



INTERMEDIARY CA CERTIFICATE POLICY

Document Classification:

Public

Version Number: 2.0

Issue Date: 15 June 2022

Document Reference

Item	Description
Document Title:	Sirar Intermediary CA Certificate Policy
Custodian Department:	Sirar's Product Management
Owner:	Sirar's Policy Authority
Version Number:	2.0
Document Status:	Final

Document Author: Sirar's Policy Authority

PKI Consultant



Signature/Date

Approved by: Fahad I. Aljutaily

Sirar CEO

Signature/Date

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	July 2019	K Hlabathi	Initial Draft
1.1	August 2019	K Hlabathi	Final Draft
1.2	September 2019	M de Waal, K Hlabathi	Final Draft after reviews
1.3	September 2019	K Hlabathi	Final draft incorporating NCDC comments
1.4	03 October 2019	K Hlabathi	Final incorporating second Deloitte Review. Split CP documents per CA Moved Certificate profiles to CPS
1.5	05 November 2019	K Hlabathi	Final for NCDC submission post review. Updated the CA key sizes to 4096 after discussion with NCDC
1.6	18 December 2019	K Hlabathi	Final for signature
1.7	22/07/2020	STCS Policy Authority	Updates based on regular review
1.8	17/08/2020	STCS Policy Authority	Addressing the comments received during the period of time audit
1.9	09/09/2020	STCS Policy Authority	Addressing the comments received from NCDC
1.10	30/09/2021	Solutions' Policy Authority	Annual review
2.0	15/06/2022	Sirar's Policy Authority	Document issuance under Sirar's name

Document Control

This document shall be reviewed annually and an update by Sirar may occur earlier if internal or external influences affect its validity.

The Digitally Signed Copy of this document shall be stored at the Sirar's PKI Repository.

Table of Contents

1. Introduction.....	10
1.1 Overview	11
1.1.1 Certificate Policy.....	11
1.1.2 Relationship between the CP and the CPS	11
1.1.3 Interaction with other PKIs	12
1.1.4 Scope.....	12
1.2 Document Name and Identification	12
1.3 PKI Participants	12
1.3.1 Certification Authorities	12
1.3.2 Registration Authorities	13
1.3.3 Subscribers	13
1.3.4 Relying Parties	13
1.3.5 Other participants.....	14
1.4 Certificate Usage.....	14
1.4.1 Appropriate Certificate Uses	14
1.4.2 Prohibited Certificate Uses	14
1.5 Policy Administration.....	14
1.5.1 Organization Administering the Document	14
1.5.2 Contact Person.....	14
1.5.3 Person Determining CPS Suitability for the Policy.....	15
1.5.4 CPS Approval Procedures.....	15
1.6 Definitions and Acronyms	15
2. Publication and Repository Responsibilities	19
2.1 Repositories	19
2.2 Publication of Certification Information.....	19
2.2.1 Publication of Certificates and Certificate Status	19
2.2.2 Publication of CA Information.....	19
2.2.3 Interoperability	19
2.3 Time or Frequency of Publication	19
2.4 Access Controls on Repositories.....	20
3. Identification and Authentication.....	21
3.1 Naming	21
3.1.1 Types of Names	21
3.1.2 Need for Names to be Meaningful.....	21
3.1.3 Anonymity or Pseudonymity of Subscribers.....	21
3.1.4 Rules for Interpreting Various Name Forms	21
3.1.5 Uniqueness of Names	21
3.1.6 Recognition, Authentication, and Role of Trademarks	21
3.2 Initial Identity Validation	21
3.2.1 Method to Prove Possession of Private Key.....	21
3.2.2 Authentication of organizational entity	22
3.2.3 Identity-Proofing of Individual Identity	22
3.2.4 Non-verified Subscriber Information.....	22
3.2.5 Validation of Authority.....	22
3.2.6 Criteria of Interoperation	22

3.3	Identification and Authentication for Re-key Requests	22
3.3.1	Identification and Authentication for Routine Re-Key	22
3.3.2	Identification and Authentication for Re-key After Revocation	22
3.4	Identification and Authentication for Revocation Requests	22
4.	<i>Certificate Life-Cycle Operational Requirements</i>	23
4.1	Certificate Application.....	23
4.1.1	Who Can Submit a Certificate Application.....	23
4.1.2	Enrollment Process and Responsibilities	23
4.2	Certificate Application Processing.....	23
4.2.1	Performing Identification and Authentication Functions	23
4.2.2	Approval or Rejection of Certificate Applications	23
4.2.3	Time to Process Certificate Applications	23
4.3	Certificate Issuance	24
4.3.1	CA Actions During Certificate Issuance	24
4.3.2	Notification of Certificate Issuance	24
4.4	Certificate Acceptance	24
4.4.1	Conduct Constituting Certificate Acceptance.....	24
4.4.2	Publication of the Certificate by the CA	24
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	24
4.5	Key Pair and Certificate Usage	24
4.5.1	Private Key and Certificate Usage.....	24
4.5.2	Relying Party Public Key and Certificate Usage	24
4.6	Certificate Renewal.....	25
4.6.1	Circumstances for Certificate Renewal.....	25
4.6.2	Who may request Certificate Renewal.....	25
4.6.3	Processing Certificate Renewal Requests	25
4.6.4	Notification of Renewed Certificate Issuance	25
4.6.5	Conduct constituting acceptance of a renewal certificate	25
4.6.6	Publication of a Renewal Certificate	25
4.6.7	Notification of Certificate Issuance by the CA to Other Entities	26
4.7	Certificate Re-Key	26
4.7.1	Circumstances for Certificate Re-key.....	26
4.7.2	Who can Request a Certificate Re-key.....	26
4.7.3	Processing Certificate Re-keying Requests.....	26
4.7.4	Notification of New Certificate Issuance to Subscriber.....	26
4.7.5	Conduct Constituting Acceptance of a Re-keyed Certificate.....	26
4.7.6	Publication of the Re-keyed Certificate by the CA	26
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	26
4.8	Certificate Modification	27
4.9	Certificate Revocation and Suspension	27
4.9.1	Circumstance for Revocation of a Certificate.....	27
4.9.2	Who Can Request Revocation of a Certificate	27
4.9.3	Procedure for Revocation Request	28
4.9.4	Revocation Request Grace Period.....	28
4.9.5	Time within which CA must Process the Revocation Request.....	28
4.9.6	Revocation Checking Requirements for Relying Parties	28
4.9.7	CRL Issuance Frequency.....	28
4.9.8	Maximum Latency of CRLs.....	28
4.9.9	Online Revocation Checking Availability	28
4.9.10	Online Revocation Checking Requirements.....	28

4.9.11	Other Forms of Revocation Advertisements Available	28
4.9.12	Special Requirements Related To Key Compromise	29
4.9.13	Circumstances for Certificate Suspension.....	29
4.9.14	Who Can Request Suspension	29
4.9.15	Procedure for Suspension Request.....	29
4.9.16	Limits on Suspension Period.....	29
4.9.17	Circumstances for Terminating Suspended Certificates	29
4.9.18	Procedure for Terminating the Suspension of a Certificate	29
4.10	Certificate Status Services	29
4.10.1	Operational Characteristics.....	29
4.10.2	Service Availability	29
4.10.3	Optional Features.....	30
4.11	End of Subscription.....	30
4.12	Key Escrow and Recovery.....	30
5.	Facility Management and Operational Controls.....	31
5.1	Physical Security Controls	31
5.1.1	Site Location and Construction	31
5.1.2	Physical Access	31
5.1.3	Power and Air Conditioning	31
5.1.4	Water Exposure.....	32
5.1.5	Fire Prevention and Protection.....	32
5.1.6	Media Storage	32
5.1.7	Waste Disposal.....	32
5.1.8	Off-Site Backup	32
5.2	Procedural Controls	32
5.2.1	Trusted Roles	32
5.2.2	Number of Persons Required per Task	33
5.2.3	Identification and Authentication for Each Role.....	33
5.2.4	Separation of Roles	33
5.3	Personnel Controls.....	33
5.3.1	Qualifications, Experience And Clearance Requirements.....	33
5.3.2	Background Check and Clearance Procedures	33
5.3.3	Training Requirements	34
5.3.4	Retraining Frequency and Requirements.....	34
5.3.5	Job Rotation Frequency and Sequence	34
5.3.6	Sanctions for Unauthorized Actions	34
5.3.7	Contracting Personnel Requirements	34
5.3.8	Documentation Supplied to Personnel.....	34
5.4	Audit Logging Procedures	35
5.4.1	Types of Events Recorded	35
5.4.2	Frequency of Processing Data.....	36
5.4.3	Retention Period for Audit Log	36
5.4.4	Protection of Audit Log	37
5.4.5	Audit Log Backup Procedures.....	37
5.4.6	Audit Collection System (Internal or External)	37
5.4.7	Notification to Event-Causing Subject.....	37
5.4.8	Vulnerability Assessments	37
5.5	Records Archival	37
5.5.1	Types of Events Archived	37
5.5.2	Retention Period for Archive.....	38
5.5.3	Protection of Archive.....	38

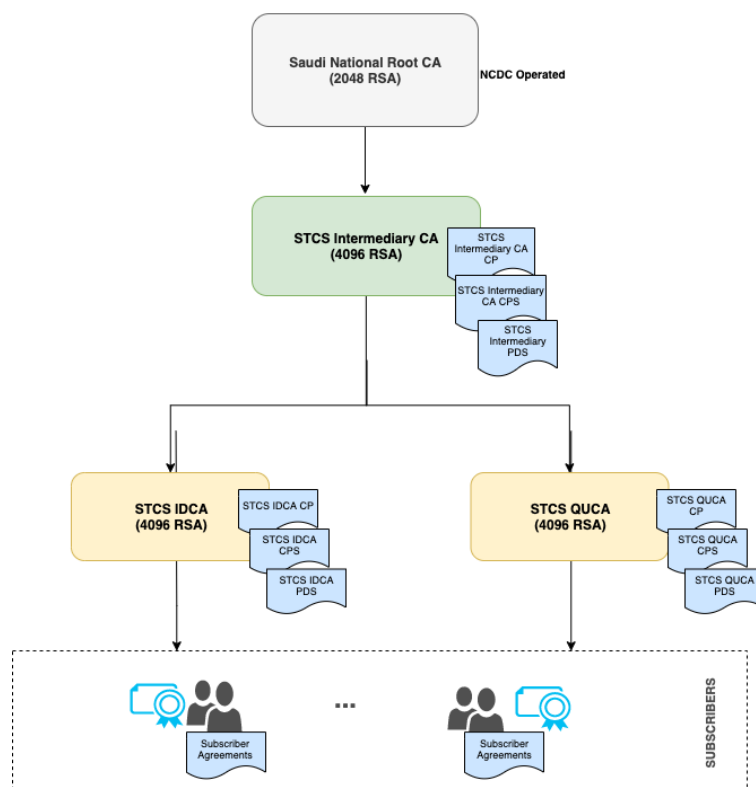
5.5.4	Archive Backup Procedures	39
5.5.5	Requirements for Time-Stamping of Records	39
5.5.6	Archive Collection System (Internal or External)	39
5.5.7	Procedures to Obtain and Verify Archive Information	39
5.6	Key Changeover.....	39
5.7	Compromise and Disaster Recovery.....	39
5.7.1	Incident and Compromise Handling Procedures.....	39
5.7.2	Computing Resources, Software, and/or Data Are Corrupted	39
5.7.3	CA Private Key Compromise Recovery Procedures	40
5.7.4	Business Continuity Capabilities after a Disaster	40
5.8	CA Termination	40
6.	Technical Security Controls.....	41
6.1	Key Pair Generation and Installation.....	41
6.1.1	Key Pair Generation	41
6.1.2	Private Key Delivery to Subscribers.....	41
6.1.3	Public Key Delivery to Certificate Issuer.....	41
6.1.4	CA Public Key Delivery to Relying Parties	41
6.1.5	Key Sizes	41
6.1.6	Public Key Parameters Generation and Quality Checking	42
6.1.7	Key Usage Purposes	42
6.2	Private Key Protection and Crypto-Module Engineering Controls.....	42
6.2.1	Cryptographic Module Standards and Controls.....	42
6.2.2	CA Private Key Multi-Person Control.....	42
6.2.3	Private Key Escrow.....	42
6.2.4	Private Key Backup	43
6.2.5	Private Key Archival.....	43
6.2.6	Private Key Transfer Into or From a Cryptographic Module	43
6.2.7	Private Key Storage on Cryptographic Module	43
6.2.8	Method of Activating Private Keys	43
6.2.9	Methods of Deactivating Private Keys	43
6.2.10	Methods of Destroying Private Keys	43
6.2.11	Cryptographic Module Rating	44
6.3	Other Aspects of Key Pair Management.....	44
6.3.1	Public Key Archive	44
6.3.2	Certificate Operational Periods and Key Usage Periods	44
6.4	Activation Data.....	44
6.4.1	Activation Data Generation and Installation	44
6.4.2	Activation Data Protection	44
6.4.3	Other Aspects of Activation Data.....	44
6.5	Computer Security Controls.....	45
6.5.1	Specific Computer Security Technical Requirements	45
6.5.2	Computer Security Rating.....	45
6.6	Life-Cycle Security Controls	45
6.6.1	System Development Controls.....	45
6.6.2	Security Management Controls.....	45
6.6.3	Life Cycle Security Ratings.....	45
6.7	Network Security Controls	46
6.8	Time Stamping	46
7.	Certificate, CRL and OCSP Profiles.....	47

7.1	Certificate Profile	47
7.1.1	Version Numbers	47
7.1.2	Certificate Extensions.....	47
7.1.3	Algorithm Object Identifiers.....	47
7.1.4	Name Forms	47
7.1.5	Name Constraints	47
7.1.6	Certificate Policy Object Identifier.....	47
7.1.7	Usage of Policy Constraints Extension.....	47
7.1.8	Policy Qualifiers Syntax and Semantics	48
7.1.9	Processing Semantics for the Critical Certificate Policy Extension	48
7.2	CRL Profile.....	48
7.2.1	Version Numbers	48
7.2.2	CRL and CRL Entry Extensions.....	48
7.3	OCSP Profile.....	48
7.3.1	Version Number	48
7.3.2	OCSP Extensions	48
8.	Compliance Audit and Other Assessments	49
8.1	Frequency of Audit or Assessments	49
8.2	Identity and Qualifications of Assessor	49
8.3	Assessor's Relationship to Assessed Entity.....	49
8.4	Topics Covered By Assessment	49
8.5	Actions Taken As A Result of Deficiency.....	50
8.6	Communication of Results.....	50
9.	Other Business and Legal Matters	51
9.1	Fees	51
9.1.1	Certificate Issuance/Renewal Fee	51
9.1.2	Certificate Access Fees	51
9.1.3	Revocation or Status Information Access Fee	51
9.1.4	Fees for Other Services	51
9.1.5	Refund Policy.....	51
9.2	Financial Responsibility.....	51
9.2.1	Insurance Coverage	51
9.2.2	Other Assets	51
9.2.3	Insurance/warranty Coverage for End-Entities.....	51
9.3	Confidentiality of Business Information	52
9.3.1	Scope of Confidential Information	52
9.3.2	Information not within the Scope of Confidential Information	52
9.3.3	Responsibility to Protect Confidential Information.....	52
9.4	Privacy of Personal Information	52
9.4.1	Privacy Plan	52
9.4.2	Information Treated as Private.....	52
9.4.3	Information not Deemed Private	52
9.4.4	Responsibility to Protect Private Information	53
9.4.5	Notice and Consent to Use Private Information	53
9.4.6	Disclosure Pursuant to Judicial/Administrative Process	53
9.4.7	Other Information Disclosure Circumstances	53
9.5	Intellectual Property Rights.....	53

9.6	Representations and Warranties	53
9.6.1	CA Representations and Warranties.....	53
9.6.2	RA Representations and Warranties.....	54
9.6.3	Relying Parties Representations and Warranties	54
9.6.4	Subscriber Representations and Warranties	54
9.6.5	Representations and Warranties of other participants	54
9.7	Disclaimers of Warranties	54
9.8	Limitations of Liability.....	55
9.9	Indemnities	55
9.10	Term and Termination	56
9.10.1	Term	56
9.10.2	Termination	56
9.10.3	Effect of Termination and Survival.....	56
9.11	Individual Notices and Communications with Participants	56
9.12	Amendments	56
9.12.1	Procedure for Amendment.....	56
9.12.2	Notification Mechanism and Period	56
9.12.3	Circumstances under which OID must be changed	57
9.13	Dispute Resolution Procedures.....	57
9.13.1	Dispute Resolution Committee	57
9.13.2	Dispute Resolution Policy.....	57
9.14	Governing Law	57
9.15	Compliance with Applicable Law.....	57
9.16	Miscellaneous Provisions.....	57
9.16.1	Entire Agreement	57
9.16.2	Assignment.....	57
9.16.3	Severability	57
9.16.4	Enforcement (Attorney Fees/Waiver of Rights)	58
9.16.5	Force Majeure	58
9.17	Other Provisions	58
9.17.1	Fiduciary Relationships	58
9.17.2	Administrative Processes	58

Sirar, a subsidiary of the Saudi Telecommunications Company (STC) that owns and operates a Public Key Infrastructure (PKI) under the Saudi National PKI. Sirar's PKI has core offerings of digital trust services designed to enable electronic signature and authentication services for business entities and individuals.

- STCS Qualified Certificate Authority (STCS QUCA) and
- STCS Identity Certificate Authority (STCS IDCA)



This CP shall define the policies by which the Intermediary CA operates. This CP complies with the following requirements:

- Saudi National PKI Policy,
- Saudi National Root CA CPS,
- RFC3647 — Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Sections that are not applicable to the QUCA are labelled “No Stipulation”. Where necessary, additional information is presented in subsections to the standard structure,
- RFC5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,
- Current version of the AICPA/CICA, WebTrust Principles and Criteria for Certification Authorities v2.2, and
- Adobe Approved Trust List (AATL) Certificate policies.

1.1 OVERVIEW

This CP defines a high level of trust and assurance for use by all the Intermediary CA PKI participants.

The Intermediary CA is an intermediate CA that issues certificates to approved Level-2 Issuing CAs and supportive functions for the Intermediary CA operations and Certificate Revocation Lists (CRLs). Different Subscriber type certificates based on the business requirement will be issued from the level 2 Issuing CAs.

This CP has been developed under the direction of the Sirar’s Policy Authority (PA) who has the responsibility for directing the development, seek approval and update of this Intermediary CA CP.

Any use of or reference to this CP outside the context of the Intermediary CA and Saudi National PKI is completely at the using party’s risk.

It is the responsibility of all parties applying for or using a Digital Certificate issued under this CP, to read this CP and the Intermediary CA CPS (hereinafter, the CPS) to understand the practices established for the lifecycle management of the Certificates issued by the Intermediary CA. Any application for Digital Certificates or reliance on validation services of the Intermediary CA issued Certificates signifies understanding and acceptance of this CP as well as the CPS.

1.1.1 CERTIFICATE POLICY

X.509 certificates issued by the STCS Intermediary CA to the Issuing CAs will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party (RP) to decide whether a certificate is trusted for a particular purpose.

1.1.2 RELATIONSHIP BETWEEN THE CP AND THE CPS

This CP states what assurance can be placed in a certificate issued by the Intermediary CA to the Issuing CAs participating in the Saudi National PKI. The Certificate Practice Statement (CPS) states how the Intermediary CA meets the requirements of this CP.

The CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by the Intermediary CA as governed by this CP and related documents which describe Sirar’s PKI requirements and use of Certificates.

1.1.3 *INTERACTION WITH OTHER PKIs*

The Intermediary CA will not be cross certified with other CAs, it will only be chained to the NCDC Root CA.

1.1.4 *SCOPE*

This CP applies to all certificates issued by the Intermediary CA. The Intermediary CA operates under the Saudi National PKI hierarchy and owned by Sirar. The Intermediary CA is an offline CA, that issues certificates to the approved Issuing CAs, that in turn issue subscriber certificates.

1.2 *DOCUMENT NAME AND IDENTIFICATION*

This document is the Intermediary CA Certificate Policy (CP), and is identified by the object identifier (OID):

OID: 2.16.682.1.101.5000.1.4.1.2.1.1

1.3 *PKI PARTICIPANTS*

The following are subcomponents of the Intermediary CA governed under this CP.

Several parties constitute the participants of the Intermediary CA. The parties mentioned hereunder including the Certification Authorities, the Sirar's PKI Committee (hereinafter, the PKI Committee), subscribers and relying parties are collectively called PKI participants.

1.3.1 *CERTIFICATION AUTHORITIES*

Sirar's PKI is an umbrella term referring to Sirar as an organization that runs PKI services under the Saudi National Root CA. Sirar's PKI implements a Two-tier PKI Architecture consisting of an offline intermediary CA (STCS intermediary CA), and two Issuing CAs under it, these being the STCS Identity CA (IDCA) and the STCS Qualified CA (QUCA). These Issuing CAs issue subscriber certificates, OCSP responder, timestamping certificates and other certificates required by the internal PKI components. The Issuing CAs issue certificates to Subscribers in accordance with each respective CP and the CPS, their RA Agreement, Subscriber Agreement, Relying Party Agreement, and the Saudi National PKI Policy.

Sirar as an entity is responsible for:

- Control over the designation of RAs;
- Conduct regular internal security audits;
- Assist in audits conducted by or on behalf of NCDC; and
- Performance of all aspects of the services, operations and infrastructure related to Sirar's PKI.

1.3.1.1 *SAUDI NATIONAL ROOT CA*

The Saudi National Root CA is the trust anchor for the entire Saudi National PKI. It is self-signed CA and operated by NCDC.

1.3.1.2 STCS INTERMEDIARY CA

The Intermediary CA is an offline CA that is chained to the Saudi National Root. It issues certificates to the Issuing CAs (STCS QUCA and STCS IDCA) underneath in the PKI hierarchy.

1.3.1.3 STCS QUALIFIED CA (QUCA)

The STCS QUCA is an issuing Certificate Authority under the Intermediary CA. It issues certificates for the Digital Trust Services, i.e., digital signature certificates.

1.3.1.4 STCS IDENTITY CA (IDCA)

The STCS IDCA is an issuing Certificate Authority under the Intermediary CA. It issues authentication certificates used to identify end-users.

1.3.2 REGISTRATION AUTHORITIES

Sirar runs its own RA function for the Intermediary CA through Sirar, which is tasked to request issuance and revocation of a certificate under this CP. The RA team's role is to execute the Intermediary CA operational cycle, including the key ceremonies for the QUCA and IDCA, as well as the generation of OCSP certificates and the Certificate Revocation Lists (CRL).

1.3.3 SUBSCRIBERS

The subscribers of STCS Intermediary CA are Issuing CAs that are owned and operated by Sirar.

These subscribers:

- are identified in the Subject field of their certificate, issued by the Intermediary CA
- control the private key corresponding to the public key that is listed in their certificate

1.3.4 RELYING PARTIES

A Relying Party in this context is the entity that relies on the validity of the binding of the STCS Intermediary CA of an identity to a public key. The Relying Party is responsible for checking the validity of the certificate by examining the appropriate certificate status information, using validation services provided by the STCS Intermediary CA. A Relying Party's right to rely on a certificate issued under this CP, requirements for reliance, and limitations thereon, are governed by the terms of the Intermediary CA CP and the Relying Party Agreement.

Relying Parties shall rely on a certificate that has been issued under this CP if:

- The certificate has been used for the purpose for which it has been issued, as described in this CP;
- The Relying Party has verified the validity of the digital certificate, using procedures described in the Relying Party Agreement;
- The Relying Party has accepted and agreed to the Relying Party Agreement at the time of relying on the certificate; it shall be deemed to have done so by relying on the certificate; and

- The relying party accepts in totality, the certificate policy applicable to the certificate, which can be identified by reference of the certificate policy OID mentioned in the certificate.

1.3.5 OTHER PARTICIPANTS

1.3.5.1 Sirar's PKI Committee

Sirar's PKI Committee operates as the governance function for Sirar's PKI. It groups the necessary functions for this purpose including the policy, compliance and design functions. The PKI Committee provides strategic direction and continuously supervises the PKI operations team. The members of this committee are appointed by Sirar's CEO.

1.3.5.2 Sirar's Policy Authority (Sirar's PA)

The Sirar's Policy Authority (Sirar's PA) is an assigned role responsible for the development, maintenance of the Sirar's PKI Policies, amongst other duties.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

STCS Intermediary CA only issues Sub-CA certificates for the issuing certificate authorities that are part of Sirar's PKI hierarchy. In particular it issues certificates to the QUCA and IDCA Certificate Authorities.

OCSP Responder certificates are used to sign responses for certificate status information requests.

1.4.2 PROHIBITED CERTIFICATE USES

Certificates issued under this CP shall not be authorized for use in any circumstances or in any application which is illegal under Saudi Arabia law, could lead to death, personal injury or damage to property, or in conjunction with on-line control equipment in hazardous environments such as in the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control or direct life support machines, and Sirar shall not be liable for any claims arising from such use.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

This CP is administered by the Sirar's PA and approved by the PKI Committee. The chairperson of the PKI Committee signs-off on the approved documents by the PKI Committee.

1.5.2 CONTACT PERSON

Queries regarding this CP shall be directed to:

Email: PolicyAuthority@sirar.com.sa

Telephone: 909

Any formal notices required by this CP shall be sent in accordance with the notification procedures specified in section [9.12.2](#) of this CP.

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The Sirar's PA is responsible for ensuring that the Intermediary CA CPS conforms to the requirements of this CP in accordance with policies and procedures specified by Sirar's PKI. The PA shall ensure that the CPS, after ensuring conformity to this CP, is approved by the PKI Committee.

1.5.4 CPS APPROVAL PROCEDURES

Changes or updates to this CP document must be made in accordance with the stipulations of Saudi e-Transactions act and bylaws and the provisions contained in this CP and are subject to PKI Committee. The PKI Committee reviews the initial version of this CP and any subsequent updates. The PKI Committee interacts with NCDC to formally approve major changes on this document.

The approved changes shall be published as set forth in section [2.2.2](#).

1.6 DEFINITIONS AND ACRONYMS

The following sections contain the definitions of terms and acronyms. The source of a definition is cited when available.

Activation Data — Secret information, other than cryptographic keys, that are required to operate cryptographic modules that need to be protected; for example, a PIN, a password or pass-phrase, or a manually held key share

Audit Report — A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements

CA — Certification Authority

CA Certificate — A certificate for one CA's public key issued by another CA

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

CCTV — Closed Circuit TV

Certificate Policy (CP) — A named set of rules that indicates the applicability of a certificate to a particular community/class of application with common security requirements

Certification Practice Statement (CPS) — A statement of the practices which a certification authority employs in issuing certificates

Certification Practice Statement (CPS) — A statement of the practices which a certification authority employs in issuing and managing certificates.

Control — “Control” (and its correlative meanings, “controlled by” and “under common control with”) means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for “control” under the law of the entity’s Jurisdiction of Incorporation or Registration, but in no case less than 10%

Country — Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations

CRL — Certificate Revocation List

DRP — Disaster Recovery Plan

DN — Distinguished Name

FIPS — Federal Information Processing Standards

HSM — Hardware Security Module, a device designed to provide cryptographic functions, especially the safekeeping of private keys

HTTP — Hyper Text Transfer Protocol

HVAC — Heating, Ventilation and Air Conditioning

IEC — International Electro-technical Commission

IETF — Internet Engineering Task Force

IPSEC — Internet Protocol Security

ISO — International Standards Organization

Issuer — The name of the CA that signs the certificate

Issuing Certification Authority (Issuing CA) — In the context of a particular certificate, the issuing CA is the CA that issued the certificate

ITU — International Telecommunications Union

Key Compromise — A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see <http://wiki.debian.org/SSLkeys>) or if there is clear evidence that the specific method used to generate the Private Key was flawed

KGC — Key Generation Ceremony, the complex procedure for the generation of a CA’s private key

LDAP — Lightweight Directory Access Protocol, a common standard for accessing directories

OID — Object Identifier, a value (distinguishable from all other such values) which is associated with an object. (ITU-T X680) Referred in many RFCs and used in the ASN.1 encoding of certificates

OSCP — Online Certificate Status Protocol

PA — Policy Authority

PIN — A Personal Identification Number or password used to protect the private information and keys on hardware tokens

PKCS # 1 — Public-Key Cryptography Standards (PKCS) #1

PKCS # 7 — Cryptographic Message Syntax

PKCS #10 — Certification Request Syntax Specification

PKCS #12 — Personal Information Exchange Syntax published by RSA Security

PKI — Public Key Infrastructure

PKIX-CMP — Internet X.509 Public Key Infrastructure - Certificate Management Protocol

Policy Qualifier — Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate

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

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

Public Key Infrastructure — A set of hardware, software, people, procedures, rules, policies and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography

RA — Registration Authority

Re-Key — Ceasing use of a key pair and then generating a new key pair to replace it

Relying Party — A recipient of a certificate who acts in reliance on that certificate/digital signatures verified using that certificate

Renewal — Issuance of a new certificate to the subscriber without changing the subscriber's public key or any other information in the certificate

Repository — A trustworthy system for storing and retrieving certificates or other information relevant to certificates

RSA — The acronym for the inventors of the RSA algorithm; Ron Rivest, Adi Shamir and Leonard Adleman

Secret Shares — A set of devices, smart cards, PINs, etc. used with MofN control

SHA — Secure Hash Algorithm

S/MIME — Secure Multipurpose Internet Mail Extensions

SSL/TLS — Secure Sockets Layer/Transport Layer Security

Sponsor — An individual or organization authorized to vouch for another individual in their employment or an electronic device in their control

SubjectAltName — A certificate attribute field that often contains the subject's e-mail address

Subject — A subject is the entity named in a certificate

Subscriber — A subject who is issued a certificate

Trusted Role — Those individuals who perform a security role that is critical to the operation or integrity of a PKI

UPS — Uninterruptible Power Supply

URI — Universal Resource Identifier, a URL, FTP address, email address, etc.

X.501 — A common standard for directory entry naming (ITU)

X.509 — A public key certificate specification originally developed as part of the X.500 directory specification, often used in public key systems; it is now governed by IETF standards

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Sirar shall publish relevant certificates and the certificate status information (e.g. CRLs) about all digital certificates it issues in (an) online publicly accessible Certificate Dissemination Webpage at <https://sirar.com.sa/repository/> and is provided on a 24/7 basis.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

Sirar's PKI repositories shall allow Relying Parties to make on-line enquiries regarding revocation and other certificate status information. The Intermediary CA shall provide Relying Parties with information as part of the certificate on how to find the appropriate repository to check certificate status as well as how to find the appropriate OCSP (Online Certificate Status Protocol) responder.

Sirar's PKI repositories shall contain the following PKI related elements:

- Issuing CA certificates; and
- CRLs: CRLs shall be made publicly available to allow Relying Parties to verify the status of certificates.

The Intermediary CA shall publish CRLs including any changes since the publication of the previous CRL, at regular intervals.

2.2.2 PUBLICATION OF CA INFORMATION

This CP shall be made available to all participants at the Sirar's Certificate Dissemination Webpage: <https://sirar.com.sa/repository/> This Webpage is the only source for up-to-date documentation and Sirar reserves the right to publish newer versions of the documentation without prior notice. Additionally, Sirar shall publish an approved, current and digitally signed version of the CPS at the same repository.

2.2.3 INTEROPERABILITY

Repositories used to publish CA certificates and CRLs shall be based on standard HTTP distribution points.

2.3 TIME OR FREQUENCY OF PUBLICATION

The Issuing CAs certificates shall be published at the repository as soon as possible after issuance. CRLs shall be issued within 24 hours after revocation. Each CRL includes a monotonically increasing sequence number for each CRL issued.

This CP and any subsequent changes should be made available to the participants as set forth in section [2.2.2](#) within two weeks of approval by the PKI Committee and NCDC.

2.4 ACCESS CONTROLS ON REPOSITORIES

Certificates and certificate status information at Sirar's PKI repository shall be made available to Sirar's PKI participants and other parties on a 24x7 basis as determined by the applicable agreements and Sirar's Privacy Policy, and subject to routine maintenance.

Sirar shall protect repository information that is not intended for public dissemination or modification using strong authentication, access controls, and an overall Information Security Management System that prevents unauthorized access to information.

The controls employed by Sirar shall prevent unauthorized persons from adding, deleting or modifying repository entries. Access restrictions shall be implemented on directory search to prevent misuse and unauthorized harvesting of information.

This CP and accompanying CPS documents are provided as public documents and not subject to access control restrictions.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

Each Certificate must have a unique identifiable Distinguished Name (DN) according to the X.500 standard. Common Names (CN) must be unique within each naming space.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The Issuing CA certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates are understood and used by Relying Parties.

The Intermediary CA DN (LDAP Notation) in the Issuer field of all certificates and CRLs that are issued will be:

CN=STCS Intermediary CA, O=STCS, C=SA

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The Intermediary CA may not issue anonymous or pseudonymous certificates.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

The naming convention used by the Intermediary CA is ISO/IEC 9594 (X.500) Distinguished Name (DN). The PKI Committee may further stipulate how names are to be interpreted by publishing such rules in the CPS.

3.1.5 UNIQUENESS OF NAMES

All distinguished names shall be unique across the Intermediary CA.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

Names can only contain trademarks in case the subscriber has the legal right to use the trademark in question. Where applicable, The Intermediary RA enforces this verification as part of the certificate enrolment process.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

The Intermediary CA shall accept certificate signing requests from the Issuing CAs that have demonstrated possession of the Private Key by using a self-signed PKCS#10 request.

3.2.2 *AUTHENTICATION OF ORGANIZATIONAL ENTITY*

The Intermediary CA operates under the Saudi National PKI and as such complies with the requirements as set forth by the NCDC. The Intermediary CA does not issue certificates to other entities other than Sirar's own Issuing CAs (IDCA and QUCA).

3.2.3 *IDENTITY-PROOFING OF INDIVIDUAL IDENTITY*

The Intermediary CA does not issue certificates for individuals.

3.2.4 *NON-VERIFIED SUBSCRIBER INFORMATION*

All subscriber information contained within certificate issued by the Intermediary CA shall be verified by the Intermediary RA.

3.2.5 *VALIDATION OF AUTHORITY*

The PKI Committee shall, before certificate issuance, ensure that the applicant has specific rights, entitlements or permissions to obtain a certificate on behalf of the Issuing CAs.

3.2.6 *CRITERIA OF INTEROPERATION*

No stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 *IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY*

For any re-key of Issuing CAs, a scripted and witnessed processes shall be followed.

3.3.2 *IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION*

If any one of the Issuing CAs is revoked, a key ceremony shall be constituted to regenerate new keys and issue new certificates for the revoked CA after approval by the PKI Committee.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

Prior to the revocation of the Issuing CA Certificates, the PKI Committee shall verify that the revocation has been requested by authorized personnel and that such a request is approved by the PKI Committee.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The Intermediary CA does not accept external applications for Issuing CA certification. The PKI Committee approves the Issuing CAs following internal service requests from the authorized personnel.

4.1.1 *WHO CAN SUBMIT A CERTIFICATE APPLICATION*

Applications for the establishment of internal the Issuing CAs under the Intermediary CA is be made by the authorized personnel to the PKI Committee. The PKI Committee shall consider the request and advice the requester of the outcome.

4.1.2 *ENROLLMENT PROCESS AND RESPONSIBILITIES*

The overall process of enrolling the Issuing CAs shall be documented as an internal key ceremony procedure that need to be tested and verified by the relevant functions in the PKI Committee.

Once the key ceremony procedure is finally approved by the PKI Committee, the certificate application processing for the Issuing CAs can then be planned and executed according to the approved key ceremony procedure.

Further details on the enrolment process shall be specified in the CPS.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 *PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS*

Refer to section [4.1](#) of this CP. More details on the verification process shall be specified in the CPS.

4.2.2 *APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS*

The PKI Committee may approve requests for Issuing CA establishment after considering the application. The committee may also reject the establishment of the Issuing CAs when requisite information is not provided in the application or for any other reason that the committee may dim fit.

4.2.3 *TIME TO PROCESS CERTIFICATE APPLICATIONS*

The PKI Committee shall process the applications as soon as is reasonably possible after receipt of such applications.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

The Intermediary CA shall verify the source of the certificate request before issuance. Once the authenticity of the application is confirmed, the Intermediary CA will create and sign the Issuing CA certificate provided all certificate requirements (including correct population of the certificate fields and extensions) as described in the Key Ceremony Script have been met.

4.3.2 NOTIFICATION OF CERTIFICATE ISSUANCE

The Intermediary CA shall notify the applicant of the Issuing CA immediately, as the issuance forms part of a scripted and witnessed Key Ceremony process.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

On receipt of the signed certificate from the Intermediary CA, the Issuing CA may be established, and this action constitutes acceptance of the certificate by the Issuing CA.

The use of the Issuing CA Certificate or the reliance upon the Certificate signifies acceptance by that person of the terms and conditions of the CP and applicable agreements by which they irrevocably agree to be bound.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

The Issuing CA Certificates will be published, once accepted, in the appropriate repository as described in section [2.1](#).

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No Stipulation.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 PRIVATE KEY AND CERTIFICATE USAGE

The Issuing CAs may only use the Private Key and associated public key contained in the certificate once accepted. The Issuing CAs shall only use their Private Keys for the purposes as contained in the Issuing CA certificate extensions such as key usage, extended key usage, certificate policies etc.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

The Relying Party Agreement becomes effective when the Relying Party relies on information provided by the Intermediary CA or a subscriber regarding a specific transaction that the Relying Party uses to accept or reject their participation in the transaction. The Relying Party's use of the Sirar's PKI Repository, CRL, or the OCSP is governed by the Relying Party Agreement and Intermediary CA CP. The Relying Party is solely responsible for deciding

whether or not to rely on the information in a certificate provided by Intermediary CA. The Relying Party bears the legal consequences of any failure to comply with the obligations set in the Relying Party agreement.

4.6 CERTIFICATE RENEWAL

Certificate renewal is the issuance of a new certificate without changing the public key or any other information in the certificate. Certificate renewal is supported for Intermediary CA issued certificates to the Issuing CAs.

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

The STCS Intermediary CA may renew the Issuing CA certificates provided the following conditions are met:

- The original Issuing CA certificate to be renewed has not been revoked;
- The details in the original Issuing CA certificate remains accurate and that no new or additional validation is required.

Should the above not be met, a new Issuing CA certificate must be issued following a Key Generation process similar to what was followed for issuing the initial Issuing CA certificate.

4.6.2 WHO MAY REQUEST CERTIFICATE RENEWAL

The request for renewal may only be made by authorized personnel. The PKI Committee shall approve all such requests.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

The renewal request may only be processed after receiving such a renewal request from the original authorized personnel or a representative. The PKI Committee shall process all Issuing CA Certificate Renewal Requests after satisfying itself of the authenticity and validity of the request.

4.6.4 NOTIFICATION OF RENEWED CERTIFICATE ISSUANCE

Issuing CA certificate renewals shall follow the same notification method as a new Issuing CA certificate issuance.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Issuing CA renewal certificate acceptance shall follow the same conditions for a new Issuing CA acceptance.

4.6.6 PUBLICATION OF A RENEWAL CERTIFICATE

The Issuing CA renewed certificate shall be published at the same location as the original certificate.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Generally, Intermediary CA does not notify other entities of a renewed Issuing CA certificate apart from requesting party.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate (key update) refers to the issuance of new certificate with a different key pair and serial number while retaining other subject information from old certificate.

The new Certificate may be assigned a different validity period and/or signed using a different issuing CA private key.

4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

Certificate re-key may happen while the Issuing CAs' certificate is still active, after it has expired, or after a revocation. The re-key operation shall invalidate any existing active certificate for an Issuing CA.

4.7.2 WHO CAN REQUEST A CERTIFICATE RE-KEY

In accordance with the conditions specified in previous section, Certificate re-key may be requested by authorized personnel. The PKI Committee shall approve all Issuing CA certificate re-key requests.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

Processing of Issuing CA certificate re-keying request shall be initiated only after successful verification of the re-key request from an authorized personnel; in each case the PKI Committee shall approve all re-key requests.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Notification of issuance of a re-keyed certificate to Subscribers shall follow the same procedures as notification for newly issued CA certificates.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Conduct constituting acceptance of a re-keyed Issuing CA certificate is same as listed in section [4.4.1](#).

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

After successful completion of the re-key process, the Issuing CA certificate shall be published in appropriate repositories, in the same manner as for a newly issued certificate.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Generally, Intermediary CA does not notify other entities of a re-keyed certificate apart from the requesting party.

4.8 CERTIFICATE MODIFICATION

The Intermediary CA does not support any form of Issuing CA certificate modification. The issued CA certificate must first be revoked, and a new process followed to Re-key the certificate as specified in section [4.7](#).

4.9 CERTIFICATE REVOCATION AND SUSPENSION

The Issuing CA Certificate shall be revoked when the binding between the Subject and the Subject's Public Key defined within a Certificate is no longer considered valid.

The Intermediary CA will notify other participants of certificate revocation through access to the CRL at the Sirar's PKI repository or through the OCSP.

4.9.1 CIRCUMSTANCE FOR REVOCATION OF A CERTIFICATE

The STCS Intermediary Certificate Authority shall revoke subordinate Issuing CA Certificates for the following non-exhaustive reasons:

- The Intermediary CA suspects or determines that the Issuing CA Private Key is compromised.
- If a subordinate Issuing CA contravenes any provisions of the Saudi National PKI Policy, Saudi e-Transactions Act and applicable By-laws;
- The Intermediary CA suspects or determines that revocation of an Issuing CA Certificate is in the best interest of the integrity of the Sirar's PKI Hierarchy;
- The Intermediary CA determines that a Certificate was not issued correctly in accordance with this CP;

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed in a CRL.

The PKI committee shall decide on the actions related to the Issuing CA subscribers' certificates because of the CA certificate revocation.

More details on the revocation procedure and the PKI Committee relevant actions are specified in the CPS.

4.9.2 WHO CAN REQUEST REVOCATION OF A CERTIFICATE

The following entities can request revocation of a certificate:

- NCDC can request the revocation of any certificates issued by any CA participating in the Saudi National PKI;
- The PKI Committee can request the revocation of any of the Issuing CA certificates issued under the Intermediary CA PKI Hierarchy;
- A legal, judicial or regulatory agency can request a revocation of any of the Issuing CA certificates

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). The Intermediary CA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements. The PKI Committee has the final approval for the revocation of an Issuing CA certificates.

4.9.4 *REVOCATION REQUEST GRACE PERIOD*

Revocation request grace period is not permitted once a revocation request has been verified. The Intermediary CA will revoke certificates as quickly as practical upon receipt of a legitimate revocation request, or at a time agreed by the PKI committee as long as the revocation is not due to a compromise. The Issuing CA are required to request revocation within one day after detecting the loss or compromise of the Private Key.

4.9.5 *TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST*

The Intermediary CA shall process authorized revocation requests within 24 hours or at a time agreed by the PKI committee as long as the revocation is not due to a compromise.

4.9.6 *REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES*

Revocation information shall be offered to relying parties through the CRLs or the OCSP responder. Relying parties shall use any of these methods while processing a certificate issued by the Intermediary CA.

4.9.7 *CRL ISSUANCE FREQUENCY*

The STCS Intermediary CA shall issue CRLs at least every 6 months and within 24 hours after revocation of an Issuing CA.

4.9.8 *MAXIMUM LATENCY OF CRLS*

CRLs shall be published in the Repositories within 24 hours of Certificate revocation.

4.9.9 *ONLINE REVOCATION CHECKING AVAILABILITY*

Certificate status information shall be provided through the OCSP for the Intermediary CA.

4.9.10 *ONLINE REVOCATION CHECKING REQUIREMENTS*

It is at the discretion of the relying party to decide whether using CRL or relying on OCSP.

4.9.11 *OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE*

The Intermediary CA will not provide other forms of revocation advertisements.

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

If the Intermediary CA discovers, or has a reason to believe, that there has been a compromise of the private key of the Intermediary CA or any Issuing CA, Intermediary CA will immediately declare a disaster and invoke the business continuity plan. Intermediary CA will

- 1) Determine the scope of certificates that must be revoked,
- 2) Revoke the affected certificates as per Intermediary CA procedures
- 3) Publish a new CRL as stipulated in section [4.9.7](#),
- 4) Update the OCSP responder,
- 5) Generate new CA key pair as per Sirar's operations policies and procedures.

4.9.13 CIRCUMSTANCES FOR CERTIFICATE SUSPENSION

Not applicable.

4.9.14 WHO CAN REQUEST SUSPENSION

Not applicable.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

Not applicable.

4.9.16 LIMITS ON SUSPENSION PERIOD

Not applicable.

4.9.17 CIRCUMSTANCES FOR TERMINATING SUSPENDED CERTIFICATES

Not applicable.

4.9.18 PROCEDURE FOR TERMINATING THE SUSPENSION OF A CERTIFICATE

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

The status of the Issuing CAs public certificates shall be made available through CRLs in the repositories as well as the OCSP responder.

4.10.1 OPERATIONAL CHARACTERISTICS

CRLs shall be published by on a public repository which is available to relying parties through HTTP protocol queries.

The OCSP responders shall expose an HTTP interface accessible to relying parties.

4.10.2 SERVICE AVAILABILITY

The repository, including the latest CRL, should be available 24X7 for at least 99% of the time.

4.10.3 *OPTIONAL FEATURES*

No stipulation — this section is intentionally left blank.

4.11 *END OF SUBSCRIPTION*

No stipulation.

4.12 *KEY ESCROW AND RECOVERY*

The Intermediary CA does not support Key Escrow.

5. FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

Sirar's PKI is hosted at Sirar's data center, with appropriate physical and procedural access controls for all hardware and software sub-systems used in the issuance and revocation of certificates. Access to functions critical to registration and certification is limited to personnel in Trusted Roles.

Sirar shall enforce physical and environmental security policies for systems used for certificate issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery. Controls should be implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities

5.1.1 SITE LOCATION AND CONSTRUCTION

The location and construction of the facility hosting the Intermediary CA and Sirar's Data Center equipment is 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, provides robust protection against unauthorized access to the Intermediary CA equipment and records.

5.1.2 PHYSICAL ACCESS

The Intermediary CA systems shall be protected by at least four tiers of physical security, with access to the lower tier required before gaining access to the higher tier. Progressively restrictive physical access privileges control access to each tier. Sensitive Intermediary CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Physical access shall be automatically logged, and video recorded. Additional tiers enforce individual access control through the use of biometric authentication. Unescorted personnel, including un-trusted employees or visitors, should not be allowed into such secured areas. Sirar employ Security Personnel that continually monitor the facility hosting CA equipment on a 24x7 basis. Sirar shall provide normal and emergency lighting to the CA facilities.

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

5.1.3 POWER AND AIR CONDITIONING

Sirar shall ensure that the power and air conditioning facilities are sufficient to support the PKI Operations environment.

The Intermediary CA equipment shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Any of the Intermediary CA on-line servers (e.g.,

CAs hosting servers) shall be provided with Uninterrupted Power sufficient to support a smooth shutdown of the PKI operations.

5.1.4 WATER EXPOSURE

Sirar shall ensure that the Intermediary CA systems are protected from exposure to water sources

5.1.5 FIRE PREVENTION AND PROTECTION

The Intermediary CA equipment shall be housed in a facility with appropriate fire suppression and protection systems.

5.1.6 MEDIA STORAGE

Sirar shall ensure that the Intermediary CA media shall be stored so that they are protected from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive or backup information is duplicated and stored in a location separate from the CAs.

5.1.7 WASTE DISPOSAL

Sensitive media and documentation that are no longer needed for operations are destroyed using appropriate disposal processes.

5.1.8 OFF-SITE BACKUP

Full system backups of CAs, sufficient to recover from system failure, are made on a periodic schedule as described in Sirar's Operations Policies and Procedures.

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. The people selected to fill these roles must be extraordinarily responsible or the integrity of the PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the Intermediary CA. The following are the trusted roles for Sirar's PKI:

- CA Administrator – general CA administration and approval of the generation, and revocation of certificates
- Security Officer – overall responsibility for administering the implementation of the CA's security practices, cryptographic key lifecycle management functions
- Sirar's Policy Authority – responsible for the overall development, maintenance and ensures approval of CA policies
- Operations Authority – responsible for the implementation of the CA policies and development of operational procedures and guidelines
- CA Auditor – internal auditor is responsible for ensuring the CA is operating in line with approved policies and procedures. The auditor is also responsible for checking that procedures are being followed correctly during Key Ceremonies

- CA Key Manager – responsible for CA Key Lifecycle management functions
- CA Operator – The CA Operator role is responsible for: Daily operation and maintenance of the system equipment; System backup and recovery operations; and Storage media renewal.
- CA Key Shareholders – holders of the CA key components

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Sirar shall ensure separation of duties for critical CA functions to prevent one person from maliciously using the PKI systems without detection. Each user's system access is limited to those actions for which they are required to perform in fulfilling their responsibilities. Separate individual shall fill each of the roles specified in Governance and Operating Model document. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over the system operation.

A single person may be sufficient to perform tasks associated with a role, except for the activation of the CA certificate signing Private Key. Activation of the CA certificate signing Private Key shall require M/N protection (i.e. actions by any three (3) out of twelve people (12)).

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

Before exercising the responsibilities of a trusted role:

- Sirar shall confirm the identity of the employee by carrying out background checks.
- Sirar shall issue an access card to administrators who need to access equipment located in the secure enclave.
- Sirar shall provide the necessary credentials that allow administrators to conduct their functions.

5.2.4 SEPARATION OF ROLES

Individual CA personnel are specifically designated to the roles defined in section [5.2k1](#) of this CP and Governance and Operating Model document. The Intermediary CA will ensure that no individual shall be assigned more than one Trusted Role.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE AND CLEARANCE REQUIREMENTS

All persons filling trusted roles shall be selected on the basis of skills, experience, loyalty, trustworthiness, and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA are set forth in the Governance and Operating Model document.

5.3.2 BACKGROUND CHECK AND CLEARANCE PROCEDURES

Sirar enforces background investigations for all Sirar's PKI personnel including trusted roles and management positions. Background check shall take into account the following:

- Availability of satisfactory character reference, i.e., one business and one personal;
- A check (for completeness and accuracy) of the applicant's CV;

- Confirmation of claimed academic and professional qualifications;
- Independent identity check (National ID card, Passport or similar document);
- Interviews with references shall be done as required; and
- More detailed checks, such as security clearance.

Security clearance shall be repeated every 3 years for personnel holding trusted roles. All persons filling the Trusted Roles shall only be granted access to the Sirar's PKI systems once the background clearance procedures detailed above have been completed and confirmed.

5.3.3 *TRAINING REQUIREMENTS*

Sirar shall ensure that all personnel receive appropriate training. Such training shall address relevant topics such as basic Public Key Infrastructure knowledge, security requirements, operational responsibilities and associated procedures.

5.3.4 *RETRAINING FREQUENCY AND REQUIREMENTS*

Individuals responsible for PKI roles are made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

The Intermediary CA shall review and update its training program at least once a year to accommodate changes in the CA system.

5.3.5 *JOB ROTATION FREQUENCY AND SEQUENCE*

The STCS Intermediary CA shall ensure that any change in the staff complement will not affect the operational effectiveness of the PKI services and security thereof.

5.3.6 *SANCTIONS FOR UNAUTHORIZED ACTIONS*

The Intermediary CA shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions (i.e., not permitted by the CP, CPS and/or other procedures) involving the Intermediary CA or the Sirar's PKI repository.

5.3.7 *CONTRACTING PERSONNEL REQUIREMENTS*

Contractor personnel employed to perform functions pertaining to the Sirar's PKI Operations shall be subjected to the same processes, sanctions, assessment, security and operational procedure as permanent personnel, under adequate supervision and perform only assigned tasks.

5.3.8 *DOCUMENTATION SUPPLIED TO PERSONNEL*

Sirar will make available to its personnel its CP, CPS, and any relevant documents required to perform their duties.

5.4 AUDIT LOGGING PROCEDURES

Audit log files are generated for all events relating to the security of the Intermediary CA, and other associated components. The security audit logs for each auditable event defined in this section are maintained in accordance with onsite retention period and for archive.

5.4.1 TYPES OF EVENTS RECORDED

the PKI Committee shall ensure recording in audit log files all events relating to the security of the CA system hosted in Sirar's data centre. All security audit capabilities of the CA operating system and CA applications shall be enabled. Such events include, but are not limited to:

1. CA key lifecycle management events, including:
 - a. Key generation, backup, storage, recovery, archival, and destruction; and
 - b. Cryptographic device lifecycle management events.
2. Issuing CA Certificate lifecycle management events, including:
 - c. Certificate requests, renewal, and re-key requests, and revocation;
 - d. All verification activities stipulated in these Requirements and the Issuing CAs' Certification Practice Statement;
 - e. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
 - f. Acceptance and rejection of certificate requests;
 - g. Issuance of Certificates; and
 - h. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
 - i. Successful and unsuccessful PKI system access attempts;
 - j. PKI and security system actions performed, such as:
 - the value of maximum authentication attempts is changed;
 - an administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
 - k. Security profile changes;
 - l. System crashes, hardware failures, and other anomalies;
 - m. Firewall and router activities; and
 - n. Entries to and exits from the Sirar's PKI facility.
 - o. Equipment failure or electrical power outages
 - p. Changes to CA configuration and system clock time

Log entries MUST include the following elements:

- Date and time of entry;
- Identity of the person making the journal entry; and
- Description of the entry.

All logs, whether electronic or manual, must contain the date and time of the event and the identity of the Entity which caused the event. The CA shall also collect, either electronically or manually, security information not generated by the CA system such as:

- Physical access logs;
- System configuration changes and maintenance;
- CA personnel changes;
- documentation relating to certificate requests and the verification;
- documentation relating to certificate revocation;
- Discrepancy and No compromise reports;
- Information concerning the destruction of sensitive information;
- Current and past versions of all Certificate Policies;
- Current and past versions of Certification Practice Statements;
- Vulnerability Assessment Reports;
- Threat and Risk Assessment Reports;
- Compliance Inspection Reports; and
- Current and past versions of Agreements.

5.4.2 *FREQUENCY OF PROCESSING DATA*

The PKI Committee shall ensure that the designated personnel reviews log files at regular intervals to validate log integrity and ensure timely identification of anomalous events.

Designated personnel must report and perform follow-up of these events and any issues affecting audit log integrity.

Log files and audit trails shall be periodically archived for inspection by authorized personnel.

The log files shall be properly protected by an access control mechanism, so that no others can have access. Log files and audit trails shall be backed up.

All log entries include the following elements:

- Date and time of entry
- Identity of the person making the journal entry
- Description of the entry.

5.4.3 *RETENTION PERIOD FOR AUDIT LOG*

Sirar shall retain all system generated (electronic and manual) audit records onsite for a period not less than twelve months from the date of creation.

5.4.4 *PROTECTION OF AUDIT LOG*

Sirar shall protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction.

5.4.5 *AUDIT LOG BACKUP PROCEDURES*

Sirar shall back up all audit logs and audit summaries in a secure location and protected to the same degree as the originals.

5.4.6 *AUDIT COLLECTION SYSTEM (INTERNAL OR EXTERNAL)*

Refer to the applicable CPS for details on the audit collection systems in use.

5.4.7 *NOTIFICATION TO EVENT-CAUSING SUBJECT*

Event-causing subject are not notified.

5.4.8 *VULNERABILITY ASSESSMENTS*

Routine vulnerability assessments of security controls shall be performed by the Intermediary CA for its Issuing CAs and other PKI supporting systems hosted in Sirar's data centre.

Sirar's PKI security program shall include an annual Risk Assessment which includes identification of foreseeable internal and external threats, assess the likelihood and potential damage of these threats and assess the sufficiency of the policies, procedures, information systems and technology. The program shall also ensure vulnerability assessments are performed, reviewed and revised following an examination of audit events.

Based on the Risk Assessment exercise, Sirar shall develop, implement, and maintain a security plan to control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

5.5 RECORDS ARCHIVAL

5.5.1 *TYPES OF EVENTS ARCHIVED*

Sirar shall retain in a trustworthy manner records of digital certificates, audit data, systems information and documentation. Sirar shall ensure that at least the following records are archived:

1. CA key lifecycle management events, including:
 - a. Key generation, backup, storage, recovery, archival, and destruction; and
 - b. Cryptographic device lifecycle management events.
2. Issuing CA Certificate lifecycle management events, including:
 - c. Certificate requests, renewal, and re-key requests, and revocation;
 - d. All verification activities stipulated in these Requirements and the Issuing CAs' Certification Practice Statement;

- e. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
 - f. Acceptance and rejection of certificate requests;
 - g. Issuance of Certificates; and
 - h. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
- i. Successful and unsuccessful PKI system access attempts;
 - j. PKI and security system actions performed, such as:
 - o the value of maximum authentication attempts is changed;
 - o an administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
 - k. Security profile changes;
 - l. System crashes, hardware failures, and other anomalies;
 - m. Firewall and router activities; and
 - n. Entries to and exits from the Sirar's PKI facility.
 - o. Equipment failure or electrical power outages
 - p. Changes to CA configuration and system clock time

Log entries MUST include the following elements:

- Date and time of entry;
- Identity of the person making the journal entry; and
- Description of the entry.

5.5.2 RETENTION PERIOD FOR ARCHIVE

The minimum retention periods for archive data are established in accordance with applicable regulatory guidance, laws, Agreements, and as specified by the PKI Committee. Intermediary CA's minimum retention period for archive data is established at ten (10) years.

The Intermediary CA shall retain all documentation relating to the Intermediary CA certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least ten (10) years after any Certificate based on that documentation ceases to be valid.

5.5.3 PROTECTION OF ARCHIVE

Only authorized personnel shall be permitted to review the archive. The contents of the archive shall not be released except as determined by NCDC, the PKI Committee, or as required by law. Records and material information relevant to use of, and reliance on, a certificate shall be archived. Archive media shall be stored in a secure storage facility separate from the component itself. Any secondary site must provide adequate protection from environmental threats such as temperature, humidity and magnetism. Data to be migrated periodically to fresh media; and protection against obsolescence of hardware, operating systems, and other software, by, for example, retaining as part of the archive the hardware, operating systems, and/or other software in order to permit access to and use of archived records over time.

5.5.4 *ARCHIVE BACKUP PROCEDURES*

Only one copy of the archive is maintained. In other words, archive itself is not backed up.

5.5.5 *REQUIREMENTS FOR TIME-STAMPING OF RECORDS*

Certificates, CRLs, and other revocation database entries shall contain time and date information. System logs shall be time stamped and systems use a dedicated time server to maintain synchronized time.

5.5.6 *ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)*

Only authorized and authenticated staff shall be allowed to access archived material. PKI operations team use a dedicated backup, restore and archive procedures that describe how the archive information is created, transmitted and stored involving the archive collection systems.

5.5.7 *PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION*

Only authorized personnel with a clear hierarchical control and a definite job description may obtain and verify archive information. Sirar retains records in electronic or in paper-based format.

5.6 KEY CHANGEOVER

The CA system utilized by the Intermediary CA may periodically perform key rollover, allowing CA keys to be changed periodically as required to minimize risk to the integrity of the Intermediary CA. Once changed the new key is used for certificate signing purposes. The unexpired older keys are used to sign CRL's until all certificates signed by the unexpired older private key have expired.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 *INCIDENT AND COMPROMISE HANDLING PROCEDURES*

If Sirar detects a potential hacking attempt or other form of compromise to the CA, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Sirar's Operations Policies and Procedures shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the Intermediary CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

5.7.2 *COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED*

The Intermediary CA shall maintain backup copies of hardware, system, databases, and private keys in order to rebuild the Intermediary CA capability in case of software and/or data corruption.

5.7.3 CA PRIVATE KEY COMPROMISE RECOVERY PROCEDURES

Sirar shall develop and maintain Recovery Policies and Procedures. Same shall be followed in the case of the Intermediary CA Private Key compromise.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

Intermediary CA shall develop robust Business Continuity Management System for critical PKI services to in order to provide the minimum acceptable level of assurance to its subscribers for service availability.

Sirar's PKI critical infrastructure equipment at the primary site (Sirar's data centre) shall have built-in hardware fault-tolerance and configured to be highly available with auto-failover switching. Sirar shall maintain copies of backup media and infrastructure system software, which include but are not limited to PKI services related critical data; database records for all certificates issued and audit related data, at its offsite business continuity and disaster recovery storage facilities.

Business Continuity Management components of Sirar's PKI shall be regularly tested, verified, and updated to be operational to address crisis situation in the event of a disruption.

Sirar shall develop Disaster recovery plans to mitigate the effects of any kind of natural, man-made or equipment failure related disaster. Sirar shall implement an alternate recovery site as per industry standards to provide full recovery of critical PKI services in case of the disaster related events.

5.8 CA TERMINATION

When it is necessary to terminate the Intermediary CA, the impact of the termination must be minimized as much as possible in light of the prevailing circumstances and is subject to the applicable Sirar PKI Agreements. Procedures to be followed for the termination of the STCS Intermediary CA shall be developed, and must at a minimum include the following:

- Ensure minimal disruption caused by the termination of the CA
- Ensure notification of the Issuing CAs, Relying Parties and other relevant Stakeholders, such as the NCDC
- Ensure certificate status information services are provided and maintained for the duration of the termination
- Ensure process for revoking certificates are maintained

Sirar shall nominate a custodian of the Intermediary CA archival records in case of termination of Sirar's PKI.

Should a successor CA be appointed to take over the functions of the Intermediary CA, such a successor shall, to the extent as it is practical and reasonable, assume the same rights, obligations and duties as the terminated the Intermediary CA.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

Key pair generation for the Intermediary CA shall be witnessed and attested to by a party separate from the Intermediary CA operator or the CA administrator as mentioned in the Key Generation Script for each CA.

Key Pair generation shall be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. The Sirar's PKI CAs shall use Hardware Security Modules (HSMs) for CA key generation and storage. HSM's should be minimum FIPS 140-2 Level 3 validated.

The Intermediary CA and Issuing CAs key pair generation is performed by multiple trusted personnel using trustworthy systems and processes that provide security and required cryptographic strength for the generated keys.

The Intermediary CA and Issuing CAs key pair is generated in pre-planned Key Generation Ceremony in accordance with the requirements of NCDC. The activities performed during the Key Generation Ceremony are video recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by Sirar's PKI management.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBERS

The Intermediary CA does not generate nor issue subscriber private keys or certificates

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

The Intermediary CA shall accept Issuing CA Public Keys that are cryptographically protected, such as those using PKCS#10 mechanisms from authorized personnel. Such Public Key delivery shall be made as part of the Key Ceremony and as documented in the Key Ceremony Script.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The Intermediary CA Public Key shall be delivered to the Relying Parties by making it available as set forth in section [2.2.1](#).

6.1.5 KEY SIZES

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. Key sizes are described as below for CAs under the Sirar's PKI. All FIPS-approved signature algorithms shall be considered acceptable. If NCDC determines that the security of a particular algorithm may be compromised, it shall direct Sirar to revoke the affected certificates.

Issuing CAs keys shall be at least 4096-bit RSA while the OCSP responders keys shall be 2048-bit RSA, with Secure Hash Algorithm version 2 (SHA-256) in accordance with FIPS 186-4 or equivalent.

The key lengths under the Sirar's PKI Hierarchy are as follows;

- Intermediary CA: 4096 bits
- STCS IDCA : 4096 bits
- STCS QUCA : 4096 bits
- OCSP Key Pair: 2048 bits RSA

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The Intermediary CA and all Issuing CAs shall generate key pairs that comply with FIPS 186-4. The Intermediary CA shall use reasonable techniques to validate the suitability of the Issuing CA key pairs.

6.1.7 KEY USAGE PURPOSES

Public keys that are bound with the Issuing CAs certificates shall be certified for use in Certificate and CRL signing. The use of a specific key is determined by the key usage extension in the X.509 certificate. The Intermediary CA key is used for Certificate and CRL signing.

6.2 PRIVATE KEY PROTECTION AND CRYPTO-MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

Cryptographic modules employed for private key protection for the Intermediary CA, Issuing CAs and the OCSP Responder shall comply with FIPS-PUB 140-2 "Security Requirements for Cryptographic Modules", Level 3 and above.

6.2.2 CA PRIVATE KEY MULTI-PERSON CONTROL

Using of any CA Private signing keys shall require action by multiple persons. The Intermediary CA keys can only be accessed on the physical and logical level by adhering to the multi-person control scheme (M out of N) as described in the CPS.

The Issuing CAs keys shall be accessed on the physical level by adhering to the multi-person control scheme.

The OCSP Responder private key may not be under multi-person control.

6.2.3 PRIVATE KEY ESCROW

The Intermediary CA does not escrow the Issuing CAs' Private keys.

6.2.4 PRIVATE KEY BACKUP

The private keys of the Intermediary and Issuing CAs are backed up and held stored safely in exclusive safes maintained in the most inner security zones of the PKI facilities. Backup operations are executed as part of the CA key generation ceremonies. The DR keys are backed up under the same dual control and split knowledge as the primary keys.

6.2.5 PRIVATE KEY ARCHIVAL

The Intermediary CA does not archive Private Keys.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

The Intermediary CA shall generate, activate and store private keys in FIPS 140-2 Level 3 or above rated Hardware Cryptographic Modules. When the Private Keys are outside the HSM, they shall be kept in encrypted form.

The Intermediary CA keys can be cloned for secure backup from the master hardware cryptographic module to other hardware cryptographic module(s) using secure mechanisms so that they can be recovered if a major catastrophe destroys the productive set of keys.

The above same controls shall be also applicable on the Issuing CAs.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The Intermediary CA's and Issuing CAs' Private Key shall be stored on FIPS 140-2 Level 3 validated cryptographic module in encrypted form.

6.2.8 METHOD OF ACTIVATING PRIVATE KEYS

The Intermediary CA's private key shall be activated by the main stakeholders and authorized personnel, as defined in Sirar's Operations Policies and Procedures, supplying their activation data. Such activation data shall be held on secure media and shall require the successful completion of a multi-person authentication process.

The above same controls shall be also applicable on the Issuing CAs.

6.2.9 METHODS OF DEACTIVATING PRIVATE KEYS

The Intermediary CA's private key shall be deactivated by the main stakeholders and authorized personnel, as defined in Sirar's Operations Policies and Procedures by removing their secure media and storing it in a secure container or environment when not in use.

The above same controls shall be also applicable on the Issuing CAs.

6.2.10 METHODS OF DESTROYING PRIVATE KEYS

The Intermediary CA keys shall be destroyed as per Sirar's Cryptographic Devices Lifecycle Management Policy and Procedures.

The above same controls shall be also applicable on the Issuing CAs.

6.2.11 CRYPTOGRAPHIC MODULE RATING

As described in section [6.2.1](#).

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVE

The Intermediary CA Public Key is archived as part of the certificate archive process.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY USAGE PERIODS

The table below details key usage, length and certificate lifetime for the corresponding keys:

Key/Certificate	Key Length in Bits	Maximum Validity Period
STCS Intermediary CA signing key and certificate	4096	118 months
STCS QUCA Signing Key and Certificate	4096	118 months
STCS IDCA Signing Key and Certificate	4096	118 months
OCSP Signing Key	2048	36 months

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Activation data may be user selected.

6.4.2 ACTIVATION DATA PROTECTION

The Intermediary CA shall protect activation data from disclosure or compromise. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect and shall not be stored with the cryptographic module.

The above same controls shall be also applicable on the Issuing CAs.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 *SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS*

The computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards.

At a minimum Sirar's data centre shall have (but not limited to) the following controls to ensure security of the systems:

- Integrity checks are performed on the operating system;
- Software packages are only installed from a trusted software repository;
- Minimal network connectivity;
- Authentication and authorization for all functions;
- Strong authentication and role-based access control for all vital functions;
- Disk and file encryption for all relevant data; and
- Proactive patch management.

6.5.2 *COMPUTER SECURITY RATING*

The Intermediary CA as well as the Issuing CAs Software shall comply with at least Common Criteria EAL2 or an equivalent security profile from other applicable standards.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 *SYSTEM DEVELOPMENT CONTROLS*

The CA hardware and software shall be tested, developed, and implemented in accordance with industry best practice development and change management standards.

Purchased hardware or software shall be shipped or delivered in a sealed, tamper-proof container and be installed by trained personnel.

6.6.2 *SECURITY MANAGEMENT CONTROLS*

The configuration of the Intermediary CA systems as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to software or configuration. A formal configuration management methodology shall be used for installation and on-going maintenance of the system.

6.6.3 *LIFE CYCLE SECURITY RATINGS*

Any of the Intermediary CA or the Issuing CAs IT systems or components that are replaced are taken out of operation in such a way that the functions thereof and data contained therein cannot be misused. In addition, any changes to IT systems or components are logged.

6.7 NETWORK SECURITY CONTROLS

The Intermediary CA shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such protection mechanisms may include network security and firewall management, port restrictions and IP address filtering. Unused services shall be turned off.

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

Time stamping shall be supported for the Certificates, CRLs, and other revocation database entries containing time and date information. Sirar shall ensure the synchronization of CA components using a trusted time source, such as a Network Time Protocol (NTP) service or an atomic clock.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

This section contains the rules and guidelines followed by this CA in populating X.509 certificates and CRL extensions. The Intermediary CA shall follow the certificate profiles as described in the STCS Intermediary CPS document.

7.1.1 VERSION NUMBERS

The Intermediary CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 CERTIFICATE EXTENSIONS

The Intermediary CA critical private extensions shall be interoperable in their intended community of use. Issuing CA certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

The Intermediary CA shall sign Certificates using any one of the following:

sha256WithRSAEncryption algorithm (1.2.840.113549.1.1.11).

sha384WithRSAEncryption algorithm (1.2.840.113549.1.1.12).

The algorithm identifier of the subject Public Key shall be:

rsaEncryption (OID: = 1.2.840.113549.1.1.1).

7.1.4 NAME FORMS

Certificates issued by the Intermediary CA shall contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names are in the form of an X.501 printable string.

7.1.5 NAME CONSTRAINTS

No Stipulation.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

Certificates issued under this CP shall assert a certificate policy OID.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

No stipulation

7.1.8 *POLICY QUALIFIERS SYNTAX AND SEMANTICS*

No stipulation.

7.1.9 *PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION*

Processing semantics for the critical certificate policy extension shall conform to X.509 certification path processing rules.

7.2 CRL PROFILE

The Intermediary CA CRL Profile is as below:

Field	Content	Comment
Version	1 (Version 2)	
Algorithm	SHA256withRSA	
Issuer	CN= STCS Intermediary CA O=STCS C=SA	
This update	<issue date>	
Next update	<issue date + 6 months>	Or immediately upon revocation
AuthorityKeyIdentifier	The intermediary CA's Subject Key Identifier	
CRL number	<number>	

7.2.1 *VERSION NUMBERS*

The Intermediary CA shall issue X.509 version two (v2) CRLs (populate version field with integer "1")

7.2.2 *CRL AND CRL ENTRY EXTENSIONS*

Critical private extensions shall be interoperable in their intended community of use. CRLs shall have the CRL number and Authority Key Identify extensions set.

7.3 OCSP PROFILE

OCSP requests and responses shall be in accordance with RFC 6960.

7.3.1 *VERSION NUMBER*

The version number for request and OCSP responses shall be v1

7.3.2 *OCSP EXTENSIONS*

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The PKI Committee shall ensure that the requirements of the Intermediary CA CP and CPS and the provisions of applicable Agreements with NCDC are implemented and enforced. Intermediary CA shall undergo annual audits whose results shall be submitted to NCDC.

The PKI Committee shall ensure adherence of the Issuing CAs to this CP, accompanying CPS and any applicable laws and regulations. The committee shall also ensure the Issuing CAs comply with audit requirements.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The Intermediary CA shall be subjected to periodic compliance audits which are no less frequent than once a year and after each significant change to the deployed procedures and techniques.

Further, the PKI Committee shall also be performing internal audit at least on a quarterly basis against a randomly selected sample for monitoring adherence and service quality.

The Subordinate Issuing CAs shall also follow the same audit frequency to ensure compliance against defined requirements.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The annual audit of the Intermediary CA shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme; and
- Bound by law, government regulation, or professional code of ethics.

A licensed WebTrust auditor will be appointed by Intermediary CA for the audit.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

To provide an unbiased and independent evaluation, the auditor and audited party shall not have any current or planned financial, legal or other relationship that could result in a conflict of interest.

8.4 TOPICS COVERED BY ASSESSMENT

The compliance audits will verify whether the Sirar's PKI operations environment is in compliance with the applicable CP, CPS and supporting operational policies and procedures. The term Sirar PKI Operations environment defines the total environment and includes:

- All documentation, records;
- Contracts/agreements;
- Compliance with applicable Law;
- Physical and logical controls;
- Personnel and approved roles/tasks;
- Hardware (e.g., servers, desktops, hardware security modules, network devices and security devices); and
- Software and information.

The auditor shall provide the PKI Committee and/or NCDC with a compliance report highlighting any discrepancies.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If irregularities are found by the auditor, the audited party (Intermediary CA) shall be informed in writing of the findings. The audited party must submit a report to the auditor or directly to NCDC or the PKI Committee, as determined by NCDC, as to any remedial action the audited party will take in response to the identified deficiencies. This report shall include a time for completion to be approved by the auditor, or by NCDC as appropriate.

Where an audited party fails to take remedial action in response to the identified deficiencies, NCDC shall be informed by the auditor and shall take the appropriate action, according to the severity of the deficiencies.

- Noting the deficiencies but allowing the CA to continue operations until the next planned, or newly scheduled, inspection; or
- Revoking the CA's certificate.

8.6 COMMUNICATION OF RESULTS

An Audit Compliance Report, including identification of corrective measures taken or being taken by the audited party, shall be provided to the PKI Committee and/or NCDC as applicable.

The Intermediary CA shall make the Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, an explanatory letter is to be signed by the Qualified Auditor.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE/RENEWAL FEE

Sirar may charge fees for certificate issuance or renewal. Fees may also be charged for certificate reissuance or re-key.

9.1.2 CERTIFICATE ACCESS FEES

Sirar may charge access fees at its discretion to any database which stores issued certificates.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEE

Sirar does not charge fees to access certificate status information via the CRL nor the OCSP responder.

9.1.4 FEES FOR OTHER SERVICES

Sirar may charge fees for other services such as timestamping.

9.1.5 REFUND POLICY

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

Sirar disclaims all liability implicit or explicit due to the use of any certificates issued by the Issuing CAs which certify public keys of subscribers.

9.2.1 INSURANCE COVERAGE

Sirar shall hold insurance cover in lieu of its performance and obligations that is deemed sufficient by the Intermediary CA:

- Commercial general liability insurance with policy limits as determined by Sirar;
- Professional Liability (Errors and Omissions) Insurance with policy limits as determined by Sirar

9.2.2 OTHER ASSETS

Sirar shall have sufficient financial resources to maintain their operations and perform their duties.

9.2.3 INSURANCE/WARRANTY COVERAGE FOR END-ENTITIES

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Information pertaining to the CA and not requiring protection may be made publicly available at the discretion of the PKI committee. Specific confidentiality requirements for business information are defined in Sirar's Privacy Policy and the applicable Agreements.

9.3.1 *SCOPE OF CONFIDENTIAL INFORMATION*

Any corporate or personal information held by Sirar, the Intermediary CA and Issuing CAs related to the application and issuance of Certificates is considered confidential and will not be released without the prior consent of the relevant holder, unless required otherwise by law or to fulfil the requirements of this CP, and in accordance with Sirar's Privacy Policy. Sirar's Information Assets Classification & Control Policy specifies which documents are confidential. Information contained in certificates and related certificate status is not confidential.

9.3.2 *INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION*

Such information as specified by the PKI Committee, Sirar's Privacy Policy, Sirar's Information Assets Classification & Control Policy, Sirar's Operations Policies and procedures and applicable Agreements.

9.3.3 *RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION*

All Sirar's PKI participants shall be responsible for protecting the confidential information they possess in accordance with Sirar's Privacy Policy and applicable laws and Agreements.

9.4 PRIVACY OF PERSONAL INFORMATION

Any personal identifying information collected by the Intermediary CA shall be protected in accordance with Sirar's Privacy Policy. The Intermediary CA shall use reasonable measures to protect personal identifying information from disclosure to any third party.

9.4.1 *PRIVACY PLAN*

All personally identifying information as defined by Sirar's Privacy Policy shall be protected from unauthorized disclosure.

9.4.2 *INFORMATION TREATED AS PRIVATE*

Any information about Issuing CAs that is not publicly available through the content of the issued certificate, repository and online CRL's is treated as private.

9.4.3 *INFORMATION NOT DEEMED PRIVATE*

Information appearing in Issuing CA Certificates such as the organization name, and public key will not be deemed private. Sirar's Privacy Policy identifies the personally identifiable information that can be collected to enable issuance of a certificate.

9.4.4 *RESPONSIBILITY TO PROTECT PRIVATE INFORMATION*

Sirar's employees, suppliers and contractors handle personal information in strict confidence under the Sirar's contractual obligations that at least as protective as the terms specified in section [9.4.1](#).

9.4.5 *NOTICE AND CONSENT TO USE PRIVATE INFORMATION*

Requirements for notice and consent to use private information are defined in the respective Agreements and Sirar's Privacy Policy.

9.4.6 *DISCLOSURE PURSUANT TO JUDICIAL/ADMINISTRATIVE PROCESS*

Any disclosure shall be handled in accordance with Sirar's Privacy Policy.

9.4.7 *OTHER INFORMATION DISCLOSURE CIRCUMSTANCES*

Any disclosure shall be handled in accordance with Sirar's Privacy Policy.

9.5 *INTELLECTUAL PROPERTY RIGHTS*

Sirar retains exclusive rights to any products or information developed under or pursuant to this CP.

9.6 *REPRESENTATIONS AND WARRANTIES*

9.6.1 *CA REPRESENTATIONS AND WARRANTIES*

Sirar provides representations and warranties in accordance with this CP, respective agreements and applicable laws and regulations as below:

- Providing the operational infrastructure and certification services;
- Making reasonable efforts to ensure it conducts an efficient and trustworthy operation. "Reasonable efforts" include but are not limited to operating in compliance with:
 - Documented CP and CPS;
 - Documented Sirar's Operations Policies and Procedures; and
 - Within applicable agreements, Saudi Law and regulations.
- At the time of Certificate issuance; Sirar's implemented procedure for verifying accuracy of the information contained within it before installation and first use;
- Implemented a procedure for reducing the likelihood that the information contained in the Certificate is not misleading;
- Maintaining 24x7 publicly accessible repositories with current information and replicates the relevant certificate information as well as CRLs;
- For the CA's, the Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the CA keys and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key CA private key is generated using multi-person control "m-of-n" split key knowledge scheme;

- Backing up of the CA signing Private Key is under the same multi-person control as the original Signing Key;
- Keep confidential, any passwords, PINs or other personal secrets used in obtaining authenticated access to PKI facilities and maintain proper control procedures for all such personal secrets;
- Use its private signing key only to sign certificates and CRLs and for no other purpose;
- Perform authentication and identification procedures in accordance with applicable Agreement and Sirar's Operations Policies and Procedures;
- Provide certificate and key management services in accordance with the CP and CPS; and
- Ensure that CA personnel use private keys issued for the purpose of conducting CA duties only for such purposes.

9.6.2 *RA REPRESENTATIONS AND WARRANTIES*

Sirar warrant that it performs registration functions as per the stipulations specified in this CP and the CPS.

9.6.3 *RELYING PARTIES REPRESENTATIONS AND WARRANTIES*

Relying Parties who rely upon the certificates issued under the Intermediary CA shall:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Verify the Validity by ensuring that the Certificate has not expired;
- Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 amendment;
- Ensure that the Certificate has not been revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon; and
- Determining that such Certificate provides adequate assurances for its intended use.

9.6.4 *SUBSCRIBER REPRESENTATIONS AND WARRANTIES*

No Stipulation. The Intermediary CA does not issue certificates to third-party subscribers.

9.6.5 *REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS*

No stipulation.

9.7 *DISCLAIMERS OF WARRANTIES*

Sirar, through its associated components, seeks to provide digital certification services according to international standards and best practices, using the most secure physical and electronic installations.

Sirar provides no warranty, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of the Intermediary CA or for the legal validity, acceptance or any other type of recognition of its own certificates, those issued by it

through its Subordinate Issuing CAs, any digital signature backed by such certificates, and any products provided by Sirar. Sirar further disclaims any warranty of merchantability or fitness for a particular purpose of the above-mentioned certificates, digital signatures and products.

9.8 LIMITATIONS OF LIABILITY

Limitations on Liability:

- Sirar will not incur any liability to any person to the extent that such liability results from their negligence, fraud or willful misconduct;
- Sirar assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under Certificate Policy for any use other than in accordance with Certificate Policy. Relying Parties will immediately indemnify Sirar from and against any such liability and costs and claims arising there from;
- Sirar will not be liable to any party whosoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services;
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations described in the Relying Party agreement;
- Sirar denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

9.9 INDEMNITIES

Notwithstanding any limitations on its liability to its Sub-CAs and Relying Parties, Sirar understands and acknowledges that the Application Software Suppliers who have supplied the CA software in use by the Intermediary CA do not assume any obligation or potential liability of Sirar under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, Sirar SHALL defend, indemnify and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the Intermediary CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the Intermediary CA 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 the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

Sirar shall indemnify, defend and hold harmless the following parties:

- Its directors, officers, employees, agents, consultants, and subsidiaries from any and all claims, damages, costs (including, without limitation, attorney's fees), judgments, awards or liability;
- Any parties relying on the Intermediary CA Certificates or arising as a result of an infringement or violation of any patents, copyrights, trade secrets, licenses, or other property rights of any third party.

9.10 TERM AND TERMINATION

9.10.1 TERM

This CP shall be effective upon approval by the PKI Committee. The NCDC shall be notified of all changes to this document. Once the CP becomes effective it is published in the repository. Amendments to this CP upon approval become effective and replace the older version in the repository.

9.10.2 TERMINATION

This CP as amended from time to time shall remain in force until it is replaced by a new version. The latest version of this CP can be found at: <https://sirar.com.sa/repository/>.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this CP, all the Intermediary CA participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

All communication between NCDC, NCDC PA, Saudi National Root CA, and Sirar, the Intermediary CA shall be in writing or via digitally signed communication. If in writing, the communication shall be signed on the appropriate organization letterhead. If electronically, a Digital Signature shall be made using a Private Key whose companion Public Key is certified using a Certificate meeting this CP's Certificate assurance level.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

The PKI Committee shall review this CP at least once per year. Errors, updates, or suggested changes to this CP shall be communicated to the PKI Committee and/or NCDC. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change. Any technical changes in the Intermediary CA shall be managed as per the Sirar's Change Management Policy.

Intermediary CA reserves the right to change this CP from time to time. Intermediary CA will incorporate any such change into a new version of this CP and, upon approval, publish the new version. The new CP will carry a new version number.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

The PKI Committee reserves the right to amend this CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URL's, and changes to contact information. All the Saudi PKI participants and other parties designated by the PKI Committee shall provide their comments to the PKI Committee in accordance with NCDC rules.

The PKI Committee's decision to designate amendments as material or non-material shall be at the PKI Committee's sole discretion.

Any changes to this CP shall be made available within two weeks of approval by NCDC.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

The policy OID shall only change if the change in the CP results in a material change to the trust by the relying parties, as determined by Sirar.

9.13 DISPUTE RESOLUTION PROCEDURES

Any dispute arising out of or related to the digital certificates issued by the Intermediary CA shall initially be submitted to voluntary mediation. If mediation is not successful, then the dispute will be resolved by binding arbitration, in accordance with Sirar's Dispute Resolution Policy.

9.13.1 DISPUTE RESOLUTION COMMITTEE

The Sirar Dispute Resolution Committee will arbitrate on all claims or disputes arising out of or related to the operation of Sirar's CAs.

9.13.2 DISPUTE RESOLUTION POLICY

Sirar's Dispute Resolution Policy is applicable to all participants of Sirar's PKI.

9.14 GOVERNING LAW

This CP will be governed and construed in accordance with the laws of the Kingdom of Saudi Arabia.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP is subject to applicable national, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

No stipulation.

9.16.2 ASSIGNMENT

Except where specified by other contracts, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of Sirar.

9.16.3 SEVERABILITY

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section [9.12](#).

9.16.4 ENFORCEMENT (ATTORNEY FEES/WAIVER OF RIGHTS)

This document shall be treated according to laws of Kingdom of Saudi Arabia. Legal disputes arising from the operation of the Intermediary CA will be treated according to the laws of the Kingdom of Saudi Arabia.

9.16.5 FORCE MAJEURE

The Intermediary CA shall not be in default or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms of this CP or the Intermediary CA CP or any other related agreement due to any causes beyond its reasonable control, which causes include, without limitation, acts of God, riots and insurrections, terrorist activities, war, accidents, fire, strikes and other labour difficulties, embargoes, judicial action specifically preventing the operation of the Intermediary CA, lack of or inability to obtain energy, or utilities, or acts of civil or military authorities.

9.17 OTHER PROVISIONS

9.17.1 FIDUCIARY RELATIONSHIPS

Nothing contained in this CP shall be deemed to constitute either Sirar, or any of its subcontractors, agents, officers, suppliers, employees, partners, principals, or directors to be a partner, Affiliate, trustee, of any Relying Party or any third party, or to create any fiduciary relationship between Sirar and any Relying party, or any third party, for any purpose whatsoever.

Nothing in this CP or any Agreement between a third party and a Relying Party shall confer on any Customer, Relying Party, Applicant or any third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of Sirar.

9.17.2 ADMINISTRATIVE PROCESSES

As specified in Sirar Operations Policies and applicable Agreement.