or RA shall receive comprehensive training. Training shall be conducted in the following areas:

- CA (or RA) security principles and mechanisms;
- All PKI software versions in use on the CA (or RA) system;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of this policy

5.3.4 Retraining Frequency and Requirements

Individuals responsible for CA roles shall be aware of changes in the CA operation. Any significant change to the operations shall include the appropriate training, and the training shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorised Actions

The OA shall take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or its repository not authorised in this policy or other procedures approved and published by the PA.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the CA shall meet applicable requirements as set forth in this policy. Contracts providing personnel that serve in the Trusted Roles defined in this CP shall explicitly cite compliance with this CP and other references necessary to ensure that personnel are contractually bound to serve in their roles responsibly.

5.3.8 Documentation Supplied to Personnel

Authorised PKI personnel will be provided with the policies, procedures and other relevant documentation that is necessary to perform their job functions

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CAs and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form such as a register, 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.

5.4.1 Types of Events Recorded

All security auditing capabilities of CA operating system and CA applications shall be enabled during installation. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;
- A success or failure indicator when executing the CA's signing process;
- A success or failure indicator when performing certificate revocation; and
- The identity of the entity and/or operator that caused the event

A message from any source requesting an action by the CA is an auditable event; the corresponding audit record must also include message date and time, source, destination, and contents.

The CA shall record the events identified in the list below. Where these events cannot be electronically logged, the CA shall supplement electronic audit logs with physical logs as necessary.

a. Security Audit
b. Identification and Authentication
c. Local Data Entry
d. Remote Data Entry
e. Data Export and Output
f. Key Generation
g. Private Key Load and Storage
h. Trusted Public Key Entry, Deletion and Storage
i. Secret Key Storage
j. Private and Secret Key Export
k. Certificate Registration
l. Certificate Revocation
m. Certificate Status Change Approval
n. CA Configuration
o. Account Administration
p. Certificate Profile Management
q. Revocation Profile Management
r. Certificate Revocation List Profile Management
s. Miscellaneous
t. Physical Access / Site Security
u. Anomalies

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed at least once every two months. At a minimum, a statistically significant set of security audit data generated by the CA, since the last review, shall be examined, as well as a reasonable search for any evidence of malicious activity. The OA shall explain all significant events in an audit log summary. At a minimum, review shall involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any logged alerts or irregularities that might have an impact on the overall security and/or trustworthiness of the PKI. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two months as well as being retained in the manner described below. The individual who removes audit logs from the CA system shall be an official different from the individuals who, in combination, command the CA signature key.

5.4.4 Protection of Audit Log

The audit process shall not be done by or under the control of the OA. CA system configuration and procedures must be implemented together to ensure that:

- only Authorised people have read access to the logs;
- only Authorised people may archive audit logs; and
- audit logs are not modified

The entity performing audit log archive need not have modify access, but procedures shall be implemented to protect archived data from destruction prior to the end of the audit log retention period (If a system over-writes audit logs after a given time, the audit log is not considered deleted or destroyed if the audit log has been backed up and archived). Audit logs shall be moved to a secure storage location separate from the CA equipment.

5.4.5 Audit Log Backup Procedures

The audit logs generated on the PKI equipment may be backed up on the same schedule as the rest of the data on the PKI equipment, but at a minimum must be backed up at least once per month. Audit log backups shall be moved at least once per month to a safe, secure storage location separate from the PKI equipment.

5.4.6 Audit Collection System (Internal vs. External)

There is no requirement for the audit log collection system to be external to the PKI equipment. Audit processes shall be invoked at system start-up and cease only at system shutdown. Should it become apparent that an automated audit system has failed, the PKI operation shall cease until the audit capability can be restored. The PA shall determine whether to resume operations.

5.4.7 Notification to Event-Causing Subject

This CP imposes no requirement to provide notice that an event was audited to the individual, Organisation, device, or application that caused the event. Real-time alerts are neither required nor prohibited by this policy.

5.4.8 Vulnerability Assessments

The OA shall perform routine self-assessments of security controls.

5.5 Records Archival

5.5.1 Types of Records Archived

CA archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive in accordance with this policy:

Data to be Archived

- CA accreditation (if applicable)
- This Certificate Policy and Certification Practice Statement
- Contractual obligations
- Other agreements concerning operations of the CA

- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued or published
- Record of Re-key
- All Audit Logs
- Revocation requests
- Subscriber identity data
- Subscriber agreements
- Documentation of receipt of tokens and/or certificates
- All ARLs and CRLs issued and/or published
- Other data or applications to verify archive contents
- Documentation required by compliance auditors

5.5.2 Retention Period for Archive

Archive data shall be retained for a minimum of 3 years. Archives of audit trail files shall be retained for at least seven (7) year(s) after any certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

No unauthorised user shall be permitted to write to, modify, or delete the archive. For the CA, archived records may be moved to another medium when Authorised by the OA. The contents of the archive shall not be released except as determined by the PA for the CA or as required by law. Records of individual transactions may be released upon request of any Subscribers involved in the transaction or their legally Recognised agents. Archive media shall be stored in a safe, secure storage facility separate from the CA.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

CA archive records shall be automatically time-stamped as they are created.

5.5.6 Archive Collection System (Internal or External)

Archive data shall be collected in the most expedient manner.

5.5.7 Procedures to Obtain and Verify Archive Information

Only SSS IT Security Specialists SHALL have access to primary and backup archives. SSS IT Security Specialists MAY, at its own discretion, release specific archived information, following a formal request from a Subscriber, a Relying Party, or an authorized agent thereof.

5.6 Key Changeover

To minimize risk from compromise of a CA's private signing key, that key may be changed often. From that time on, only the new key will be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected.

When a CA updates its private signature key and thus generates a new public key (and corresponding certificate), the CA shall notify all CAs, RAs, and Subscribers that rely on the CA's certificate that it has been changed. A CA that distributes self-signed certificates generates key rollover certificates, where the old public key signs the new private key, and vice versa. This permits acceptance of newly issued certificates

and CRLs without distribution of the new self-signed certificate to current users. For self-signed certificates, such certificates shall be conveyed to users in a secure fashion to preclude malicious substitution attacks.

5.7 Compromise and Disaster Recovery

The SSS CA shall have an Incident Response Plan and a Disaster Recovery Plan.

The CA and repository system shall be deployed to provide availability as determined by the criticality of the CA and its components. The CA shall implement features to provide high levels of reliability. The following subsections outline the policy for instances that may prevent such maintenance of reliability.

The CA shall have recovery procedures in place to reconstitute the CA in the event of a catastrophic failure, as described in the following subsections.

5.7.1 Incident and Compromise Handling Procedures

The SSS PA and OA shall be notified if any CAs operating under this policy experience any of the following:

- suspected or detected compromise of the CA systems;
- suspected or detected compromise of an Online Certificate Status Protocol server (OCSP) if
    - (1) the OCSP certificate has a lifetime of more than 2 weeks
- physical or electronic penetration of CA systems;
- successful denial of service attacks on CA components; or
- any incident preventing the CA from issuing a CRL prior to the time specified in the next update field of its currently valid ARL/CRL.

The SSS OA shall re-establish operational capabilities as quickly as possible.

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

If any of the CAs equipment is damaged or rendered inoperative, but the CA's signature keys are not destroyed, CA operation shall be re-established as quickly as possible, giving priority to the ability to generate certificate status information. The PA shall be notified as soon as possible.

5.7.3 Entity Private Key Compromise Procedures

In case of a CA key compromise, a superior CA shall revoke the compromised CA's certificate and the revocation information shall be published immediately in the most expedient manner. In the event that the revocation information cannot be published immediately, the CA shall securely notify all interested parties (including Subscribers and Subordinate CAs) at the earliest possible time.

Subsequently, the CA installation shall be re-established. The CA shall re-issue all CA certificates and Subscriber certificates. Subscriber certificates may be renewed automatically by the CA under the new key pair.

If the compromised CA is a Root CA, the trusted self-signed certificate shall be revoked and the new one distributed.

If the CA cannot issue an ARL/CRL prior to the time specified in the next update field of its currently valid ARL/CRL, then the OA shall be securely notified as soon as practical. The CA shall re-establish revocation capabilities as quickly as possible.

The PA shall be informed of the cause of failure and the expected time to restore and may make a determination as to any temporary or permanent actions to be taken on the assurance level assigned to the CA.

5.7.4 Business Continuity Capabilities after a Disaster

CAs shall be required to maintain a Disaster Recovery Plan. In the case of a disaster where the CA installation is physically damaged, and all copies of the CA signature key are destroyed as a result, the PA shall take whatever action it deems appropriate. In cases where CA operations are not impacted by such an event, through establishment of an alternative operational facility that offers the same security controls as the primary facility, the OA shall inform the PA of what services or capabilities, if any, will not be available until operations are restored to the primary facility. Further, the OA shall inform the PA of the expected time during which operations will remain at the alternate facility. Based on this information, the PA may choose to temporarily alter the assurance level at which the CA operates or other similar actions.

The CA Disaster Recovery Plan shall be coordinated with any overarching Disaster Recovery Plan that the broader organization may have. The Disaster Recovery Plan shall identify what procedures are in place to mitigate risks to environmental controls, procedures for annual testing of processes to restore service, individuals on call for this type of activity, and the order of restoral of equipment and services.

5.8 CA or RA Termination

In the event of termination of the CA operation, certificates signed by the terminated CA shall be revoked and all Subscribers promptly notified.

Prior to CA termination, the CA shall provide archived data to a PA approved archival facility.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation and Installation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used by a CA to sign certificates, CRLs or status information shall be generated in a FIPS 140 validated cryptographic module that meets or exceeds Security Level 2.

The SSS PKI SHALL have effective practices and controls in place to reasonably assure that the generation of Root and Policy CA key pairs are performed in a physically secured environment, and generate auditable evidence that the documented procedures were followed.

. The audit trail must identify and document any failures or anomalies in the key generation process, and any corrective actions taken. The documentation of the procedure must be detailed enough to show that appropriate role separation was used.

6.1.1.2 Subscriber Key Pair Generation

The Subscriber, CA, or RA may perform subscriber key pair generation. If the CA or RA generates Subscriber key pairs, the requirements for key pair delivery specified in this Policy must also be met. Key generation shall be performed using a FIPS approved method and shall take place within a FIPS 140 validated cryptographic module that meets or exceeds Security Level 3.

6.1.2 Private Key Delivery to Subscriber

A private key shall only be delivered to a Subscriber once the Subscriber is authenticated through means commensurate with the level of assurance of the certificate corresponding to the associated public key.

If subscribers generate their own key pairs, then there is no need to deliver private keys, and this section does not apply.

A private key shall not appear outside of the module it was generated in, unless it is encrypted. The encrypted private key may be output for local transmission or for storage by a key recovery mechanism.

In those cases where Subscriber key pairs (other than signature keys) are generated by the CA on behalf of the Subscriber, the private key shall be downloaded or retrieved by the Subscriber.. The delivery mechanism shall provide authentication and confidentiality commensurate with the strength of the cryptography offered by the key. In all cases, the following requirements must be met:

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber.
- The private key must be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct key pairs and activation data are provided to the correct Subscribers.
    - For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key.
- Activation data shall be delivered using a separate secure channel.

The CA must maintain a record of the Subscriber acknowledgement of receipt of the key pair.

6.1.3 Public Key Delivery to Certificate Issuer

Subscriber public signature keys shall be delivered to the CA in an authenticated manner done as part of a certificate request.

6.1.4 CA Public Key Delivery to Relying Parties

Each CA asserting this CP shall have its public key included in a certificate for use by Relying Parties. All CAs asserting this policy shall request a certificate from a CA Authorised to issue CA certificates.

This CP does not require CAs to provide for delivery of certificates to Relying Parties. Certificates shall contain information to aid relying parties in additional certificate retrievals, as described in this CP.

6.1.5 Key Sizes

This CP requires use of RSA PKCS#1 signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA or elliptic curve public keys.

All certificates that expire on or before December 31, 2030 shall contain subject public keys of at least 2048 bits for RSA and be signed with the corresponding private key.

All certificates that expire after December 31, 2030 shall contain subject public keys of at least 4096 bits for RSA, and be signed with the corresponding private key.

CAs that generate certificates and CRLs under this policy should use the SHA-256 hash algorithm when generating digital signatures. ECDSA signatures on certificates and CRLs shall be generated using SHA-256 as appropriate for the key length.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

The use of a specific key is determined by the key usage extension in the X.509 certificate. Public keys that are bound into human subscriber certificates may be used for signing, encrypting, or both. Certificates to be used for digital signatures shall set the *digitalsignature* bit; the nonrepudiation bit may be asserted only if the associated private key is not escrowed. Certificates to be used for encryption shall contain the key usage extension with: *keyEncipherment* bit set if the encryption algorithm is a key transfer algorithm such as RSA, or *keyAgreement* bit set if the encryption algorithm is a key agreement algorithm; such as Diffie Hellman or Elliptic Curve Diffie Hellman.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the *keyCertSign* bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the *cRLSign* bit. CA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses shall assert the *digitalSignature* and/or *nonRepudiation* bits.

Public keys that are bound into device certificates may be used for signing, encrypting, or both. Device certificates to be used for digital signatures (including authentication) shall assert the *digitalSignature* bit. Device certificates that contain RSA public keys that are to be used for key transport shall assert the *keyEncipherment* bit. Device certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the *keyAgreement* bit. Device certificates shall not assert the *nonRepudiation* bit.

The *dataEncipherment*, *encipherOnly*, and *decipherOnly* bits shall not be asserted in certificates issued under this policy.

Certificates asserting a purpose other than *keyEncipherment* or *keyAgreement* shall not have their corresponding private keys escrowed.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

SSS PKI CAs shall use a hardware cryptographic module validated to FIPS 140-2 Level 2 (or higher), or some other equivalent standard for signing operations.

6.2.2 Private key (n out of m) multi-person control

A minimum of two person control shall be established on any CA signature key for all purposes including activation and backup, and may be implemented as a combination of technical and procedural controls. Persons involved in management and use of CA private signing keys shall be designated as Authorised by the CA for this purpose. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

Under no circumstances shall signature keys used to support non-repudiation services be escrowed by a third-party.

6.2.4 Private Key Backup

CA private signature keys and subscriber private signatures keys shall not be archived. Subscriber key management (public encryption, public verification, and private decryption) keys may be archived (escrowed) to provide key recovery. Any escrowed keys must be protected with the same security mechanisms as the corresponding certificates.

6.2.4.1 Backup of CA Private Signature Key

The SSS PKI Root and Policy CA's private signature keys shall be backed up under the same multi-person control as the creation of the original signature key. At least one copy of the private signature key shall be stored off-site. All copies of the SSS PKI Root and Policy CA's private signature key is considered accountable material and protected in the same manner as the original.

6.2.4.2 Backup of Subscriber Private Signature Key

Backing up subscriber private signature keys is in the control of the subscriber and the protection of such keys is the sole and individual responsibility of the subscriber identified in the distinguished name or the Designated Device Holder for Device certificates.

6.2.4.3 Backup of Device, Application and Code Signing Private Keys

Device, application and code signing private keys may be backed up or copied but must be held under the control of the AOR. Backed up private keys shall not be stored in plaintext form outside the cryptographic module. Backup copies shall be controlled at the same security level as the original cryptographic module.

6.2.5 Private Key Archival

CA private signature keys and subscriber private signatures keys shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys shall be generated by and remain in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic token boundary. The CA private keys may be backed up in accordance with this CP. Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure. A private key shall only be inserted into a cryptographic module that meets the requirements of this CP and commensurate with the level of assurance asserted by the corresponding certificate.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in FIPS 140.

Subscriber's private keys must only be stored on the systems that actively uses the certificate tied to that private key.

6.2.8 Method of Activating Private Key

SSS PKI CA Root and Policy CA private keys shall be activated using FIPS 140-2 compliant hardware performed by multiple Trusted Role personnel.

6.2.9 Method of Deactivating Private Key

Private keys may be deactivated through any means defined by the cryptographic module provider. All cryptographic modules and/or controlling software shall include a timer which locks or deactivates private keys after a specified idle period. Hardware cryptographic modules shall deactivate private keys when disconnected from a power source.

6.2.10 Method of Destroying Private Key

Individuals in trusted roles shall destroy CA, RA, and CSS (e.g., OCSP server) private signature keys when they are no longer needed. Physical destruction of hardware is not required.

6.2.11 Cryptographic Module Rating

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Copies of CA and Subscriber certificates and Public Keys SHALL be archived in accordance with Section 5.5..

6.3.2 Certificate operational periods and key pair usage periods

The usage period for the Root CA key pair is a maximum of 20 years.

For all other CAs operating under this policy, the usage period for a CA key pair is a maximum of 15 years. The CA private key may be used to sign certificates for a maximum of 1 year, but may be used to sign CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

Subscriber public keys in certificates other than code signing certificates have a maximum usage period of 1 year. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.

Subscriber public keys in code signing certificates have a maximum usage period of 1 year. The private keys corresponding to the public keys in these certificates have a maximum usage period of 1 year. For OCSP responders operating under this policy, the maximum private key usage period is 2 weeks.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

SSS PKI CA shall protect activation data from compromise or disclosure. Appropriate cryptographic and physical access controls shall be implemented to prevent unauthorized use of any SSS PKI CA Private Key activation data..

6.4.2 Activation Data Protection

Data used to unlock SSS CA private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms.

6.4.3 Other Aspects of Activation Data

Approved cryptographic modules shall ensure that consecutive failed activation attempts result in either permanent lockout or erasure of private keys contained within the module.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The SSS PKI CA and its components shall include the following functionality:

- Require authenticated logins;
- Provide Discretionary Access Control;
- Provide a security audit capability;
- Restrict access control to CA services and PKI roles;
- Enforce separation of duties for PKI roles;
- Require identification and authentication of PKI roles and associated identities;
- Archive CA history and audit data;

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The System Development Controls for the CA and RA are as follows:

- Each CA shall use software that has been designed and developed under a formal, documented development methodology
- Hardware and software procured to operate each CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the CA physical location, handled under dual control and/or hashing for integrity upon receiving from vendor
- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software, which are not part of the CA operation
- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA shall be obtained, from sources Authorised by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically afterward
- Hardware and software updates shall be 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 SSS PKI CA system as well as any modifications and upgrades shall be documented and controlled.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

Many components of a CA are connected to each other and their customers via various forms of networks. While it is necessary for connections to customers and administrative systems, care needs to be taken to ensure those connections do not adversely impact the security of those components.

A network guard, firewall, or filtering router must protect network access to CA equipment. The network guard, firewall, or filtering router shall limit services allowed to and from the CA equipment to those required to perform CA functions.

Protection of CA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the CA equipment shall be necessary to the functioning of the CA application.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries SHALL contain time and date information.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

Each certificate issued by a CA shall be given a serial number consisting of a unique, positive integer, not longer than 20 octets. Each certificate issued by a CA shall be given a serial number consisting of a unique, positive integer, not longer than 20 octets.

7.1.1 Version Number(s)

The CA shall issue X.509 v3 certificates (version field populated with "V3").

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure yet be flexible enough to meet the needs of the various CAs and communities.

The key usage extension (*keyUsage*) shall be marked as critical. Certificates shall assert the minimum number of key usages required for functionality. Signature certificates shall assert *digitalSignature*. Encryption certificates shall assert either *keyEncipherment* or *keyAgreement*. CA certificates shall assert *keyCertSign* and *cRLSign*.

Certificates shall assert the minimum number of extended key usages (*extKeyUsage*) required for functionality. The *anyExtendedKeyUsage* key purpose shall not be asserted.

The basic constraints extension (*basicConstraints*) shall be marked critical in Device CA certificates, and the path length constraint should be set to 0.

The basic constraints extension (*basicConstraints*) shall be marked critical in General Purpose CA certificates, and the path length constraint should be set to 1.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use at least one the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512withRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
id-RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-Sha256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}
ecdsa-with-Sha384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}
sha256withDSA	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3)nistalgorithm(4) hashalgs(2) 1 }

The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter (for details, see [PKCS#1]). If certificates are issued under this CP using RSA-PSS, then the SHA-256 hash algorithm must be used when generating RSA-PSS signatures and the following OID shall be used to specify the hash in an RSA-PSS digital signature:

id-sha256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}

Certificates under this CP will use the following OIDs for identifying the algorithm for which the subject key was generated

Reference Certificate Policy (Draft)sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549)pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549)pkcs(1)pkcs-1(1) 12}
sha512withRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549)pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
id-RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549)pkcs(1) pkcs-1(1) 10}
ecdsa-with-Sha256	{iso(1) member-body(2)us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2}
ecdsa-with-Sha384sha256withDSA	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)csor(3)nistalgorithm(4) hashalgs(2) 1 }

7.1.4 Name Forms

Where required as set forth above, the subject field of the base certificate shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280. The issuer fields of certificates issued under the policies in this document shall be populated with an X.500 Distinguished Name, with the attribute type as further constrained by RFC 5280.

7.1.5 Name Constraints

CAs operating under this policy reserve the right to issue certificates with Name Constraints and mark them as critical where applicable.

7.1.6 Certificate Policy Object Identifier

Subordinate CA certificates and Subscriber end-user certificates issued in compliance with this CP shall assert the following OID in the certificate policies extension, as appropriate:

`1.3.6.1.4.1.58631.1.4.1`

7.1.7 Usage of Policy Constraints Extension

When included in a certificate, the *policyConstraints* extension shall be compliant with RFC 5280.

7.1.8 Policy Qualifiers Syntax and Semantics

When used, the *PolicyQualifiers* extension shall be populated and processed as described in RFC5280.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Critical extensions, when marked, shall be interpreted as defined in RFC 5280.

7.2 CRL Profile

All CRLs and ARLs shall be published in accordance with all requirements established by this Certificate Policy..

7.2.1 Version Numbers

The CAs operating under this policy shall issue X.509 version two (2) CRLs

7.2.2 CRL and CRL Entry Extensions

Not applicable.

7.3 OCSP Profile

7.3.1 Version number(s)

If OCSP is implemented, the OA shall document the applicable OCSP system version information.

7.3.2 OCSP Extensions.

All PKI software must correctly process all OCSP extensions identified in the OCSP Profile. The profile for OCSP responses conforms to RFC 5019 and RFC 6960 standards.

8 Compliance Audit and Other Assessment

All CAs operating under this policy shall have a compliance audit mechanism in place to ensure that the requirements of the policy are being implemented and enforced.

8.1 Frequency or circumstances of assessment

The CAs and RAs operating under this policy shall be subject to a periodic compliance audit which is no less frequent than once per year.

If no significant changes to policies, procedures or operations have occurred during the previous year, a delta compliance audit is acceptable in lieu of a full compliance audit. However, a full compliance audit is mandatory every third year, regardless.

The PA has the right to require periodic and aperiodic compliance audits or inspections of CAs or RAs to validate that the entities are operating in accordance with the security practices and procedures described in this policy. The PA shall state the reason for any aperiodic compliance audit.

8.2 Identity/Qualifications of Assessor

The compliance auditor must demonstrate competence in the field of compliance audits and must be thoroughly familiar with requirements that the PA imposes on the issuance and management of the SSS PKI certificates.

The OA shall be responsible for identifying and engaging a qualified auditor for auditing all aspects of this policy.

8.3 Assessor's Relationship to Assessed Entity

The compliance auditor for the SSS PKI either shall be a private firm that is independent from SSS IT Security Specialists, or it shall be sufficiently organisationally separated from the OA to provide an unbiased, independent evaluation. The PA shall determine whether a compliance auditor meets this requirement.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a CA and RA comply with all the requirements of the current version of this policy. All aspects of the CA and RA operation shall be subject to compliance audit inspections.

8.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the requirements of this policy and the design, operation, or maintenance of the CAs/RAs, the following actions shall be performed:

- The compliance auditor shall note the discrepancy
- The compliance auditor shall notify the parties identified in this Policy of the discrepancy and
- The party responsible for correcting the discrepancy shall propose a remedy, including expected time for completion, to the PA and the appropriate OA

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PA may decide to halt temporarily operation of the affected CA, to revoke a certificate issued by the CA, or take other actions it deems appropriate. The PA shall develop procedures for making and implementing such determinations.

8.6 Communication of Result

An Audit Compliance Report, including identification of corrective measures taken or being taken by affected parties, shall be provided to the PA as set forth in this policy. The PA may, at its discretion, require a special compliance audit to confirm the implementation and effectiveness of the remedy.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

SSS is entitled to charge Subscribers and End-Entities for the issuance, reissuance, management, rekey, and renewal of Certificates.

9.1.2 Certificate access fees

SSS may, in its discretion, charge a fee to make a Certificate available in a repository or available to a Relying Party

9.1.3 Revocation or status information access fees

SSS does not charge a fee for access to revocation or status information. SSS may, in its discretion, charge a fee to provide customized revocation or status information in non-standard formats.

9.1.4 Fees for other services

SSS IT Security Specialists does not charge a fee for access to this CP/CPS.

9.1.5 Refund policy

SSS may, in its discretion, develop a refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

Relying Parties and Subscribers are encouraged to maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention.

9.2.2 Other assets

Customers shall maintain adequate financial resources for their operations and duties and shall be able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Insurance or warranty coverage for end-entities

Not supported

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following Subscriber documentation shall be maintained in confidence.

- CA application records, whether approved or disapproved
- Certificate Application records
- Subscriber Agreement
- Private keys held by customers and subscribers and information needed to recover such Private Keys
- Transactional records
- Contingency planning and disaster recovery plans; and
- Security measures controlling the operations of CA hardware and software and the administration of Certificate services and designated enrolment services.

9.3.2 Information not within the scope of confidential information

Certificates, Certificate revocation and other status information, CA repositories and information contained within them SHALL NOT be considered Confidential/Private Information. Information not expressly deemed Confidential/Private Information under Section 9.3.1 shall be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to protect confidential information

SSS shall protect and secure confidential information from disclosure.

9.4 Privacy of personal information

9.4.1 Privacy plan

Any CA governed by this CP shall develop and publish a Privacy Plan or Privacy Policy, which shall be made available to CA participants such as Relying Parties, Subscribers, etc.

9.4.2 Information treated as private

Information about Subscribers that is not publicly available through the content of the issued Certificate and revocation or status information is treated as private.

9.4.3 Information not deemed private

Subscriber information issued in the Certificates, Certificate directory, and revocation or status information is not deemed private information, subject to applicable law.

9.4.4 Responsibility to protect private information

Recipients of private information shall secure it from unauthorized access and disclosure to third parties and shall comply with all applicable local privacy laws in their jurisdiction.

9.4.5 Notice and consent to use private information

Unless where otherwise stated in this CP/CPS, the applicable Privacy Policy, or by agreement, private information will not be used without the consent of the party to whom that information applies. This section is subject to applicable privacy laws.

9.4.6 Disclosure pursuant to judicial or administrative process

SSS shall be entitled to disclose Confidential/Private Information if, in good faith, SSS believes that:

- Disclosure is necessary in response to subpoenas and search warrants.
- Disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other information disclosure circumstances

Refer to section 9.4.6

9.5 Intellectual property rights

SSS retains all rights, title, and interest, including without limitation intellectual property rights to the following:

- This combined CP and CPS;
- Certificates;
- Revocation Information;
- Policies and procedures supporting the operation of the SSS PKI;
- Distinguished Names (DNs) used to represent entities within the SSS PKI Services CA hierarchy; and
- CA infrastructure and Subscriber key pairs

9.6 Representations and warranties

9.6.1 CA representations and warranties

SSS IT Security Specialists warrants that, to the best of SSS IT Security Specialists' knowledge:

- There are no material misrepresentations of fact with the Certificates.
- There are no errors in the information within the Certificates caused by SSS IT Security Specialists' failure to exercise reasonable care in approving, creating, issuing, and managing the Certificates.
- The Certificates comply with the material requirements of this policy; and
- SSS IT Security Specialists' revocation services comply with this policy.

9.6.2 RA representations and warranties

RAs warrants that, to the best of their knowledge:

- There are no material misrepresentations of fact with the Certificates;
- There are no errors in the information within the Certificates caused by the RAs failure to exercise reasonable care in approving, creating, issuing, and managing the Certificates;
- The certificates comply with the material requirements of this policy; and

9.6.3 Subscriber representations and warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created.
- Their private key is protected, and that no unauthorized person has ever had access to the Subscriber's private key;

- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true;
- All information supplied by the Subscriber and contained in the Certificate is true;
- The Certificate is being used exclusively for authorized and legal purposes consistent with this CP/CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.
- No subscriber private key associated with any certificate issued within the SSS public key infrastructure shall be used to affix a digital signature to any document, contract, or letter.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying party representations and warranties

Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences and liability of their failure to perform the Relying Party obligations in terms of this CP/CPS. In no event shall a Relying Party construe a signature affixed to any document or message, that has been created utilising a private key corresponding to a SSS PKI CA issued certificate, as legally binding. Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and warranties of other participants

Not applicable.

9.7 Disclaimers of warranties

Except for express warranties stated in this CP/CPS, SSSIT Security Specialists disclaims all other warranties, promises and other obligations. In addition, SSS is not liable for any loss:

- To CA or RA services due to war, natural disasters or other uncontrollable forces;
- Incurred between the time a Certificate is revoked and the next scheduled issuance of revocation or status information;
- Due to unauthorized use of Certificates issued by SSS PKI, or use of Certificates beyond the prescribed use defined by this CP/CPS;
- Arising from the negligent or fraudulent use of Certificates or revocation or status information issued by SSS PKI; and
- Due to disclosure of personal information contained within Certificates, revocation or status information responses.

9.8 Limitations of liability

NOTHING HEREIN LIMITS LIABILTY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM SSS IT SECURITY SPECIALISTS' NEGLIGENCE OR (II) FRAUD COMMITTED BY SSS IT SECURITY SPECIALISTS'. EXCEPT AS STATED ABOVE, ANY ENTITY USING A SSS PKI CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF SSS RELATED TO SUCH USE, PROVIDED THAT SSS IT SECURITIES SPECIALISTS' HAS MATERIALLY COMPLIED WITH THIS POLICY IN PROVIDING THE CERTIFICATE OR SERVICE. Subscriber agreements and agreements with relying parties may contain different limitations on liability, in which case the agreement controls.

All liability is limited to actual and legally provable damages. SSS IT Security Specialists' is not liable for:

1. Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if SSS is aware of the possibility of such damages;
2. Liability related to fraud or wilful misconduct of the Applicant;
3. Liability related to use of a certificate that exceeds the limitations on use, value, or transactions as stated either in the certificate or this CP/CPS;
4. Liability related to the security, usability, or integrity of products not supplied by SSS IT Security Specialists, including the Subscriber's and Relying Party's hardware; or
5. Liability related to the compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether SSS failed to follow any provision of this CP/CPS, or (v) whether any provision of this CP/CPS was proven ineffective.

The disclaimers and limitations on liabilities in this CP/CPS are fundamental terms to the use of SSS IT Security Specialists' certificates and services.

9.9 Indemnities

9.9.1 Indemnification by SSS IT Security Specialists

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, SSS IT Security Specialists understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with SSS IT Security Specialists do not assume any obligation or potential liability of SSS IT Security Specialists under this CP/CPS or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. SSS IT Security Specialists shall not be liable to Application Software Supplier for any claim, damages, or loss suffered by an Application Software Supplier related to a Certificate issued by SSS IT Security Specialists where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from SSS online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify SSS IT Security Specialists and its affiliates (including, but not limited to, its parent company, officers, directors, employees, agents, partners, successors and assigns) against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CP/CPS, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of the Certificate or Private Key.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify SSS IT Security Specialists and its affiliates (including, but not limited to, its parent company, officers, directors, employees, agents, partners, successors and assigns) 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 CP/CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

The applicable Subscriber and/or Relying Party Agreements may set forth additional indemnity obligations.

9.10 Term and termination

9.10.1 Term

This CP/CPS, and any amendments thereto, are effective upon publication in SSS IT Security Specialists' Repository.

9.10.2 Termination

This CP/CPS, as may be amended from time to time, are effective until replace by a new version, which shall be published in in SSS IT Security Specialists Repository.

9.10.3 Effect of termination and survival

Upon termination of this CP/CPS, customers, Subscribers, and Relying Parties are bound by its terms for all Certificates issued, while it's effective, for the remainder of the validity periods of such Certificates.

9.11 Individual notices and communications with participants

SSS IT Security Specialists, Subscribers, Applicants, Relying Parties and other participants will use commercially reasonable methods to communicate with each other.

9.12 Amendments

9.12.1 Procedure for amendment

This CP/CPS is periodically reviewed and updated by the SSS IT Security Specialists. Controls are in place to reasonably ensure that this CP/CPS is not amended and published without the prior authorization of SSS IT Security Specialists.

9.12.2 Notification mechanism and period

SSS IT Security Specialists reserves the right to amend this policy document without notification for amendments that are not material. SSS IT Security Specialists' decision to designate an amendment's materiality shall be within the sole discretion of SSS IT Security Specialists. Updates, amendments, and new versions of the SSS IT Security Specialists certificate policies shall be posted in SSS IT Security Specialists' repository. Such publication shall serve as notice to all relevant entities.

9.12.3 Circumstances under which OID must be changed

SSS IT Security Specialists is solely responsible for determining whether an amendment to the CP/CPS requires an OID change upon the notification from relevant policy management authorities.

9.13 Dispute resolution provisions

Parties are required to notify SSS and attempt to resolve disputes directly with SSS before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14 Governing law

The laws of New Zealand govern the interpretation, construction, and enforcement of this CP/CPS and all proceedings related to SSS IT Security Specialists products and services, including tort claims, without regard to any conflicts of law principles. Applicants, Subscribers, and Relying Parties irrevocably consent to jurisdiction in New Zealand.

9.15 Compliance with applicable law

This CP/CPS is subject to all applicable laws and regulations, including New Zealand restrictions on the export of software and cryptography products.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CP/CPS and the applicable Subscriber Agreement and Relying Party Agreement represent the entire agreement between any Subscriber or Relying Party and SSS and shall supersede any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CPS and any other express agreement between a Subscriber or Relying Party with SSS with respect to a Certificate, including but not limited to a Subscriber Agreement, and Relying Party such other agreement shall take precedence.

9.16.2 Assignment

Any entities operating under this CP/CPS may not assign their rights or obligations without the prior written consent of SSS IT Security Specialists. Unless specified otherwise in a contract with a party, SSS IT Security Specialists does not provide notice of assignment. This CP/CPS shall be binding on all successors of the parties.

9.16.3 Severability

If any provision of this policy shall be held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of this policy shall remain in full force and effect.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

The waiver or failure to exercise any right provided for in this policy shall not be deemed a waiver of any further or future right under this policy.

9.16.5 Force Majeure

SSS IT Security Specialists' is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond SSS IT Security Specialists' reasonable control.

9.17 Other provisions

No stipulation unless otherwise specified in the relevant legal agreements.