TIMESTAMPING CA (TSCA) CERTIFICATION PRACTICE STATEMENT

Document Classification:

Public

Version Number: 1.0

Issue Date: 08 Feb 2026

Document Reference

Item	Description
Document Title:	sirar Timestamping CA (TSCA) Certificate Practice Statement
Custodian Department:	sirar's Product Management
Owner:	sirar's Policy Authority
Version Number:	1.0
Document Status:	Final

Document Author:	sirar's Policy Authority	
	PKI Consultant	Signature/Date
Document Reviewer:	Thaar F. AlOtaibi	Thaar alotaibi
	Managed Security Services General Manager	Signature/Date
Approved by:	Aiman H. AlJumoay	Aiman AlJumoay
	Chief Managed Services Officer	Signature/Date

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	08/02/2026	sirar's Policy Authority	Final incorporating reviews

Document Control

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

Digitally Signed Copy of this document shall be stored at sirar's PKI Repository.

Table of Contents

1 Introduction 10

1.1 Overview 10
1.1.1 sirar's PKI Hierarchy 11
1.1.2 Certificate Policy 12
1.1.3 Relationship between the CP and the CPS 12
1.1.4 Interaction with other PKIs 12
1.1.5 Scope 12

1.2 Document Name and Identification 12

1.3 PKI Participants 12
1.3.1 Certification Authorities 13
1.3.2 Registration Authority (RA) 13
1.3.3 Subscribers 13
1.3.4 Relying Parties 14
1.3.5 Other participants 14

1.4 Certificate Usage 14
1.4.1 Appropriate Certificate Uses 14
1.4.2 Prohibited Certificate Uses 15

1.5 Policy Administration 15
1.5.1 Organization Administering the Document 15
1.5.2 Contact Person 15
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 16

2.1 Repositories 16

2.2 Publication of Certification Information 16
2.2.1 Publication of Certificates and Certificate Status 16
2.2.2 Publication of CA Information 16
2.2.3 Interoperability 16

2.3 Time or Frequency of Publication 16

2.4 Access Controls on Repositories 17

3 Identification and Authentication 18

3.1 Naming 18
3.1.1 Types of Names 18
3.1.2 Need for Names to be Meaningful 18
3.1.3 Anonymity or Pseudonymity of Subscribers 18
3.1.4 Rules for Interpreting Various Name Forms 18
3.1.5 Uniqueness of Names 18
3.1.6 Recognition, Authentication and Role of Trademarks 18

3.2 Initial Identity Validation 19
3.2.1 Method to Prove Possession of Private Key 19
3.2.2 Authentication of Organization Identity 19
3.2.3 Identity-Proofing of Individual Identity 20
3.2.4 Non-verified Subscriber Information 20
3.2.5 Validation of Authority 20
3.2.6 Criteria of Interoperation 20

3.3 Identification and Authentication for Re-key Requests 20
3.3.1 Identification and Authentication for Routine Re-Key 20
3.3.2 Identification and Authentication for Re-key After Revocation 21

3.4 Identification and Authentication for Revocation Requests 21

4 Certificate Life-Cycle Operational Requirements 22

4.1 Certificate Application 22
4.1.1 Who Can Submit a Certificate Application 22
4.1.2 Enrollment Process and Responsibilities 22

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 23
4.3.1 CA Actions During Certificate Issuance 24
4.3.2 Notification to subscriber by the CA of issuance of certificate 24

4.4 Certificate Acceptance 24
4.4.1 Conduct Constituting Certificate Acceptance 24
4.4.2 Publication of the Certificate by the CA 25
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 25

4.5 Key Pair and Certificate Usage 25
4.5.1 Subscriber Private Key and Certificate Usage 25
4.5.2 Relying Party Public Key and Certificate Usage 25

4.6 Certificate Renewal 25
4.6.1 Circumstances for Certificate Renewal 26
4.6.2 Who may request Certificate Renewal 26
4.6.3 Processing Certificate Renewal Requests 26
4.6.4 Notification of Renewed Certificate Issuance 26
4.6.5 Conduct constituting acceptance of a renewal certificate 26
4.6.6 Publication of a Renewal Certificate 26
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 27
4.7.4 Notification of New Certificate Issuance to Subscriber 27
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 27
4.7.6 Publication of the Re-keyed Certificate by the CA 27
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 27

4.8 Certificate Modification 27

4.9 Certificate Revocation and Suspension 27
4.9.1 Circumstance for Revocation of a Certificate 28
4.9.2 Who Can Request Revocation of a Certificate 28
4.9.3 Procedure for Revocation Request 29
4.9.4 Revocation Request Grace Period 29
4.9.5 Time within which CA must Process the Revocation Request 29
4.9.6 Revocation Checking Requirements for Relying Parties 29
4.9.7 CRL Issuance Frequency 29
4.9.8 Maximum Latency of CRLs 30
4.9.9 Online Revocation Checking Availability 30
4.9.10 Online Revocation Checking Requirements 30

4.9.11 Other Forms of Revocation Advertisements Available 30
4.9.12 Special Requirements Related To Key Compromise 30
4.9.13 Circumstances for Certificate Suspension 30
4.9.14 Who Can Request Suspension 30
4.9.15 Procedure for Suspension Request 30
4.9.16 Limits on Suspension Period 30

4.10 Certificate Status Services 30
4.10.1 Operational Characteristics 31
4.10.2 Service Availability 31

4.11 End of Subscription 31

4.12 Key Escrow and Recovery 31

5 Facility Management and Operational Controls 32

5.1 Physical Security Controls 32
5.1.1 Site Location and Construction 32
5.1.2 Physical Access 32
5.1.3 Power and Air Conditioning 32
5.1.4 Water Exposure 33
5.1.5 Fire Prevention and Protection 33
5.1.6 Media Storage 33
5.1.7 Waste Disposal 33
5.1.8 Off-Site Backup 33

5.2 Procedural Controls 33
5.2.1 Trusted Roles 33
5.2.2 Number of Persons Required per Task 34
5.2.3 Identification and Authentication for Each Role 34
5.2.4 Separation of Roles 34

5.3 Personnel Controls 34
5.3.1 Background, Qualifications and Experience Requirements 34
5.3.2 Background Check and Clearance Procedures 34
5.3.3 Training Requirements 35
5.3.4 Retraining Frequency and Requirements 35
5.3.5 Job Rotation Frequency and Sequence 35
5.3.6 Sanctions for Unauthorized Actions 35
5.3.7 Contracting Personnel Requirements 35
5.3.8 Documentation Supplied to Personnel 35

5.4 Audit Logging Procedures 36
5.4.1 Types of Events Recorded 36
5.4.2 Frequency for Processing and Archiving Audit Logs 37
5.4.3 Retention Period for Audit Log 37
5.4.4 Protection of Audit Log 38
5.4.5 Audit Log Backup Procedures 38
5.4.6 Audit Collection System (Internal or External) 38
5.4.7 Notification to Event-Causing Subject 38
5.4.8 Vulnerability Assessments 38

5.5 Records Archival 38
5.5.1 Types of Events Archived 38
5.5.2 Retention Period for Archive 39
5.5.3 Protection of Archive 39
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 40
5.7.1 Incident and Compromise Handling Procedures 40
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 40
5.7.3 CA Private Key Compromise Recovery Procedures 40
5.7.4 Business Continuity Capabilities after a Disaster 40
5.8 CA OR RA Termination 41
5.8.1 CA Termination 41
5.8.2 RA Termination 42
6 Technical Security Controls 43
6.1 Key Pair Generation and Installation 43
6.1.1 Key Pair Generation 43
6.1.2 Private Key Delivery to Subscribers 43
6.1.3 Public Key Delivery to Certificate Issuer 44
6.1.4 CA Public Key Delivery to Relying Parties 44
6.1.5 Key Sizes 44
6.1.6 Public Key Parameters Generation and Quality Checking 44
6.1.7 Key Usage Purposes 44
6.2 Private Key Protection and Crypto-Module Engineering Controls 44
6.2.1 Cryptographic Module Standards and Controls 44
6.2.2 Subscriber Private Key Multi-Person Control 44
6.2.3 Private Key Escrow 45
6.2.4 Private Key Backup 45
6.2.5 Private Key Archival 45
6.2.6 Private Key Transfer Into or From a Cryptographic Module 45
6.2.7 Private Key Storage on Cryptographic Module 45
6.2.8 Method of Activating Private Keys 45
6.2.9 Methods of Deactivating Private Keys 45
6.2.10 Methods of Destroying Private Keys 45
6.2.11 Cryptographic Module Rating 45
6.3 Other Aspects of Key Pair Management 46
6.3.1 Public Key Archive 46
6.3.2 Certificate Operational Periods and Key Usage Periods 46
6.4 Activation Data 46
6.4.1 Activation Data Generation and Installation 46
6.4.2 Activation Data Protection 46
6.4.3 Other Aspects of Activation Data 46
6.5 Computer Security Controls 46
6.5.1 Specific Computer Security Technical Requirements 46
6.5.2 Computer Security Rating 47
6.6 Life-Cycle Security Controls 47
6.6.1 System Development Controls 47
6.6.2 Security Management Controls 47
6.6.3 Life Cycle Security Ratings 47
6.7 Network Security Controls 47
6.8 Time Stamping 47
7 Certificate, CRL and OCSP Profiles 49

7.1 Certificate Profile....49
7.1.1 Version Numbers....51
7.1.2 Certificate Extensions....51
7.1.3 Algorithm Object Identifiers....51
7.1.4 Name Forms....51
7.1.5 Name Constraints....51
7.1.6 Certificate Policy Object Identifier....51
7.1.7 Usage of Policy Constraints Extension....51
7.1.8 Policy Qualifiers Syntax and Semantics....51
7.1.9 Processing Semantics for the Critical Certificate Policy Extension....51

7.2 CRL Profile....51
7.2.1 CRL Profile....52
7.2.2 Version Numbers....52
7.2.3 CRL and CRL Entry Extensions....52

7.3 OCSP Profile....52
7.3.1 Version Number....53
7.3.2 OCSP Extensions....53

8 Compliance Audit and Other Assessments....53

8.1 Frequency of Audit or Assessments....54

8.2 Identity and Qualifications of Assessor....54

8.3 Assessor's Relationship to Assessed Entity....54

8.4 Topics Covered By Assessment....54

8.5 Actions Taken As A Result of Deficiency....54

8.6 Communication of Results....55

9 Other Business and Legal Matters....56

9.1 Fees....56
9.1.1 Certificate Issuance/Renewal Fee....56
9.1.2 Certificate Access Fees....56
9.1.3 Revocation or Status Information Access Fee....56
9.1.4 Fees for Other Services....56
9.1.5 Refund Policy....56

9.2 Financial Responsibility....56
9.2.1 Insurance Coverage....56
9.2.2 Other Assets....56
9.2.3 Insurance/warranty Coverage for End-Entities....56

9.3 Confidentiality of Business Information....57
9.3.1 Scope of Confidential Information....57
9.3.2 Information not within the Scope of Confidential Information....57
9.3.3 Responsibility to Protect Confidential Information....58

9.4 Privacy of Personal Information....58
9.4.1 Privacy Plan....58
9.4.2 Information Treated as Private....58
9.4.3 Information not Deemed Private....58
9.4.4 Responsibility to Protect Private Information....58
9.4.5 Notice and Consent to Use Private Information....58
9.4.6 Disclosure Pursuant to Judicial/Administrative Process....58
9.4.7 Other Information Disclosure Circumstances....58

9.5 Intellectual Property Rights....59

9.6 Representations and Warranties 59
9.6.1 CA Representations and Warranties 59
9.6.2 RA Representations and Warranties 60
9.6.3 Relying Parties Representations and Warranties 60
9.6.4 Subscriber Representations and Warranties 60
9.7 Disclaimers of Warranties 61
9.8 Limitations of Liability 61
9.9 Indemnities 61
9.10 Term and Termination 62
9.10.1 Term 62
9.10.2 Termination 62
9.10.3 Effect of Termination and Survival 62
9.11 Individual Notices and Communications with Participants 62
9.12 Amendments 62
9.12.1 Procedure for Amendment 62
9.12.2 Notification Mechanism and Period 62
9.12.3 Circumstances under which OID must be changed 63
9.13 Dispute Resolution Procedures 63
9.14 Governing Law 63
9.15 Compliance with Applicable Law 63
9.16 Miscellaneous Provisions 63
9.16.1 Entire Agreement 63
9.16.2 Assignment 63
9.16.3 Severability 63
9.16.4 Enforcement (Attorney Fees/Waiver of Rights) 63
9.16.5 Force Majeure 63
9.17 Other Provisions 64
9.17.1 Fiduciary Relationships 64
9.17.2 Administrative Processes 64
Appendix-A: TSU Certificate Policy 65

1 INTRODUCTION

The Government of Saudi Arabia has embarked on an ambitious e-transaction program, recognizing that there is a tremendous opportunity to better utilize information technology to improve the quality of care/service, lower the cost of operations, and increase customer satisfaction. To ensure the secure, efficient transmission and exchange of information electronically, the Kingdom of Saudi Arabia has established the “Saudi National PKI” that consists of:

- The shared National PKI Center at National Information Center (NIC-PKIC) hosts and operates the Saudi National Root CA and the Government CA,
- The regulator of Digital Trust Services in the Kingdom of Saudi Arabia being the Digital Government Authority (DGA),
- Commercial Certification Authorities (CAs) owned and operated by Digital Trust Service Providers (DTSPs) that are expressly approved by NIC.

sirar, a subsidiary of the Saudi Telecommunications Company (STC) is an approved DTSP under the Saudi National PKI. sirar has established its own PKI infrastructure offering digital trust services designed to enable electronic signature and authentication services for business entities and individuals.

This CPS complies with the following requirements:

- Saudi National PKI Policy,
- The Issuing CAs CP (hereafter, “CP”),
- RFC3647 — Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Sections that are not applicable 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, and
- Adobe Approved Trust List (AATL) Certificate policies.

1.1 OVERVIEW

This Certification Practice Statement (CPS) establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of the digital certificates issued by the Timestamping CA (hereinafter, TSCA), as governed by the Issuing CAs Certificate Policy (hereinafter, the CP).

More specifically, this CPS describes the practices that the TSCA employs for:

- Securely managing the core infrastructure hosting the TSCA;
- Issuing, managing, revoking, and renewing TSU certificates used to support the issuance of Time-Stamp Tokens (TSTs); and
- Implementing the technical, procedural, and personnel controls in accordance with the requirements of the CP.

Any use of or reference to this CPS outside the context of the TSCA and the Saudi National PKI is entirely at the using party’s risk. The terms and provisions of this CPS shall be interpreted under, and governed by, the CP and sirar’s Operations Policies and Procedures.

It is the responsibility of all parties relying on the TSU Certificates or the resulting Time-Stamp Tokens issued under this CPS to read the CP in order to understand the practices established for the lifecycle management of TSU Certificates issued by the TSCA.

1.1.1 SIRAR'S PKI HIERARCHY

sirar's PKI comprises an intermediary CA that is called "STCS Intermediary CA" (hereinafter, the Intermediary CA), the Intermediary CA is root signed by the Saudi National Root CA. Underneath the Intermediary CA, there are subordinate Issuing Certificate Authorities (hereinafter, Issuing CAs) responsible for issuing certificates to end-users.

Some Issuing CAs are owned by sirar and issue certificates to sirar's subscribers, while others are owned by third-party DTSPs but operated by sirar on their behalf. This service allows DTSPs to outsource the hosting and operation of their Issuing CAs to sirar. Policies and procedures of the issuing CAs belonging to third-party DTSPs must follow and be in full compliance with this CPS as well as other applicable policies and standards under sirar's PKI.

sirar's own issuing CAs signed by the Intermediary CA are:

- STCS Qualified Certificate Authority (STCS QUCA),
- STCS Identity Certificate Authority (STCS IDCA), and
- sirar Timestamping Certificate Authority

The full hierarchy of sirar's PKI is indicated below:

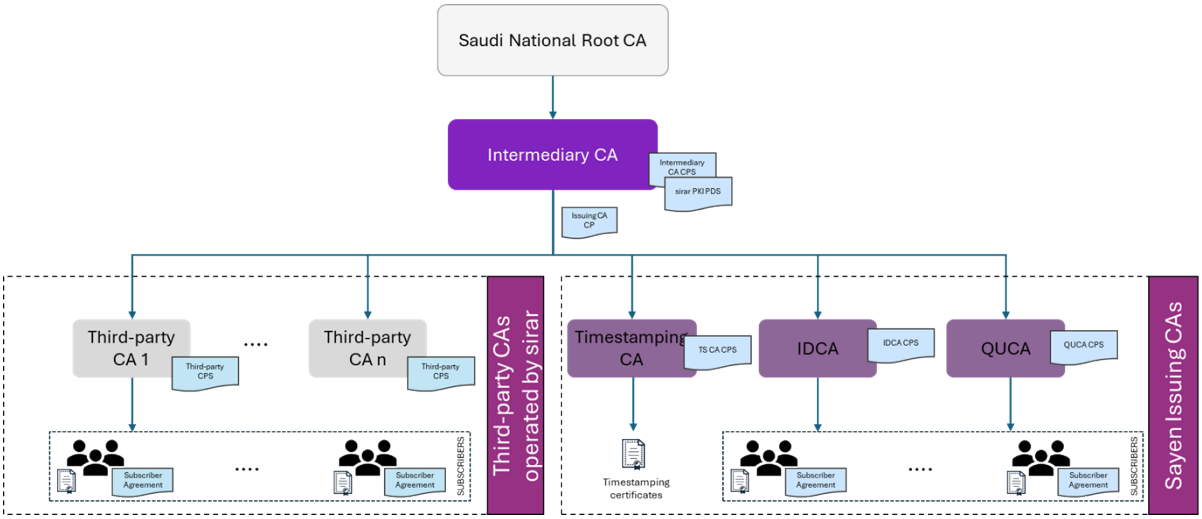

Figure 1-sirar's PKI and Governance Hierarchy

Issuing CAs owned by third-party DTSPs shall be approved by sirar's PKI Committee under the following conditions:

- The Issuing CA(s) must be hosted within sirar's PKI environment and operated under the oversight of sirar's PKI Committee;
- The business practices and services of the Issuing CA(s) may be defined by their owners, provided that the CPS complies with this CPS and other applicable policies and standards under sirar's PKI;

- The final CPS document must be reviewed, approved, and published by sirar's PKI Committee;
- The Issuing CA(s) must be technically constrained, using Extended Key Usage, to restrict the scope within which they may issue end-user certificates;
- Third-party DTSPs operating Issuing CA(s) signed by the Intermediary CA are responsible for the issuance and lifecycle management of the certificates they generate. They must also perform regular compliance audits of their Registration Authorities (RAs) to ensure adherence to applicable identification and authentication requirements;
- The certificate(s) of the Issuing CA(s) SHALL be revoked if the agreement between sirar and the third-party DTSP is terminated.

1.1.2 CERTIFICATE POLICY

X.509 certificates issued by the TSCA to subscribers contain a registered OID in the certificate policy extension that in turn may be used by a Relying Party (RP) to decide whether a certificate is trusted for a particular purpose.

1.1.3 RELATIONSHIP BETWEEN THE CP AND THE CPS

This CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of TSU certificates issued by the Timestamping CA (TSCA), as governed by the CP and related documents that describe the TSCA requirements and the use of TSU Certificates and Time-Stamp Tokens.

1.1.4 INTERACTION WITH OTHER PKIS

The TSCA does not directly interact with other external Certificate Authorities, it will only be chained to the STCS Intermediary CA.

1.1.5 SCOPE

This CPS applies to all certificates issued by the TSCA. The TSCA is operated under the sirar's PKI hierarchy, maintained and operated by sirar for issuance and management of certificates and revocation lists under the hierarchy.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the TSCA Certification Practice Statement (CPS), and is identified by the following object identifier (OID):

OID: 2.16.682.1.101.5000.1.4.1.2.1.31.

1.3 PKI PARTICIPANTS

The following are roles relevant to the administration and operation of the TSCA under the CPS.

Several parties constitute the participants of the TSCA. The parties mentioned hereunder, including the Certification Authorities, sirar's 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 sirar's Issuing CAs as well as the issuing CAs belong to third-party DTSPs. 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 the Issuing CAs CP and each respective 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 CAs and RAs;
- Performance of all aspects of the services, operations and infrastructure related to the sirar's PKI.
- Conduct regular internal security audits; and
- Assist in audits conducted by or on behalf of DGA.

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 NIC.

1.3.1.2 STCS Intermediary CA

The STCS Intermediary CA is an offline CA that is root signed by the Saudi National Root CA. It issues certificates to the Issuing CAs underneath sirar's PKI hierarchy, including the TSCA.

1.3.1.3 sirar Timestamping CA

The TSCA is an online Issuing CA that is signed by the STCS Intermediary CA, which in turn is root-signed by the Saudi National Root CA. It issues Timestamping Unit (TSU) certificates that are used exclusively for generating Time-Stamp Tokens (TSTs) to provide proof of existence for electronic data at a specific point in time.

1.3.2 REGISTRATION AUTHORITY (RA)

sirar runs its own RA function internally for this CA. the RA team is involved in validating and accepting certificate issuance and management operations, in addition to triggering related certification operations by the TSCA.

1.3.3 SUBSCRIBERS

Subscribers are the organizations that operate the Timestamping Units (TSUs) to whom TSU certificates are issued, including sirar itself. The Subscriber is legally responsible for the operation, management, and protection of the TSU and its private key. Subscribers are bound by the conditions of use of TSU certificates as defined in the Subscriber Agreement. In general, the Subscriber asserts that the TSU private key and corresponding certificate are used solely in accordance with the CP and this CPS to generate Time-Stamp Tokens (TSTs).

1.3.4 RELYING PARTIES

A Relying Party in this context is the entity that relies on the binding between an identity and a public key established by the TSCA. 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 TSCA. A Relying Party's right to rely on a certificate issued under this CPS, requirements for reliance, and limitations thereon, are governed by the terms of the CP and the Relying Party Agreement.

Relying Parties can rely on a certificate that has been issued under this CPS if:

- The certificate has been used for the purpose for which it has been issued, as described in this CPS
- 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 (hereinafter, 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. This committee is appointed by sirar.

1.3.5.2 sirar Policy Authority (sirar's PA)

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

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The TSCA issues certificates exclusively to Timestamping Units (TSUs) operated by sirar. TSU certificates are used solely for the generation of Time-Stamp Tokens (TSTs), providing cryptographic proof that specific electronic data existed at a particular point in time.

The TSCA issues TSU certificates under this CPS only to those Subscribers (organizations owning TSUs) who have signed their acceptance of a Subscriber Agreement in the appropriate form and whose application for TSU certificates has been approved by the TSCA.

Certificates	Description

• *TSU certificates*	These certificates are issued by the TSCA to create and verify electronic time stamps. TSU Certificates are issued under this CPS to sirar's Timestamping Units (TSUs) or other TSUs owned by approved organizations yet operated by sirar. Those TSUs are used to provide Time Stamping Service, in accordance with the Time Stamping Policy and Practice Statement, available under https://sirar.com.sa/repository/.

1.4.2 Prohibited Certificate Uses

Subscribers are authorized to use their certificates for the purposes specified in section 1.4.1 of this document. The use of certificates for any other purposes is strictly prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

1.5.2 Contact Person

Queries regarding this CPS shall be directed at:

Email: PolicyAuthority@sirar.com.sa

Telephone: 909

Any formal notices required by this CPS shall be sent in accordance with the notification procedures specified in section 9.12.2 of this CPS.

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS Approval Procedures

The CPS shall be effective upon approval by sirar's Committee. Procedure for approval and amendments are covered under section 9.12.1.

The approved changes shall be published as set forth in section 2.2.2.

1.6 Definitions and Acronyms

The Definitions and Acronyms terms used in this document shall have the same meaning as defined in the issuing CAs CP.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

sirar publishes relevant certificates and 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 that allow the PKI participants to make on-line enquiries regarding revocation and other certificate status information. TSCA provides PKI participants 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 contain the following PKI related elements:

- The TSCA certificate;
- TSU certificates for the timestamping unites operated by sirar; and
- CRLs: CRLs that are made publicly available to allow PKI participants to verify the status of certificates.

The TSCA publishes the CRLs including any changes since the publication of the previous CRL, at regular intervals. The URL where a CRL is published is mentioned in section 7.1 as part of the certificate profile of each certificate file.

2.2.2 PUBLICATION OF CA INFORMATION

This CPS is made available to all TSCA PKI Participants at sirar's Certificate Dissemination Webpage: https://sirar.com.sa/repository/. This Webpage is the only authoritative source for up-to-date documentation and TSCA reserves the right to publish newer versions of the documentation without prior notice. Additionally, the TSCA publishes an approved, current and digitally signed version of this CPS.

2.2.3 INTEROPERABILITY

Repositories used to publish CA certificate and CRLs are based on standard HTTP distribution points.

2.3 TIME OR FREQUENCY OF PUBLICATION

CRL publication is in accordance with section 4.9.7 of the CP. Other certificate status information is published in accordance with the provisions of this CPS.

Updates to this CPS are published in accordance with section 9.12.2.

This CPS 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 sirar's PKI Committee.

2.4 ACCESS CONTROLS ON REPOSITORIES

Certificates and certificate status information in sirar's PKI repository is 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 will protect repository information not intended for public dissemination or modification through the use of 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 CPS and the CP 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. Naming conventions for TSCA are approved by sirar's Policy authority, refer to section 7.1 where the naming conventions for different certificate types are specified.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The subject name contained in certificates issued by the TSCA ensures association exists between the name and the entity to which it belongs.

The Distinguished name (DN) of certificates and CRLs issued under the TSCA shall have the Issuer field set to the following (LDAP Notation):

CN= sirar Timestamping Certification Authority, O= sirar, CA=SA

The common name in the Subscriber DN will represent the Subscriber in a way that is easily understandable for humans. The certificate types supported by the TSCA are covered in Appendix-A of this document.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The TSCA is not issuing anonymous or pseudonymous certificates.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

The naming convention used by this TSCA is based on ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.5 UNIQUENESS OF NAMES

All distinguished names are unique across the TSCA. After a subscriber certificate expires or is revoked, the name can be re-used to re-issue a new certificate to the same subscriber.

The TSCA is configured in such a manner as to enforce name uniqueness for certificates that it issues. The TSCA is responsible for ensuring name uniqueness in subscriber certificates issued by it.

3.1.6 RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

Certificate applicants are prohibited from using names in their certificate application that infringe upon the Intellectual Property Rights of others. The TSCA and its RAs, however, does not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application.

The TSCA may revoke a Certificate upon receipt of a properly authenticated order from DGA, NIC, an arbitrator, or court of competent jurisdiction requiring the revocation of a Certificate or Certificates containing a Subject name in dispute.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

TSU private keys are generated within secure cryptographic modules under the control of the Subscriber organization operating the Timestamping Unit (TSU). Key generation is performed in a secure environment and is witnessed and documented in accordance with sirar's key management procedures.

The private key corresponding to the TSU certificate is securely generated and stored within a hardware cryptographic module (e.g., HSM) and never leaves the protection mechanisms of that module. A self-signed PKCS#10 Certificate Signing Request (CSR) is generated by the cryptographic module for submission to the TSCA.

The TSCA verifies the CSR during the certificate issuance process and confirms that the contents match the approved certificate request documentation. At a minimum, the TSCA verifies the following:

- The Subject Distinguished Name (DN) complies with the TSU certificate profile.
- The key length and algorithm meet the requirements defined in this CPS; and
- The CSR is signed using the private key corresponding to the public key contained in the CSR, thereby proving possession of the private key

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

For TSU certificates issued to third-party subscribers:

As the subject of the TSU certificate includes the organization's name, the TSCA or an RA shall verify the identity and address of the organization. The organization's address shall also be verified to confirm if it is the same address where the organization conducts its operation. The TSCA/RA shall verify these details using documentation provided by the applicant or verifying against any of the following:

- A government agency within the jurisdiction of the organization's legal existence or recognition.

- A third-party database that is periodically updated and considered a reliable data source; or

- An attestation letter written by a lawyer, a judge or other third party that is customarily relied upon for such information.

For more details on the collection and verification of information provided by the applicant, refer to Appendix-A that describes the processes based on the certificate type requirements defined by the TSCA.

For TSU certificates issued to sirar's TSA service: The verification of sirar's identity as the Subscriber is demonstrated through the documented operational key ceremony, which

establishes authorized control of the TSU and satisfies the organizational identity verification requirements.

3.2.3 IDENTITY-PROOFING OF INDIVIDUAL IDENTITY

Not applicable

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Non-verified information is NOT to be included in certificates issued under TSCA.

3.2.5 VALIDATION OF AUTHORITY

For TSU certificates issued to third-party subscribers:

Before certificate issuance, TSCA ensures that the applicant has specific rights, entitlements, or permissions to obtain a certificate on behalf of the organization that is operating the TSU. The following information is submitted by the applicant and verified by TSCA:

- The applicant must be an authorized person from the Organization requesting the certificate. In addition, the certificate application form needs to be signed by an authorizing representative from the Organization. The certificate application form can be alternatively authorized by an individual previously duly authorized/delegated by a verified authorized representative.
- Proof of Identity (e.g. national Identity document) of the applicant and the authorizing personnel.
- Contact details in the certificate application form shall be provided and verified by communicating, via a reliable means.

For OCSP certificates and TSU certificates issued to sirar's TSA service: The certification process is initiated by an authorized administrator under the supervision of the PKI Committee through a dedicated operational key ceremony documented by sirar.

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

Subscribers operating Timestamping Units (TSUs) are required to generate new key pairs at least once every year, consistent with the private key usage period defined in section 6.3.2. TSU certificates have a maximum validity period of three (3) years; however, the associated TSU private key shall not be used for a period exceeding one (1) year.

During the routine re-key process, the TSCA issues a new TSU certificate with the same subject information and certificate characteristics as the previous certificate, but with a newly generated key pair and a new serial number. The new certificate may be assigned a new validity period or retain a validity period aligned with the remaining lifecycle constraints defined in the CP.

Because TSU private keys must be regenerated annually, the TSCA will normally authenticate a re-key request using the currently valid TSU certificate. If authentication using the existing certificate is not possible, the identification and authentication steps for re-key shall follow the same procedures as applied during the initial issuance of the TSU certificate.

If, for any reason, the TSCA cannot verify the Subscriber's authorization to request a re-key using the existing certificate, or if the existing certificate is no longer valid, the re-key process shall follow the full initial certificate issuance procedures

The routine re-key of sirar's Timestamping (i.e., sirar's TSU) and the OCSP certificates is done according to sirar's internal Operations Policies and Procedures.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

If a TSU certificate is revoked, the Subscriber must undergo the same identification and authentication procedures required for the initial issuance of a TSU certificate in order to obtain a new one.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

For TSU certificates issued to third-party subscribers: Prior to the revocation of a Subscriber certificate, the TSCA shall verify that the revocation has been requested by an entity authorized to request revocation.

Acceptable procedures for authenticating the revocation requests include:

- Receiving a formal revocation request form fulfilling the following conditions:
    - The signature of a revocation request form by the subscriber or an authorized representative.
    - The verification of the identity of the requesters against the information available to the TSCA/RA (provided during the subscriber registration);
    - Communication with the Subscriber to provide reasonable assurances that the revocation request is authentic. Such communication, depending on the circumstances, may include one or more of the following: telephone, e-mail or courier service.
- Receiving a message from a Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked; or
- Communication with the requesting entity to provide reasonable assurances that the person or organization requesting revocation is who they claim to be. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

For OCSP certificates and TSU certificates issued to sirar's TSA service: certificate revocation is conducted as part of sirar's internal procedure that requires an approval from the PKI Committee.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The TSCA/RA performs the following steps when an applicant applies for a certificate:

- Establish the applicant's authorization to obtain a certificate;
- Establish and record the identity of the applicant; and
- Transmit to the TSCA a confirmation that the Applicant has met the authentication requirements and the information which is to appear in the Certificate.

The TSCA performs the following steps when it receives the confirmation and certificate information from the RA:

- Verify that the transmission is from an authorized RA;
- Verify the private key ownership by the applicant. This can be achieved by verifying the signature and information in the PKCS#10 request;
- Generate the Certificate relating to that Applicant; and
- Transmits the Certificate to the Applicant and/or to the requesting RA.

Communication between the TSCA and the RA is authenticated and protected from modification and by requiring the CA and RA to validate the integrity and authenticity of the messages. These communications are transmitted via a secure protocol. Where shared secrets are transmitted electronically, these transmissions are conducted over encrypted channels using cryptographic mechanisms that are commensurate with the strength of the public/private key pair being used. Any out-of-band communications will protect the confidentiality and integrity of the data.

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

Either the Applicant or an individual authorized to request certificates on behalf of the Applicant can submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to the TSCA.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

Applicants for TSU certificates shall follow the enrolment process defined in Appendix-A of this document.

4.1.2.1 TSU certificates issued to third-party subscribers:

Subscriber certificate applicants shall agree to the terms of the Subscriber Agreement and undergo an enrollment process consisting of:

- Completing a Certificate Application and providing true and correct information;
- Providing the required identity documentation and fulfilling the requirements for TSU certificates as defined in Appendix-A;
- Generating, or arranging to have generated, a key pair;
- Delivering his/her public key to the RA; and

- Demonstrating possession of the private key corresponding to the public key delivered to the RA, as specified in section 3.2.1 of this CPS.

4.1.2.2 OCSP certificates and TSU certificates issued to sirar's TSA service

The certification process is initiated by an authorized administrator under the supervision of the PKI Committee through a dedicated operational key ceremony documented by sirar.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

RAs shall perform identification and authentication of all required Subscriber information as described in section 3.2 of this CPS.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

For TSU certificates issued to third-party subscribers:

The TSCA/RA approves an application for a subscriber certificate if the following criteria are met;

- Successful identification and authentication of all required Subscriber information as described in the Subscriber Agreement and outlined in section 3.2 of this CPS.

The TSCA/RA rejects a certificate application if:

- Identification and authentication of all required Subscriber information as described in the Subscriber Agreement cannot be completed;
- The Subscriber fails to furnish supporting documentation upon request;
- The Subscriber fails to respond to notices within a specified time; or
- The TSCA/RA believes that issuing a certificate to the Subscriber may bring the TSCA into disrepute.

For OCSP certificates and TSU certificates issued to sirar's TSA service: a certificate application is approved/rejected as part of the corresponding operational procedure.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

Certification applications is processed within a commercially reasonable time in accordance with the CPS or any agreement signed with the PKI participants. The TSCA shall not be held liable for any processing delays initiated by the applicant or for events outside the CA's control.

4.3 CERTIFICATE ISSUANCE

When the TSCA/RA receives a request for certificate from a Subscriber, the TSCA/RA will:

- Verify the identity of the Subscriber;

- Verify the authority of the requestor and the integrity of the information in the certificate request;
- Ensure the subscriber signs the Subscriber Agreement;
- Verify that the subscriber possesses the private key corresponding to the Certificate Signing Request (CSR), for subscriber generated keys; and
- Submit the certificate request to the TSCA.

Upon receiving a validated certificate request from RA, the TSCA will create and sign the Subscriber certificate and deliver it to the Subscriber using a secure method.

All authorization and other attribute information received from an applicant organization are verified before inclusion in the TSU certificate, unless such verification is not required for specific attributes or identifiers defined in Appendix-A. The TSCA, through its RA, is responsible for verifying all data to be included in the certificate. At a minimum, the TSCA/RA shall follow the identification and authentication requirements described in Section 3.2 of the CP and this CPS.

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

Following successful completion of the registration process, the TSCA will create and sign the subscriber certificate if all certificate requirements have been met and make the certificate available to the requesting party. The following actions shall be performed by the TSCA

- Verify the source and authenticity of the request;
- Inspect the contents of the CSR to ensure accuracy;
- Sign the certificate signing request; and
- Notify the requesting party of the availability of the certificate.

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

The TSCA notifies Subscribers, either directly or through the RA that they have created the Subscriber Certificate and provide Subscribers with access to the Certificates by notifying them, using the email address provided during application, that their Certificates are available. For in-person applications, notification may also take the form of verbal notification.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Certificate acceptance is governed by the agreements set out between the RA and Applicants, any requirements imposed by CP, this CPS and the relevant agreements under which the certificate is being issued.

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

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

The TSCA, TSU and OCSP certificates are published on the dissemination page as described in Section 2.2.

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 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

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

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of private key(s) following expiration or revocation of the associated certificate.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Relying parties shall accept the terms of the Relying Party Agreement as a condition for relying on any of the TSCA Issued certificates. Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable. Before any act of reliance, Relying Parties shall independently assess:

- The appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by the CP. The Relying Party is solely responsible for assessing the appropriateness of the use of a Certificate;
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate; and
- The status of the certificate and all the CA's in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party shall not rely on the certificate or shall make its own determination given any reasons furnished for such a revocation.

If the Relying Party deems that the use of the Certificate is appropriate, it shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying the Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

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 TSCA issued certificates to Subscribers.

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

Not applicable.

4.6.2 WHO MAY REQUEST CERTIFICATE RENEWAL

Not applicable.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

Not applicable.

4.6.4 NOTIFICATION OF RENEWED CERTIFICATE ISSUANCE

Not applicable.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Not applicable.

4.6.6 PUBLICATION OF A RENEWAL CERTIFICATE

Not applicable.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not applicable.

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 have the same expiry date as the old certificate and may be signed using a different Issuing CA private key. Certificate re-key requests are processed as new Certificate requests when the expiry date is changed or any other information in the Certificate is different.

4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

Certificate re-key may happen while the certificate is still active, after it has expired, after a revocation, or when the user forgets the password protecting the private key corresponding to the subject certificate.

The re-key operation shall invalidate any existing active certificates of the same type.

4.7.2 WHO CAN REQUEST A CERTIFICATE RE-KEY

As per the initial certificate issuance.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

The TSCA follows procedures to ensure that the organization requesting the re-key of a TSU certificate is the authorized Subscriber operating the corresponding Timestamping Unit (TSU). Proof of possession of the TSU private key—demonstrated through the signature on the PKCS#10 Certificate Signing Request (CSR)—is the primary method used to authenticate routine re-key requests.

Other than the above mentioned procedures, the TSCA/RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in section 3.3.1 of this CPS for the authentication of an original Certificate Application.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Notification of issuance of a re-keyed certificate to Relying Parties follows the same procedures as notification for newly issued Subscriber certificates.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Conduct constituting acceptance of a re-keyed certificate is in accordance with section 4.4.1 of this CPS.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

Refer to section 4.4.2.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

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

4.8 CERTIFICATE MODIFICATION

The TSCA does not support any form of subscriber certificate modification. Should the subscriber wishes to change details of an existing certificate the following shall apply:

- The existing certificate shall be revoked;
- The new details requested shall be verified including the confirmation of the identity information of the subscriber; and
- Once the information is successfully validated a new certificate shall be issued the same way a new certificate is issued or through the re-key process.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

A 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 TSCA/RA will notify subscribers of certificate revocation using any or all of the below methods:

- Access to the CRL at the sirar's PKI repository;

- Email notification to subscriber (Such notification is deemed complete, once the email is sent by the TSCA to the subscriber's registered email address); or
- Telephonic notification to subscriber.

The TSCA will notify other participants of certificate revocation through access to the CRL and the OCSP responder.

4.9.1 CIRCUMSTANCE FOR REVOCATION OF A CERTIFICATE

The TSCA revokes Certificates of Subscribers for the following non-exhaustive reasons:

- A Subscriber contravened any provisions of the Saudi e-Transactions Act and Bylaws made there under;
- The Subscriber has failed to meet its obligations under this CPS or any other applicable Agreements, regulations, or laws;
- TSCA suspects or determines that revocation of a Certificate is in the best interest of the integrity of the CA;
- TSCA determines that a TSU Certificate was not issued correctly in accordance with this CPS;
- There has been an improper or faulty issuance of a certificate due to:
  - A material prerequisite to the issuance of the Certificate not being satisfied;
  - A material fact in the issued certificate is known, or reasonably believed, to be false.
- The Subscriber asks for his/her certificate to be revoked due to:
  - The Subscriber's private key is suspected to be compromised;
  - The cryptographic storage device of the Subscriber is lost or stolen;
  - If the Subscriber no longer wishes to use the certificate.
  - If the Subscriber is no longer part of the organization, i.e. affiliation to the organization is no longer valid; and
  - The Subscriber agreement has been terminated.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on a CRL and/or specified as revoked by an OCSP Responder.

4.9.2 WHO CAN REQUEST REVOCATION OF A CERTIFICATE

The following entities can request revocation of a certificate:

- DGA or NIC can request the revocation of any certificates issued by any CA participating in the Saudi National PKI;
- sirar itself may initiate revocation of a certificate in the cases described in section 4.9.1;
- The PKI Committee can request the revocation of any certificates issued under its authority;
- An RA can request the revocation of any of their Subscribers Certificate;

- Subscribers of a long-lived certificates, if any suspected misuse has been attributed to their given Certificates, can request a revocation; and

- A legal, judicial or regulatory agency in Saudi Arabia, can request certificate revocation, within applicable laws and in coordination with DGA.

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 TSCA authenticates the request as well as the authorization of the requester in accordance with the applicable Agreements.

4.9.3.1 Procedure for Requesting the Revocation of a Subscriber Certificate

The request for a subscriber certificate revocation is authenticated as described in section 3.4 of this CPS. The subscriber (or any authorized party) can follow an online or a manual process to request the revocation.

Upon successful authentication, the certificate shall be revoked and placed on a CRL which shall be issued in accordance with section 4.9.7 of this CPS while the OCSP Responder will be updated accordingly.

4.9.4 REVOCATION REQUEST GRACE PERIOD

Revocation request grace period is not permitted once a revocation request has been verified.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

TSCA processes authorized revocation requests within a commercially reasonable time.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

Relying Parties are required to comply with the Relying Party Agreement requirements for signature validation, which prescribe how certificate status information is to be obtained and used. Relying Parties may check Certificate status by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely upon. The CA provides Relying Parties with information on how to find the appropriate CRL, repository, and the OCSP responder to check for revocation status.

4.9.7 CRL ISSUANCE FREQUENCY

The TSCA publishes CRLs at regular intervals. The following rules apply for the CRLs issued by the TSCA:

- CRLs are refreshed every 24 hours;
- CRLs lifetime (i.e. value of the nextUpdate field) is set to 25 hours

4.9.8 MAXIMUM LATENCY OF CRLS

CRLs are issued timely by the TSCA as per the CRL issuance frequency listed in section 4.9.7 of this CPS.

4.9.9 ONLINE REVOCATION CHECKING AVAILABILITY

The OCSP service shall be available 24 hours a day with reasonable time allocated to maintenance.

4.9.10 ONLINE REVOCATION CHECKING REQUIREMENTS

The TSCA provides an Online revocation and status checking to its relying parties. The TSCA shall update information provided via an OCSP every 24 hours. The OCSP responses from this service expires in 25 hours.

The OCSP requests contains the following data:

- Protocol Version
- Service request
- Target certificate identifier

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

No other forms of revocation advertisements is provided other than the CRL and OCSP services.

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

No Stipulation, refer to section 4.9.1.

4.9.13 CIRCUMSTANCES FOR CERTIFICATE SUSPENSION

Certificate suspension is not supported by the TSCA.

4.9.14 WHO CAN REQUEST SUSPENSION

Not applicable.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

Not applicable.

4.9.16 LIMITS ON SUSPENSION PERIOD

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

Refer to section 4.9.6.

4.10.1 OPERATIONAL CHARACTERISTICS

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

The OCSP responder exposes an HTTP interface accessible to relying parties.

4.10.2 SERVICE AVAILABILITY

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

4.11 END OF SUBSCRIPTION

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

4.12 KEY ESCROW AND RECOVERY

The TSCA does not support Subscriber Key Escrow.

5 FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

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

sirar enforces 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 TSCA 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 layered protection against unauthorized access to the TSCA equipment and records.

5.1.2 PHYSICAL ACCESS

TSCA systems are 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 TSCA 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 is automatically logged, and video recorded. Additional tiers enforce individual access control through the use of biometric authentication. Unescorted personnel, including untrusted employees or visitors, should not be allowed into such secured areas. sirar employs 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 ensures 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 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 TSCA equipment has 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 TSCA 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 ensures that the TSCA systems are protected from exposure to water sources. Additional prevention mechanisms such as using raised flooring must be employed where possible to minimize flood water damaging equipment.

5.1.5 FIRE PREVENTION AND PROTECTION

The TSCA equipment is housed in a facility with appropriate fire suppression and protection systems.

5.1.6 MEDIA STORAGE

sirar ensures that TSCA media is stored so as to protect it 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 appropriately qualified and trusted or the integrity of the PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the TSCA. The following are the trusted roles for sirar's PKI:

- CA Administrator – general CA administration and approval of the generation, revocation of certificates
- CA Security Officer – overall responsibility for administering the implementation of the CA's security practices, cryptographic key lifecycle management functions
- 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 Key Shareholders – holders of the CA key components

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

sirar ensures 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 individuals shall fill each of the roles specified in the 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 TSCA certificate signing Private Key. Activation of the TSCA certificate signing Private Key shall require at least 3 people to present their credentials.

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 section5.2.1 of this CPS and the PKI Governance and Operating Model document. The TSCA shall ensure that no individual is assigned more than one Trusted Role, except where such assignment does not compromise segregation of duties and does not result in a conflict of interest.

5.3 PERSONNEL CONTROLS

5.3.1 BACKGROUND, QUALIFICATIONS AND EXPERIENCE 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 TSCA are set forth in the sirar's PKI Governance and Operating Model document.

5.3.2 BACKGROUND CHECK AND CLEARANCE PROCEDURES

sirar conducts background investigations for all sirar PKI personnel including trusted roles and management positions. Background checks 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 criminal record checks.

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

5.3.3 TRAINING REQUIREMENTS

sirar ensures 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.

sirar reviews and updates its training program at least once a year to accommodate changes in the CA system.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

sirar ensures 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

sirar takes 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 TSCA or sirar's PKI repository.

5.3.7 CONTRACTING PERSONNEL REQUIREMENTS

Contractor personnel employed to perform functions pertaining to 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 makes available to its personnel the 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 TSCA, 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:
    a. Certificate requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in these Requirements and the Issuing CA's Certification Practice Statement;
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of certificate requests;
    e. Issuance of Certificates; and
    f. Generation of Certificate Revocation Lists.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies;
    e. Firewall and router activities; and
    f. Entries to and exits from sirar's PKI facility.
    g. Equipment failure or electrical power outages
    h. Changes to CA configuration and system clock time

The PKI committee ensures that for TSCA, the following is as well recorded:

- Time-stamp requests and generated time-stamps .
- Events related to TSCA administration (including certificate management, key management, and clock synchronization)
- Events relating to the life cycle of TSA keys and certificates

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 FOR PROCESSING AND ARCHIVING AUDIT LOGS

The PKI Committee ensures that designated personnel review log files at regular intervals to validate log integrity and ensure timely identification of anomalous events. At a minimum, the following audit log review cycle is implemented by the PKI Committee:

- TSCA application and security audit logs shall be reviewed by the security operations team daily, as part of the regular daily operations
- On a monthly basis, PKI operations management reviews the applications and systems logs to validate the integrity of the logging processes and to test/confirm the daily monitoring function is being operated properly
- On a quarterly basis, PKI operation management reviews the physical access logs and the user management on the TSCA systems with an objective to continuously validate the on-going physical and logical access policies
- Every six (6) months, the internal audit and compliance function executes an internal audit of the TSCA operations.
- Evidence of audit log reviews, outcome of the review process, and executed remediation actions are collected and archived.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

sirar retains 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 protects 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 backs 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)

The audit log or journal is an integral part of the CA software. The audit system ensures the integrity of the audit data being collected. In case of the audit system stopping to function, the TSCA shall determine whether to suspend or continue with operations.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

Event-causing subjects are not notified.

5.4.8 VULNERABILITY ASSESSMENTS

Routine vulnerability assessments of security controls shall be performed by sirar for its Issuing CAs and other PKI supporting systems hosted in sirar's data centre. Such assessments shall be performed at least annually.

sirar's security program includes 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 also ensures 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

The TSCA archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA. The TSCA shall make these archived records available to its Qualified Auditor upon request. The data to be archived may include, but not limited to the following:

- Audit data, as specified in section 5.4
- Data related to certificate requests, verifications, issuances and revocations
- CA Procedures, policies, subscriber agreements and compliance records
- Cryptographic device and key lifecycle information
- Systems management and change control activities

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. TSCA's minimum retention period for archive data is established at ten (10) years.

The TSCA shall retain all documentation relating to the TSCA 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 individuals shall be permitted to review the archive. The contents of the archive shall not be released except as determined by NIC, the PKI Committee, or as required by law. Records and material information relevant to the use of, and reliance on, a certificate shall be archived. Archive media shall be stored in a secure storage facility separate from the original storage media. 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 TSCA 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 TSCA may periodically perform key rollover, allowing CA keys to be changed periodically as required to minimize risk to the integrity of the TSCA . 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. The old key shall be protected to the same degree as the active key.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

If sirar's 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 TSCA Private key is suspected of compromise, the procedures outlined in sirar's Incident Management Procedures shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the TSCA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

sirar invokes its Incident Management Procedures in the event of the following non-exhaustive events:

- Suspected or detected compromise of the CA system;
- Physical or electronic attempts to penetrate the CA system;
- Denial of Service attacks on a CA system component; and
- Any incident preventing a CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

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

the TSCA maintains backup copies of hardware, system, databases, and private keys in order to rebuild the TSCA capability in case of software and/or data corruption. If necessary, the procedures as outlined in the sirar's Operations Policy and Business Continuity Plan shall be enacted.

5.7.3 CA PRIVATE KEY COMPROMISE RECOVERY PROCEDURES

sirar maintains a Disaster Recovery Policies and Procedures. The recovery procedures shall contain procedures for the recovery of the CA private key, and same shall be followed in the case of the TSCA Private Key compromise.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

sirar has developed a robust Business Continuity Management System for critical PKI services to provide the minimum acceptable level of assurance to its subscriber for service availability.

All sirar's critical infrastructure equipment at the primary site (sirar's data centre) have built-in hardware fault-tolerance and configured to be highly available with auto-failover switching. sirar currently maintains 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.

sirar's Business Continuity Management System (BCMS) demonstrates the capability to restore critical PKI services at the disaster recovery site according to the following Recovery Time Objective (RTO):

- Repository (CRL and OCSP): 8 hours,
- Certificate Issuing Capability: 24 hours,
- Invoicing Capability: 72 hours.

sirar has developed a business continuity plan to mitigate the effects of any kind of natural, man-made or equipment failure related disaster. The business continuity plan is being regularly tested, verified, and updated to be operational to address crisis situation in the event of a disruption. For security reasons details of this plan are not publicly available.

sirar's business continuity plan includes:

- Conditions for activating the plan;
- Emergency procedures;
- Fall-back procedures;
- Resumption procedures;
- A maintenance schedule for the plan;
- Awareness and education requirements;
- The responsibilities of the individuals;
- Recovery time objective (RTO);
- Recovery point objective (RPO);
- Regular testing of contingency plans;
- The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
- Acceptable system outage and recovery time;
- Procedure/frequently of backup copies for essential business information and software are taken; and
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

5.8 CA OR RA TERMINATION

5.8.1 CA TERMINATION

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

- Ensure minimal disruption caused by the termination of the CA
- Ensure notification of Subscribers, Relying Parties and other relevant Stakeholders, such as the DGA and NIC
- 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 TSCA archival records in case of the termination of sirar's PKI.

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

5.8.2 RA TERMINATION

In the event of sirar terminating an RA, the termination shall be done in such a way to minimize the impact of the termination to the subscribers. Procedures for the termination of the RA shall be developed and shall at minimum address the following:

- Ensure minimal disruption caused by the termination of the RA
- Ensure notification of Subscribers, Relying Parties and other relevant Stakeholders
- Ensure process for revoking certificates are maintained

sirar shall ensure certificate records maintained by the terminated RA are kept secure and available.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

Key pair generation for the TSCA is performed in a controlled and secure environment and is witnessed and attested by an independent party who is not the TSCA operator or the CA administrator. All key generation activities are conducted in accordance with the approved Key Generation Script for the TSCA and are formally recorded to provide full traceability and assurance of compliance with this CPS and the CP.

Key Pair generation must 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. 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.

TSCA 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 TSCA key pair is generated in pre-planned Key Generation Ceremony in accordance with the requirements of NIC. 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.

For Subscriber keys generated in cryptographic hardware, the key pairs will be generated or protected, as the case may be, in cryptographic modules at least compliant to FIPS 140-2 Level 3 or higher.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBERS

For Timestamping Units (TSUs), private keys are generated and remain within the secure cryptographic module operated by sirar, including sirar itself. TSU private keys are never exported, delivered, or transferred outside the cryptographic module in plaintext or in any form that would allow duplication or compromise. The Subscriber is responsible for ensuring that TSU key generation, storage, activation, and use occur exclusively within a secure, validated cryptographic device.

Where TSU keys are generated by the Subscriber in its own cryptographic hardware, no delivery step is required, as the private key never leaves the device. The Subscriber shall ensure that no copy of the TSU private key is retained by any person or system and that the key cannot be activated, modified, or compromised during or after generation.

If sirar performs TSU key generation for its own operational TSUs, the process is executed strictly within a secure key ceremony and in accordance with sirar's internal Operations Policies and Procedures. In such cases, the private key is bound to the cryptographic module during the ceremony and is never exported or delivered outside the device.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Public keys can be delivered to the TSCA using standard secured delivery processes (e.g. PKCS#10 through e-mail or media exchange) and key management protocols (e.g., XKMS, PKIX CMP, SCEP, …).

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The TSCA Public Key is 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 below for all subscriber certificates issued by the TSCA. All FIPS-approved signature algorithms shall be considered acceptable. If NIC determines that the security of a particular algorithm may be compromised, it shall direct sirar to revoke the affected certificates.

The key lengths of certificates issued by the TSCA are at least 4096-bit RSA or at least 256-bit ECDSA; 521-bit ECDSA is recommended.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The TSCA generates its key pairs using cryptographic modules and processes that comply with FIPS 186 for random number generation and primality testing, or equivalent recognized standards providing comparable security. The TSCA shall use reasonable techniques to validate the suitability of the Subscriber key pairs.

6.1.7 KEY USAGE PURPOSES

Certificates issued to subscribers contain a key usage extension appropriate to their intended use, in accordance with RFC 5280. Refer to section 7.1 and 7.3 of this CPS.

6.2 PRIVATE KEY PROTECTION AND CRYPTO-MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

For the creation and storage of the TSCA private keys, Hardware Security Modules (HSMs) certified or compliant to FIPS 140-2 Level 3 are used. These HSMs are housed within the most secure and inner zone of the sirar's hosting facility, ensuring the highest level of protection against unauthorized access, tampering, or compromise.

6.2.2 SUBSCRIBER PRIVATE KEY MULTI-PERSON CONTROL

No Stipulation.

6.2.3 PRIVATE KEY ESCROW

TSCA's private keys are not escrowed, and the TSCA does not escrow Subscriber Private keys as it does not issue encryption certificates.

6.2.4 PRIVATE KEY BACKUP

The TSCA does not back up Subscriber private keys.

6.2.5 PRIVATE KEY ARCHIVAL

The TSCA does not offer data encryption services, thus does not support the archival of private keys.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

The TSCA does not permit subscriber key transfer into and out of cryptographic modules or devices. Subscriber keys are generated in secure cryptographic modules and shall not be transferred out of those modules.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

Subscriber keys are stored in at least FIPS 140-2 Level 3-compliant devices in encrypted form.

6.2.8 METHOD OF ACTIVATING PRIVATE KEYS

TSCA and TSU private keys are activated following the principles of dual control and split knowledge. The activation procedure shall use a PIN entry device attached to the hardware security module (i.e., HSMs).

6.2.9 METHODS OF DEACTIVATING PRIVATE KEYS

Private keys for the TSCA and TSU are deactivated in accordance with the instructions and documentation provided by the manufacturer of the hardware security module.

6.2.10 METHODS OF DESTROYING PRIVATE KEYS

Private keys for the TSCA and for TSUs operated by sirar shall be destroyed inside the cryptographic module using its approved key-deletion functions. These procedures shall ensure that the private key is permanently removed and cannot be recovered. The destruction process shall be carried out in accordance with documented procedures and witnessed by authorized Trusted Role members.

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 Subscriber 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	Maximum Validity Period
OCSP Signing Key	12 months
Timestamping signing Key (TSU)	36 months

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

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

6.4.2 ACTIVATION DATA PROTECTION

The subscriber 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 device is used to protect and shall not be stored with the cryptographic device.

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 TSCA Software complies 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

Purchased hardware or software are shipped in a sealed, tamper-proof container, and installed by qualified personnel.

Hardware and software updates shall be procured in the same manner as the original equipment.

Dedicated trusted personnel are involved in implementing the required Infrastructure CA configuration according to the documented operational procedures.

The TSCA hardware and software are tested, deployed, and configured in accordance with industry leading development and change management practices.

6.6.2 SECURITY MANAGEMENT CONTROLS

A configuration management process is enforced to ensure that the TSCA systems configuration, modification and upgrades are documented and controlled by the PKI operations management. A vulnerability management process is enforced to ensure that the TSCA equipment is scanned for malicious code on first use and periodically thereafter. The vulnerability management process prioritizes the processing of critical vulnerabilities not previously met by the Infrastructure operations team.

6.6.3 LIFE CYCLE SECURITY RATINGS

No Stipulation.

6.7 NETWORK SECURITY CONTROLS

sirar employs 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. The CA components are synchronized with a trusted time source being a Network Time Protocol (NTP) service.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

TSU Certificate Profile

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	[1]At least 64 bits of entropy, validated to avoid duplicate	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = sirar Timestamping Certification Authority O = sirar C = SA	V1 Field
NotBefore	Certificate generation process date/time.	V1 Field
NotAfter	Certificate generation process date/time + Up to 36 months	V1 Field
Subject	CN = <Timestamping Service name> O = <legal name of the Timestamping Service owner> OrganizationIdentifier=<National Unique Identifier e.g. VATSA-[VAT NUMBER]> C = SA	V1 Field
SubjectPublic KeyInfo	Key type: RSA / ECDSA Key length: 4096 (RSA) / 256 to 521 (ECDSA)	V1 Field
CRL Distribution Points	e.g. [1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.sirar.com.sa/CRL/sirar_tsca.crl	NO
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the STCS Identity CA (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING **subjectPublicKey** (excluding the tag, length, and number of unused bits).	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=<**2.16.682.1.101.5000.1.4.1.2.1.31**> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sirar.com.sa/repository [2]Certificate Policy: Policy Identifier=< **2.16.682.1.101.5000.1.4.1.2.2.1**> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sirar.com.sa/repository [3]Certificate Policy: Policy Identifier=<**2.16.682.1.101.5000.1.4.1.2.1.30.5**>	NO

[1] Applicable for the certificates issued after 2020/09/23 22:51:17.

Field / x.509 extension	Value or Value Constant	Critical
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: http://ocsp.sirar.com.sa/ [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://crl.sirar.com.sa/certs/sirar_tsca.crt	NO
Key Usage	digitalSignature	YES
Extended keyUsage	timeStamping	YES
Private Key Usage Period[2]	notBefore	NO
	notAfter	

[2] This extension indicates the period of use of the private key corresponding to the certified public key. A new Key pair will be generated each 12 months

7.1.1 VERSION NUMBERS

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

7.1.2 CERTIFICATE EXTENSIONS

X.509 v3 extensions are supported and used as indicated in the certificates profiles specified earlier in this section.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

TSCA 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).

7.1.4 NAME FORMS

Certificates issued by TSCA 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

Certificate policy object identifiers are used as an OID scheme specified for sirar's PKI. Refer to section 7.1 of this CPS for the details of the contents of the certificates issued by the TSCA including the values of the OID identifiers.

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 TSCA CRL Profile is shown below:

7.2.1 CRL PROFILE

Field	Content	Comment
Version	1 (Version 2)	
Algorithm	SHA256withRSA	
Issuer	CN = sirar Timestamping Certification Authority O = sirar C = SA	
This update	*<issue date>*	Date CRL was issued
Next update	*<issue date + 1 day>*	Or immediately upon revocation
AuthorityKeyIdentifier	The TSCA Subject Key Identifier	
CRL number	<number>	Integer that is incremented sequentially

7.2.2 VERSION NUMBERS

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

7.2.3 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

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	[3]At least 64 bits of entropy validated on duplicates.	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = sirar Timestamping Certification Authority O = sirar C = SA	V1 Field
NotBefore	Certificate generation process date/time.	V1 Field
NotAfter	Certificate generation process date/time + Up to 36 months (3 years)	V1 Field
Subject	CN = Sirar by stc TSCA OCSP Service O = STCS C = SA	V1 Field

Field / x.509 extension	Value or Value Constant	Critical
SubjectPublicKeyInfo	Key type: RSA/ECDSA Key length: 3072 or 4096 (RSA) / 256 to 521 (ECDSA)	V1 Field
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the **TSCA** (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING **subjectPublicKey** (excluding the tag, length, and number of unused bits).	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=<**2.16.682.1.101.5000.1.4.1.2.1.31**> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sirar.com.sa/repository [2]Certificate Policy: Policy Identifier=<**2.16.682.1.101.5000.1.4.1.2.1.30.6**>	NO
OCSP No Revocation Checking (id-pkix-ocsp-nocheck)		NO
Key Usage	digitalSignature, nonRepudiation	YES
Extended keyUsage	Id-kp-OCSPSigning	NO

7.3.1 VERSION NUMBER

The request shall use version 1 on the version request filed (populated with integer 0)

7.3.2 OCSP EXTENSIONS

OCSP extensions shall comply with stipulations in RFC6960. The TSCA shall sign the OCSP responses itself. Thus, it will not be necessary to populate the id-kp-OCSPSigning extension.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The PKI Committee shall be responsible for overseeing compliance of the TSCA with the CP and CPS. The PKI Committee shall ensure that the requirements of this CPS, the CP and the provisions of applicable Agreements with subscribers are implemented and enforced. The TSCA shall undergo annual WebTrust audits, the results of which shall be submitted to DGA if requested.

The PKI Committee shall also ensure periodical audits (at least annually) to its RAs are conducted to ensure compliance with the RA agreements and provisions of the CP and this CPS.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The TSCA shall be subject to periodic WebTrust compliance audits which are no less frequent than once a year. Similarly, sirar's PKI Committee has the right to require periodic inspections of its RAs to validate that the RAs are operating in accordance with the CP, CPS and/or RA agreement. sirar may internally audit each delegated third party's compliance against defined requirements on an annual basis.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The annual audit of the TSCA 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 sirar 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 TSCA is audited for compliance with the AICPA/CICA Trust Service Principles and Criteria for Certification Authorities.

The auditor shall provide sirar and/or DGA with a compliance report highlighting any discrepancies.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If irregularities are found by the auditor, sirar shall be informed in writing of the findings. sirar shall submit a report to the auditor or directly to DGA, as determined by DGA, as to any remedial action sirar will take in response to the identified deficiencies. This report shall include a time for completion to be approved by the auditor, or by DGA as appropriate.

Where sirar fails to take remedial action in response to the identified deficiencies, DGA shall be informed by the auditor and shall take the appropriate action, according to the severity of the deficiencies.

8.6 COMMUNICATION OF RESULTS

An Audit Compliance Report, including identification of corrective measures taken or being taken by sirar, shall be provided to sirar and/or DGA as applicable.

sirar 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 rekey.

9.1.2 CERTIFICATE ACCESS FEES

sirar may charge access fees at its discretion for access to any database that stores issued certificates.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEE

sirar does not charge fees for 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 Sirar's Issuing CAs that certify the 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 TSCA:

- 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 its 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 TSCA 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 associated agreements.

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

9.3.1.1 Registration Information

All registration records are considered to be confidential information, including:

- Certificate applications, whether approved or not;
- Certificate information collected as part of the registration process;
- Completed Subscriber Agreements;
- Any corporate or personal information held by sirar/RA 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 fulfill the requirements of this document, and in accordance with sirar's Privacy Policy.

9.3.1.2 Certificate Information

The reasons for a certificate being revoked is considered confidential information, with the sole exception of the revocation of the TSCA due to:

- The compromise of its private key, in which case a disclosure may be made that the private key has been compromised; or
- The termination of the TSCA in which case prior disclosure of the termination may be given.

9.3.1.3 PKI Documentation

sirar's Information Assets Classification & Control Policy specifies which documents are confidential.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

9.3.2.1 Certificate Information

Certificates published in the public repositories are not considered to be confidential information.

9.3.2.2 PKI Documentation

The following documents are public documents and are not considered to be confidential information:

- The CP;
- The CPS;
- Any other policy documents which are classified public.

9.3.2.3 Disclosure of Certificate Revocation Information

Certificate revocation information is provided via the CRL in the repositories.

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 TSCA shall be protected in accordance with sirar's Privacy Policy. sirar 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 Subscribers 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 Subscriber 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 sirar's contractual obligations that are 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

The allocation of Intellectual Property Rights among sirar's participants are governed by the applicable agreements.

sirar retains exclusive rights to any products or information developed under or pursuant to the CPS.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

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

- Providing the operational infrastructure and certification services;
- Making reasonable efforts to ensure that 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
  - In accordance with applicable agreements, Saudi Law and regulations.
- At the time of Certificate issuance; sirar implemented procedures for verifying accuracy of the information contained within it before installation and first use;
- Implemented procedures 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, 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. The 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 requires all RAs under its PKI Hierarchy to warrant that they are in compliance with the CP and may choose to include additional representations within this CPS or RA agreement.

9.6.3 RELYING PARTIES REPRESENTATIONS AND WARRANTIES

Relying Parties who rely upon the certificates issued under the sirar's PKI 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

Subscribers are individuals or organization entities to which certificates are issued.

1. It is the responsibility of the Subscriber to:
   - Always provide accurate and complete information to the CA/RA, both in the certificate request and verification process defined by the TSCA/RA for specific Certificate type to be issued by the TSCA;
   - Review and verify the Certificate contents for accuracy;
   - Secure private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes passwords, hardware token, or other activation data that is used to control access to the Subscriber's private key;
   - Use the Subscriber Certificate only for its intended uses as specified in the CP and this CPS;
   - Notify the TSCA/RA in the event that any information in the Certificate is, or becomes, incorrect or inaccurate;
   - Notify the TSCA/RA in the event of a key compromise immediately whenever the Subscriber has reason to believe that the Subscriber's private key has been lost, accessed by another individual, or compromised in any other manner;
   - Use the Subscriber Certificate in a manner that does not violate applicable laws in the Kingdom of Saudi Arabia; and
   - Upon termination of Subscriber Agreement, revocation or expiration of the Subscriber Certificate, immediately cease use of Private Key corresponding to the Public Key included in the Subscriber Certificate.
2. Subscriber agrees that any use of the Subscriber Certificate to sign or otherwise approve the contents of any electronic record or message is attributable to Subscriber. Subscriber agrees to be legally bound by the contents of any such electronic record or message.

3. Subscriber shall indemnify and hold sirar (the CA) or RA acting on behalf of sirar, harmless from and against any and all damages (including legal fees), losses, lawsuits, claims or actions arising out of:
    - Use of Subscriber's Certificate in an unauthorized manner or otherwise inconsistent with the terms of the Subscriber Agreement or this CPS and the CP;
    - A Subscriber Certificate being tampered with by the Subscriber; or
    - Inaccuracies or misrepresentations contained within the Application. A Subscriber shall indemnify and hold the TSCA/RA harmless against any damages and legal fees that arise out of lawsuits, claims or actions by third parties who rely on or otherwise use Subscriber's Certificate, where such lawsuit, claim, or action relates to a Subscriber's breach of its obligations outlined in this CPS, the CP or the Subscriber Agreement, a Subscriber's use of or reliance upon a Subscriber Certificate in connection with its business operations, a Subscriber's failure to protect its private key, or claims pertaining to content or other information or data supplied, or required to be supplied, by Subscriber.

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 warranties, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of the TSCA or for the legal validity, acceptance or any other type of recognition of its own certificates, those issued by it, 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 that person's 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

No Stipulation.

9.10 TERM AND TERMINATION

9.10.1 TERM

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

9.10.2 TERMINATION

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

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this CPS, all TSCA 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 DGA, the Saudi National Root CA, and Sirar (as the TSCA) 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 CPS's Certificate assurance level.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

This CPS shall be reviewed at least once a year by the PKI Committee. Major amendments shall be discussed with the DGA. The final agreed amendments are approved and applied by the PKI Committee.

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

9.12.2 NOTIFICATION MECHANISM AND PERIOD

This CPS and any subsequent changes shall be made available to the TSCA participants within two weeks of approval. sirar reserves the right to amend this CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. All sirar's PKI participants and other parties designated by sirar shall provide their comments to the PKI Committee in accordance with its rules. The PKI Committee's decision to designate amendments as material or non-material shall be at the PKI Committee's sole discretion.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

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

9.13 DISPUTE RESOLUTION PROCEDURES

The use of certificates issued by the TSCA is governed by contracts, agreements, and standards set forth by sirar. Those contracts, agreements and standards include dispute resolution policy and procedures that shall be employed in any dispute arising from the issuance or use of a certificate governed by this CPS. Dispute Resolution mechanism is described in sirar's Dispute Resolution Policy.

9.14 GOVERNING LAW

This CPS is governed by the laws of the Kingdom of Saudi Arabia.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CPS 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 CPS or any of its rights or duties under this CPS, without the prior written consent of sirar.

9.16.3 SEVERABILITY

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

9.16.4 ENFORCEMENT (ATTORNEY FEES/WAIVER OF RIGHTS)

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

9.16.5 FORCE MAJEURE

sirar shall not be liable for any failure or delay in its performance under this CPS due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil

or military authority, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and reasons beyond provisions of the governing law.

9.17 OTHER PROVISIONS

9.17.1 FIDUCIARY RELATIONSHIPS

Nothing contained in this CPS 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 CPS 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

Administrative processes shall be specified in the corresponding agreements and any sirar Operational policies.

APPENDIX-A: TSU CERTIFICATE POLICY

S. No.	Attribute	Digital Identity Certificate
1	Policy Name	TSU Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.30.5**
3	Application Usage	The TSU Certificates are used for signing time stamps. The trusted time source uses an accurate time source and shall comply with RFC 3161. The Timestamping Authority Services using the TSCA issued TSU Certificate should honour the Key Usage and any Extensions set in the certificate.
4	Verification Process	**For TSU certificates issued to third-party subscribers:** • The following validation data is verified by sirar RA based on the formal documents submitted along with the certificate application form: o Organization Legal Name o Organization Address o Power of Attorney/Authorized Representative o The Organization's Unique National Registration Number (e.g. VAT number, 700 number) o Organization Address • sirar RA reviews all the submitted documents and validate the filled information • sirar RA validates that the Organization is not backlisted according to sirar internal database (any malicious certificate or revocation request or a request that fails multiple (more than ten) times should be added to a blacklist) • sirar RA verifies the Organizations existence as mentioned in section 3.2.2 of this document • sirar RA verifies the organization's address to confirm if it is the same address where the organization conducts its operation • sirar RA verifies the authenticity of the provided authorization letters in order to establish that the authorizing personnel an authorized representative from the entity or an individual previously authorized by an authorized representative to authorize the certificates lifecycle management requests on behalf of the entity. Authorization shall be documented as part of the certificate application form. • sirar RA verifies the identity of the certificate requester according to the submitted identity documents. **For TSU certificates issued to sirar's TSA service:** the certificate request process is handled as per sirar's internal Operations Policies and Procedures.
5	Key Pair Generation and Protection	The keys will be generated and stored within a Hardware Security Module hosted and operated by sirar and fulfilling the requirements set forth in section 6.1.1 of this document .
6	Certificate Issuance Process	A signed PKCS#10 formatted CSR is provided to the TSCA that shall in turn sign the request. The signed certificate shall be returned to complete the process of the TSU configuration by sirar operations team.
7	Certificate Re-key	**For TSU certificates issued to third-party subscribers:** Certificate re-key may happen while the certificate is still active, after it has expired, or after a revocation. The re-key operation shall invalidate any existing active certificates of the same type. Verification of the subscriber's identity shall be performed in the same manner as during the initial registration, in addition to the following: • Requests for certificates to be re-keyed is coming through the same email.

S. No.	Attribute	Digital Identity Certificate
		• Check the existence and validity of the certificate to be rekeyed and that the information used to verify the identity and attributes of the subject are still valid. • If any of the sirar terms and conditions has changed, these shall be communicated to the subscriber and agreed to in accordance with requirements stated in the Saudi National PKI Policy and the present document. **For TSU certificates issued to sirar's TSA service:** the routine re-key of the TTS certificates is done according sirar internal Operations Policies and Procedures.