QUALIFIED CA (QUCA)
CERTIFICATION PRACTICE STATEMENT

Document Classification:

Public

Version Number: 2.0

Issue Date: 15 June 2022

Document Reference

Item	Description
Document Title:	Sirar Qualified (QUCA) Certificate Practice Statement
Custodian Department:	Sirar's Product Management
Owner:	Sirar's Policy Authority
Version Number:	2.0
Document Status:	Final

Document Author:	Sirar's Policy authority	
	PKI Consultant	Signature/Date
		Signed by:Fahad Aljutaily Signed at:2022-06-16 20:40:29 +03:00 Reason:I approve this document
Approved by:	Fahad I. Aljutaily	Fahad Aljutaily
	Sirar CEO	Signature/Date

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	22/11/2019	Katekani Hlabathi	Initial standalone version
1.1	28/11/2019	Katekani Hlabathi	Final version after review
1.2	17/12/2019	Katekani Hlabathi	Final version for NCDC approval and publishing
1.3	23/12/2019	Katekani Hlabathi	Added signatory. For final approval and publishing
1.4	04/01/2020	Katekani Hlabathi	Minor changes post Deloitte pre-audit assessment. For approval and publishing update
1.5	29/04/2020	Katekani Hlabathi	Minor changes related to profile update
1.6	05/05/2020	Mohamed Abdelshahid Katekani Hlabathi	Adding eSeal certificates Apply Updated OID spec
1.7	16/07/2020	STCS Policy Authority	Updates based on regular review
1.8	16/08/2020	STCS Policy Authority	Addressing the comments received during the period of time audit
1.9	18/01/2021	Solutions' Policy Authority	- Remove the low assurance certificates based on NCDC instructions - Specify the date/time of issuing certificates with 64 bits of entropy - Allow Arabic and English names as alternatives in the subject DN of some end-entity certificates
1.8	30/09/2021	Solutions' Policy Authority	Annual review
2.0	15/06/2022	Sirar's Policy Authority	Document issuance under Sirar's name

Document Control

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

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

Table of Contents

1 Introduction 10

1.1 Overview 11
1.1.1 Certificate Policy 11
1.1.2 Relationship between the CP and the CPS 12
1.1.3 Interaction with other PKIs 12
1.1.4 Scope 12

1.2 Document Name and Identification 12

1.3 PKI Participants 12
1.3.1 Certification Authorities 12
1.3.2 Registration 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 16
1.5.3 Person Determining CPS Suitability for the Policy 16
1.5.4 CPS Approval Procedures 16

1.6 Definitions and Acronyms 16

2 Publication and Repository Responsibilities 17

2.1 Repositories 17

2.2 Publication of Certification Information 17
2.2.1 Publication of Certificates and Certificate Status 17
2.2.2 Publication of CA Information 17
2.2.3 Interoperability 17

2.3 Time or Frequency of Publication 17

2.4 Access Controls on Repositories 18

3 Identification and Authentication 19

3.1 Naming 19
3.1.1 Types of Names 19
3.1.2 Need for Names to be Meaningful 19
3.1.3 Anonymity or Pseudonymity of Subscribers 19
3.1.4 Rules for Interpreting Various Name Forms 19
3.1.5 Uniqueness of Names 19
3.1.6 Recognition, Authentication and Role of Trademarks 20

3.2 Initial Identity Validation 20
3.2.1 Method to Prove Possession of Private Key 20
3.2.2 Authentication of Organization Identity 20
3.2.3 Identity-Proofing of Individual Identity 21
3.2.4 Non-verified Subscriber Information 22
3.2.5 Validation of Authority 22
3.2.6 Criteria of Interoperation 22

3.3 Identification and Authentication for Re-key Requests 22
3.3.1 Identification and Authentication for Routine Re-Key 22
3.3.2 Identification and Authentication for Re-key After Revocation 23

3.4 Identification and Authentication for Revocation Requests 23

4 Certificate Life-Cycle Operational Requirements 24

4.1 Certificate Application 24
4.1.1 Who Can Submit a Certificate Application 24
4.1.2 Enrollment Process and Responsibilities 24

4.2 Certificate Application Processing 25
4.2.1 Performing Identification and Authentication Functions 25
4.2.2 Approval or Rejection of Certificate Applications 25
4.2.3 Time to Process Certificate Applications 26

4.3 Certificate Issuance 26
4.3.1 CA Actions During Certificate Issuance 26
4.3.2 Notification to subscriber by the CA of issuance of certificate 26

4.4 Certificate Acceptance 27
4.4.1 Conduct Constituting Certificate Acceptance 27
4.4.2 Publication of the Certificate by the CA 27
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 27

4.5 Key Pair and Certificate Usage 27
4.5.1 Subscriber Private Key and Certificate Usage 27
4.5.2 Relying Party Public Key and Certificate Usage 27

4.6 Certificate Renewal 28
4.6.1 Circumstances for Certificate Renewal 28
4.6.2 Who may request Certificate Renewal 28
4.6.3 Processing Certificate Renewal Requests 28
4.6.4 Notification of Renewed Certificate Issuance 28
4.6.5 Conduct constituting acceptance of a renewal certificate 28
4.6.6 Publication of a Renewal Certificate 29
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 29

4.7 Certificate Re-Key 29
4.7.1 Circumstances for Certificate Re-key 29
4.7.2 Who can Request a Certificate Re-key 29
4.7.3 Processing Certificate Re-keying Requests 29
4.7.4 Notification of New Certificate Issuance to Subscriber 29
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 30
4.7.6 Publication of the Re-keyed Certificate by the CA 30
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 30

4.8 Certificate Modification 30

4.9 Certificate Revocation and Suspension 30
4.9.1 Circumstance for Revocation of a Certificate 30
4.9.2 Who Can Request Revocation of a Certificate 31
4.9.3 Procedure for Revocation Request 31
4.9.4 Revocation Request Grace Period 32
4.9.5 Time within which CA must Process the Revocation Request 32
4.9.6 Revocation Checking Requirements for Relying Parties 32
4.9.7 CRL Issuance Frequency 32
4.9.8 Maximum Latency of CRLs 32
4.9.9 Online Revocation Checking Availability 33
4.9.10 Online Revocation Checking Requirements 33

4.9.11 Other Forms of Revocation Advertisements Available 33
4.9.12 Special Requirements Related To Key Compromise 33
4.9.13 Circumstances for Certificate Suspension 33
4.9.14 Who Can Request Suspension 33
4.9.15 Procedure for Suspension Request 33
4.9.16 Limits on Suspension Period 33

4.10 Certificate Status Services 33
4.10.1 Operational Characteristics 34
4.10.2 Service Availability 34

4.11 End of Subscription 34

4.12 Key Escrow and Recovery 34

5 Facility Management and Operational Controls 35

5.1 Physical Security Controls 35
5.1.1 Site Location and Construction 35
5.1.2 Physical Access 35
5.1.3 Power and Air Conditioning 35
5.1.4 Water Exposure 36
5.1.5 Fire Prevention and Protection 36
5.1.6 Media Storage 36
5.1.7 Waste Disposal 36
5.1.8 Off-Site Backup 36

5.2 Procedural Controls 36
5.2.1 Trusted Roles 36
5.2.2 Number of Persons Required per Task 37
5.2.3 Identification and Authentication for Each Role 37
5.2.4 Separation of Roles 37

5.3 Personnel Controls 37
5.3.1 Background, Qualifications and Experience Requirements 37
5.3.2 Background Check and Clearance Procedures 37
5.3.3 Training Requirements 38
5.3.4 Retraining Frequency and Requirements 38
5.3.5 Job Rotation Frequency and Sequence 38
5.3.6 Sanctions for Unauthorized Actions 38
5.3.7 Contracting Personnel Requirements 38
5.3.8 Documentation Supplied to Personnel 38

5.4 Audit Logging Procedures 39
5.4.1 Types of Events Recorded 39
5.4.2 Frequency for Processing and Archiving Audit Logs 40
5.4.3 Retention Period for Audit Log 40
5.4.4 Protection of Audit Log 40
5.4.5 Audit Log Backup Procedures 41
5.4.6 Audit Collection System (Internal or External) 41
5.4.7 Notification to Event-Causing Subject 41
5.4.8 Vulnerability Assessments 41

5.5 Records Archival 41
5.5.1 Types of Events Archived 41
5.5.2 Retention Period for Archive 41
5.5.3 Protection of Archive 42
5.5.4 Archive Backup Procedures 42
5.5.5 Requirements for Time-Stamping of Records 42
5.5.6 Archive Collection System (Internal or External) 42

5.5.7 Procedures to Obtain and Verify Archive Information 42
5.6 Key Changeover 42
5.7 Compromise and Disaster Recovery 43
5.7.1 Incident and Compromise Handling Procedures 43
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 43
5.7.3 CA Private Key Compromise Recovery Procedures 43
5.7.4 Business Continuity Capabilities after a Disaster 43
5.8 CA OR RA Termination 44
5.8.1 CA Termination 44
5.8.2 RA Termination 45
6 Technical Security Controls 46
6.1 Key Pair Generation and Installation 46
6.1.1 Key Pair Generation 46
6.1.2 Private Key Delivery to Subscribers 46
6.1.3 Public Key Delivery to Certificate Issuer 47
6.1.4 CA Public Key Delivery to Relying Parties 47
6.1.5 Key Sizes 47
6.1.6 Public Key Parameters Generation and Quality Checking 47
6.1.7 Key Usage Purposes 47
6.2 Private Key Protection and Crypto-Module Engineering Controls 48
6.2.1 Cryptographic Module Standards and Controls 48
6.2.2 Subscriber Private Key Multi-Person Control 48
6.2.3 Private Key Escrow 48
6.2.4 Private Key Backup 48
6.2.5 Private Key Archival 48
6.2.6 Private Key Transfer Into or From a Cryptographic Module 48
6.2.7 Private Key Storage on Cryptographic Module 48
6.2.8 Method of Activating Private Keys 48
6.2.9 Methods of Deactivating Private Keys 48
6.2.10 Methods of Destroying Private Keys 49
6.2.11 Cryptographic Module Rating 49
6.3 Other Aspects of Key Pair Management 49
6.3.1 Public Key Archive 49
6.3.2 Certificate Operational Periods and Key Usage Periods 49
6.4 Activation Data 49
6.4.1 Activation Data Generation and Installation 49
6.4.2 Activation Data Protection 50
6.4.3 Other Aspects of Activation Data 50
6.5 Computer Security Controls 50
6.5.1 Specific Computer Security Technical Requirements 50
6.5.2 Computer Security Rating 50
6.6 Life-Cycle Security Controls 50
6.6.1 System Development Controls 50
6.6.2 Security Management Controls 51
6.6.3 Life Cycle Security Ratings 51
6.7 Network Security Controls 51
6.8 Time Stamping 51
7 Certificate, CRL and OCSP Profiles 52

7.1 Certificate Profile 52
7.1.1 Version Numbers 63
7.1.2 Certificate Extensions 63
7.1.3 Algorithm Object Identifiers 63
7.1.4 Name Forms 63
7.1.5 Name Constraints 63
7.1.6 Certificate Policy Object Identifier 63
7.1.7 Usage of Policy Constraints Extension 63
7.1.8 Policy Qualifiers Syntax and Semantics 63
7.1.9 Processing Semantics for the Critical Certificate Policy Extension 63

7.2 CRL Profile 63
7.2.1 QUCA CRL Profile 64
7.2.2 Version Numbers 64
7.2.3 CRL and CRL Entry Extensions 64

7.3 OCSP Profile 64
7.3.1 Version Number 65
7.3.2 OCSP Extensions 65

8 Compliance Audit and Other Assessments 66

8.1 Frequency of Audit or Assessments 66

8.2 Identity and Qualifications of Assessor 66

8.3 Assessor's Relationship to Assessed Entity 66

8.4 Topics Covered By Assessment 66

8.5 Actions Taken As A Result of Deficiency 67

8.6 Communication of Results 67

9 Other Business and Legal Matters 68

9.1 Fees 68
9.1.1 Certificate Issuance/Renewal Fee 68
9.1.2 Certificate Access Fees 68
9.1.3 Revocation or Status Information Access Fee 68
9.1.4 Fees for Other Services 68
9.1.5 Refund Policy 68

9.2 Financial Responsibility 68
9.2.1 Insurance Coverage 68
9.2.2 Other Assets 68
9.2.3 Insurance/warranty Coverage for End-Entities 68

9.3 Confidentiality of Business Information 69
9.3.1 Scope of Confidential Information 69
9.3.2 Information not within the Scope of Confidential Information 69
9.3.3 Responsibility to Protect Confidential Information 70

9.4 Privacy of Personal Information 70
9.4.1 Privacy Plan 70
9.4.2 Information Treated as Private 70
9.4.3 Information not Deemed Private 70
9.4.4 Responsibility to Protect Private Information 70
9.4.5 Notice and Consent to Use Private Information 70
9.4.6 Disclosure Pursuant to Judicial/Administrative Process 70
9.4.7 Other Information Disclosure Circumstances 70

9.5 Intellectual Property Rights 71

9.6 Representations and Warranties 71
9.6.1 CA Representations and Warranties 71
9.6.2 RA Representations and Warranties 72
9.6.3 Relying Parties Representations and Warranties 72
9.6.4 Subscriber Representations and Warranties 72
9.7 Disclaimers of Warranties 73
9.8 Limitations of Liability 73
9.9 Indemnities 73
9.10 Term and Termination 74
9.10.1 Term 74
9.10.2 Termination 74
9.10.3 Effect of Termination and Survival 74
9.11 Individual Notices and Communications with Participants 74
9.12 Amendments 74
9.12.1 Procedure for Amendment 74
9.12.2 Notification Mechanism and Period 74
9.12.3 Circumstances under which OID must be changed 75
9.13 Dispute Resolution Procedures 75
9.14 Governing Law 75
9.15 Compliance with Applicable Law 75
9.16 Miscellaneous Provisions 75
9.16.1 Entire Agreement 75
9.16.2 Assignment 75
9.16.3 Severability 75
9.16.4 Enforcement (Attorney Fees/Waiver of Rights) 75
9.16.5 Force Majeure 75
9.17 Other Provisions 76
9.17.1 Fiduciary Relationships 76
9.17.2 Administrative Processes 76
Appendix-A: Certificate Types & Policies 77
A.1 Certificate types supported 77
A.1.1 Digital Signing Certificate Service (IDS) 77
A.1.2 e-Seal Certificates 80
A.1.3 RA Identity Certificate (RA Certificate) 82
A.1.3 Online Certificate Status Protocol Certificate (OCSP Certificate) 83
A.1.4 Local Signing Services (LSS) 84
A.1.4.1 Local Signing Certificate issuance requirements And Usage 84
A.1.5 Trusted Timestamping Services (TTS) 86

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 created a National Public Key Infrastructure. Named the National Center for Digital Certification (NCDC), NCDC is created by an act of law and its mandate is stipulated in the Saudi e-Transactions Act and its bylaws.

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

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 that is operated by the NCDC. Underneath the Intermediary CA, there are subordinate Issuing Certificate Authorities (hereinafter, Issuing CAs) that issue certificates to end-users. The two Issuing CAs signed by the Intermediary CA are:

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

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

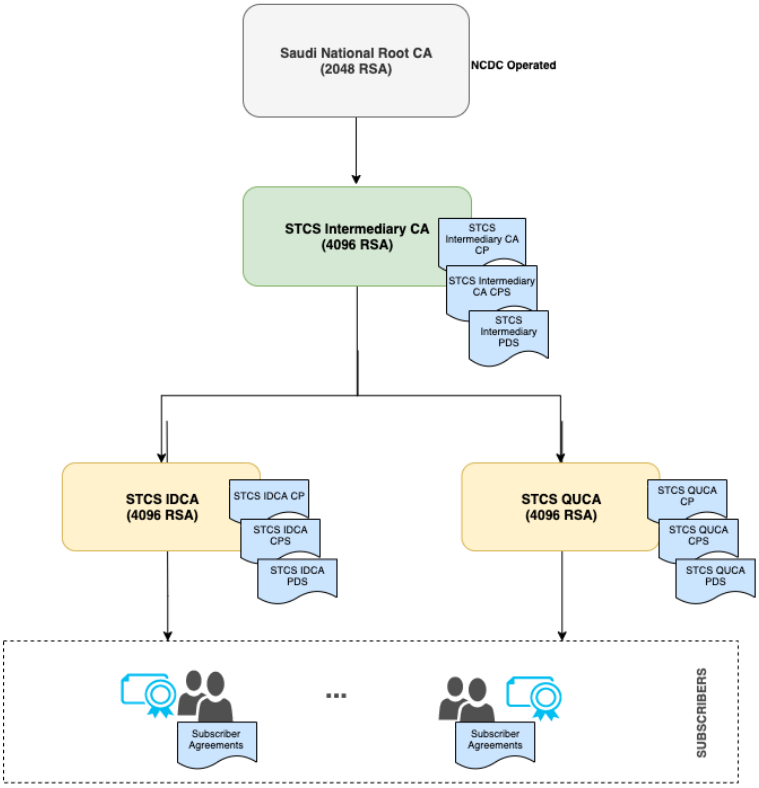

Figure 1-Sirar's PKI and Governance Hierarchy

This Certification Practice Statement (CPS) establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by

the QUCA. In particular, this CPS establishes the processes and procedures the QUCA follows to:

- Issue Subscribers' certificates in compliance with the QUCA CP and this CPS,
- Manage certificate life cycle for the end entity certificates issued under this QUCA hierarchy; and
- Operate a directory of issued sub-CA certificates; and
- Operate the CRL directory.

This CPS complies with the following requirements:

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

1.1 OVERVIEW

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

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

- Securely managing the core infrastructure hosting the QUCA, and
- Issuing, managing, revoking, and renewing subscriber certificates
- The technical, procedural and personnel management in accordance with the requirements of the CP.

Any use of or reference to this CPS outside the context of the QUCA and Saudi National PKI is completely at the using party's risk. The terms and provisions of CPS shall be interpreted under and governed by the CP and Sirar's Operations Policies and Procedures.

It is the responsibility of all parties applying for or using a Digital Certificate issued under the CPS, to read the CP to understand the practices established for the lifecycle management of the Certificates issued by the QUCA.

1.1.1 CERTIFICATE POLICY

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

1.1.2 RELATIONSHIP BETWEEN THE CP AND THE CPS

This CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by QUCA as governed by the CP and related documents which describe QUCA requirements and use of Certificates.

1.1.3 INTERACTION WITH OTHER PKIS

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

1.1.4 SCOPE

This CPS applies to all certificates issued by the QUCA. The QUCA operates 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 QUCA Certification Practice Statement (CPS), and is identified by the following object identifier (OID):

OID: 2.16.682.1.101.5000.1.4.1.2.1.12

1.3 PKI PARTICIPANTS

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

Several parties constitute the participants of the QUCA. 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 two Issuing CA's under it, these being the STCS Identity CA (IDCA) and the QUCA. These Issuing CAs issue subscriber certificates, OCSP responder certificates and other certificates required by the internal PKI components. The Issuing CAs issue certificates to Subscribers in accordance with each respective CP and the CPS, their RA Agreement, Subscriber Agreement, Relying Party Agreement, and the Saudi National PKI Policy.

Sirar as an entity is responsible for:

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

- Performance of all aspects of the services, operations and infrastructure related to the Sirar's PKI.

1.3.1.1 Saudi National Root CA

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

1.3.1.2 STCS Intermediary CA

The 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 in Sirar's PKI hierarchy, including the QUCA.

1.3.1.3 STCS Qualified CA (QUCA)

The QUCA 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 signing certificates to be used in Digital Signing of documents, data and transactions. The subscribers can be individuals or organizational entities.

1.3.2 REGISTRATION AUTHORITY (RA)

Sirar runs its own RA function through Sirar, in addition, it also appoints third-party Registration Authorities (RAs) to perform the Subscriber Identification and Authentication and Certificate request and revocation functions defined in the CP, this CPS as well as the related documents.

The third-party egistration Authority (RA) is obligated to perform certain functions pursuant to an RA Agreement including the following:

- Process Certificate application requests in accordance with this CPS, the CP and applicable RA Agreement, and other policies and procedures regarding the Certificates issued;
- Maintain and process all supporting documentation related to the Certificate application process;
- Process Certificate Revocation requests in accordance with this CPS, the CP, applicable RA Agreement, and other relevant operational policies and procedures with respect to the Certificates issued. Without limitation to the generality of the foregoing, an RA shall request the revocation of any Certificate that it has approved for issuance according to the stipulations in this CPS;
- Comply with the provisions of its RA Agreement and the provisions of this CPS and the CPS including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements; and
- Follow Sirar's Privacy Policy in accordance with this CPS, the CP and applicable RA Agreement.

1.3.3 SUBSCRIBERS

Subscribers are individuals (end users) or entities (organizations) to whom certificates are issued. Subscribers are bound by the conditions of use of certificates as contained in the

Subscriber Agreement. In general, the subscriber asserts that he or she uses the key and certificate in accordance with the CP and this CPS.

1.3.4 RELYING PARTIES

A Relying Party in this context is the entity that relies on the validity of the binding of the QUCA of an identity to a public key. The Relying Party is responsible for checking the validity of the certificate by examining the appropriate certificate status information, using validation services provided by the QUCA. 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 are 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 QUCA issues certificates for Natural Persons (Individuals) used for Digital Signing purposes.

STCS Qualified CA (QUCA) issues certificates for Legal Persons (Organizations) used to add an eSeal on a document issued\attested by an organization.

The QUCA issues certificates under this CPS only to those Subscribers who have signed their acceptance of a Subscriber Agreement in the appropriate form and whose application for certificates has been approved by the CA.

The following level of assurance are offered to subscribers in the form of end entity certificates issued by the QUCA. The Level of Assurance is in line with levels described in the Saudi National PKI Policy.

Assurance Level	Description
Low Assurance Certificates *Apply to certificates issued to natural persons (Individuals)*	These certificates provide a low level of assurance to publicly available products and services. These certificates provide little confidence in the accuracy or legitimacy of the claimed identity. It requires a no or low level of binding between the claimed identity of the subject named in the certificate and the subscriber. It is intended mainly for email protection.
Medium Assurance Certificates *Apply to certificates issued to:* • *Natural persons (Individuals),* • *Legal persons (Organizations)*	The certificates issued at this level provide medium confidence in the accuracy or legitimacy of the claimed identity. It is intended to be used for documents/transactions with serious or substantial consequences to Relying Parties. Identity at this level is verified with authoritative sources.
High Assurance Certificates *Apply to certificates issued to:* • *Natural persons (Individuals),* • *Legal persons (Organizations)*	The certificates issued at this level provide high confidence in the accuracy or legitimacy of the claimed identity. It is intended to be used for documents/transactions with high value or high risk, that can have catastrophic consequences to Relying Parties. Identities at this level is verified with authoritative sources based on face-to-face or equivalent method.

For more information about the types and usage of the certificates issued by the QUCA, refer to Appendix-A of this document.

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 terms used in this document shall have the meanings as defined in the prevailing CABForum Baseline Requirements (www.cabforum.org)

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

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

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

Sirar's PKI repositories that allow the PKI participants to make on-line enquiries regarding revocation and other certificate status information. QUCA 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 QUCA certificate; and
- CRLs: CRLs that are made publicly available to allow PKI participants to verify the status of certificates.

The QUCA 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 QUCA PKI Participants at Sirar's Certificate Dissemination Webpage: https://sirar.com.sa/repository/. This Webpage is the only source for up-to-date documentation and QUCA reserves the right to publish newer versions of the documentation without prior notice. Additionally, the QUCA 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 QUCA are approved by Sirar's Policy authority, refer to section 7.1 where the naming conversions for different certificate types are specified.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

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

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

CN=STCS QUCA, O=STCS, C=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 QUCA are covered in Appendix-A of this document.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The QUCA is not issuing anonymous or pseudonymous certificates.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

QUCA shall only use Uniform Resource Indicators (URIs) in accordance with the applicable Internet Engineering Task Force (IETF) standards. Subject Alternative Name forms are interpreted in accordance with applicable ISO and IETF Standards. The following table provides the rules for interpreting the various name forms.

Name Form	Standard
DN	X.500
URL	RFC-1738
Internet e-mail address	RFC-822
DNS	RFC-1034

3.1.5 UNIQUENESS OF NAMES

All distinguished names are unique across the QUCA. 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 QUCA is configured in such a manner as to enforce name uniqueness for certificates that it issues. The QUCA is responsible for ensuring name uniqueness in subscriber certificates issued by it. Additional naming attributes for uniquely identifying the subject include serial number, email, etc.

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 QUCA and its RAs, however, does not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application.

The QUCA may revoke a Certificate upon receipt of a properly authenticated order from NCDC, 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

Local Signing keys are generated on secure cryptographic tokens for subscribers. The generation of the keys is witnessed by the subscribers. The Private key corresponding to the certificate is held securely within the token and never leaves the protection mechanisms provided by the secure token. A self-signed PKCS#10 certificate signing request (CSR) is generated by the token for the QUCA.

Remote Singing keys are generated securely using Sirar's Remote Signing Platform. The Private key corresponding to the certificate is held securely within the Remote Signing Platform and never leaves it. A self-signed PKCS#10 certificate signing request (CSR) is generated by the token for the QUCA.

Software keys are generated using trustworthy computing equipment. If generated by the subscriber, the subscriber shall generate the keys in trustworthy systems and provide a self-signed certificate signing request in PKCS#10 format.

The QUCA inspects the contents of the CSR during the signing process and confirm that the details match those in the certificate application documentation. At minimum the following details shall be inspected to confirm the correctness thereof:

- Subject Distinguished Name (DN)
- Acceptable Key lengths and Algorithms
- The CSR is signed using the private key corresponding to the public key included in the CSR

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

If the subject of the certificate is to include the organization's name, the QUCA or an RA, as the case may be, 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 QUCA/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 RA certificates, The CA shall verify the below details using documentation provided by the applicant:

- RA Details (Full Name, ID details, email address, phone)
- Requester Organization Information and address
- Subject of RA (DN) (optional)
- Sirar's Approval together with a signed RA Agreement

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 QUCA.

3.2.3 IDENTITY-PROOFING OF INDIVIDUAL IDENTITY

The type of identification and authentication process to be followed depends on the type of certificate for an individual is applying for. QUCA issues three types of certificates:

- Low Level of Assurance Certificates – where verification is limited to email ownership verification

- Medium Level of Assurance Certificates – in addition to the requirements apply for Low Level, the individual's identity is verified based on one of the following methods:

    - using authentication credentials from an existing Identity Provider or a trusted KYC database such as a Bank's KYC

    - identity verification via recorded videos or video calls where person's face is visually matched by an officer against a photo on a government issued photo ID

    The above methods would be accepted provided that the following requirements are met:

    - Existence of ID proofing artifacts substantiate the antecedent verification outcome
    - Mechanisms are in place that bind the individual to the asserted identity

- High Level of Assurance Certificates – in addition to the requirements apply for Medium Level, there are the following additional requirements:

    - In-person verification where person's face is visually matched by an officer against a photo on a government issued photo ID, or;
    - Strong 2-factor authentication offered by IAM/NAFATH/ELM, or;
    - Biometric varication, such as face verification or fingerprint verification.

Detailed requirements for the different certificate types are provided in Appendix-A in this document.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Non-verified information is NOT to be included in certificates issued under QUCA, unless specifically mentioned in the Certificate Types section in Appendix-A of the CPS.

3.2.5 VALIDATION OF AUTHORITY

For Email protection certificates issued to Natural Persons: the QUCA or an RA, as the case may be, shall verify that the Applicant has control over the email address to be included in the Certificate through a challenge response mechanism.

For Digital Singing certificates issued to Natural Persons (Individuals) where no organization is to be mentioned in the certificate subject: the QUCA or an RA, as the case may be, shall verify do the verification through a reliable means of communication with the individual Applicant.

For Digital Singing certificates issued to Natural Persons (Individuals) where an organization is to be mentioned in the certificate subject: the QUCA or an RA, as the case may be, shall verify an authorization letter to be submitted by the applicant demonstrating no objection from the organization on the certificate application.

For certificates issued to Legal Persons (eSeal certificates): QUCA, before certificate issuance, ensures that the applicant has specific rights, entitlements, or permissions to obtain a certificate on behalf of the organization that is the subject of the certificate. The following information is submitted by the applicant and verified by QUCA:

- 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 dully 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.

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 are required to obtain new key pairs at least once every three years. (The usage periods for CA and Subscriber private keys are described in section 6.3.2.) During the Re-keying process the QUCA will create a new certificate with the same characteristics as the old certificate but with a new and different key pair and serial number. This new certificate may be given a new validity period or use the validity period that appeared in the old certificate.

When it has been less than three (3) years since the time the Subscriber was identified by the RA, the QUCA will authenticate an electronic request for a new certificate using the currently valid certificate issued to the Subscriber by the QUCA. If using the currently valid certificate is

not applicable, then the identification and authentication steps for Re-Key would be the same as applied during initial certification.

Where it has been longer than three (3) years from the time that the Subscriber's identity has been authenticated, or if the user of existing certificate is not applicable, then the Subscriber certificate re-key will follow the same procedures as the initial certificate issuance process.

The routine re-key of Timestamping and the OCSP certificates is done according Sirar's internal Operations Policies and Procedures.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

If a Subscriber Certificate is revoked, the Subscriber goes through the same initial identity-proofing process as per respective certificate type to obtain a new certificate.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

Prior to the revocation of a Subscriber certificate, the QUCA 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 from fulfilling the following conditions:
    - The signature of a revocation request form by the subscriber of an authorized representative;
    - The verification of the identity of the requesters against the information available to the QUCA/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 and timestamping certificates: 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 QUCA/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 QUCA a confirmation that the Applicant has met the authentication requirements and the information which is to appear in the Certificate.

The QUCA 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 QUCA and the RA are 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 QUCA.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

Subscriber certificate applicants, including those applying for a device or entity certificate, will follow the application process specified in Appendix-A of this document, including complying with identity proofing requirements in section 3.2.3.

4.1.2.1 Subscriber Certificates

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 identity proof and fulfilling the requirements of the applicable certificate type 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 RA Certificates

An entity wishing to become RA under the QUCA shall agree to the terms of the RA Agreement as part of the application process. The RA applicants shall provide their credentials to demonstrate their identity and contact information during the application process. The private key for RA certificates shall be generated by the CA in accordance with the Operations Procedures.

All applicants shall agree to the terms and conditions of the applicable Agreement, such as: Subscriber Agreement, Relying Party or Registration Authority Agreement. Identification and Authentication process is described in the CPS under section 3.

4.1.2.3 OCSP and Timestamping certificates

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

The QUCA/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 QUCA/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 QUCA/RA believes that issuing a certificate to the Subscriber may bring the QUCA into disrepute.

Policies specific to each certificate type have been detailed in the Certificate Types section in Appendix-A of this CPS.

For OCSP and Timestamping certificates, 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 QUCA 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 QUCA/RA receives a request for certificate from a Subscriber, the QUCA/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, and
- Verify that the subscriber possesses the private key corresponding to the certificate signing requests, for subscriber generated keys
- Submit the certificate request to the QUCA.

Upon receiving a validated certificate request from RA, the QUCA 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 are verified before inclusion in the certificate, unless such verification is not required for specific attributes, identifiers, and/or Certificate Types in Appendix-A of this CPS. The QUCA, through its RA, is responsible for verifying the data to be included in the Certificate. At a minimum the QUCA/RA will follow the steps described in section 3.2 of the CP and this CPS.

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

Following successfully completion of the registration process, the QUCA 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 QUCA

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

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

The QUCA 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 CA does not publish end-user certificates apart from sharing it with the requester.

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.

For local signing keys that are generated on secure cryptographic tokens, 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 QUCA 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 QUCA issued certificates to Subscribers.

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

Certificate renewal is supported for the QUCA issued certificates subject to the following conditions:

- The certificate to be renewed must not have been revoked;
- All details of the certificate remain accurate and no new validation of identity is required

4.6.2 WHO MAY REQUEST CERTIFICATE RENEWAL

The QUCA may accept a request for renewal of certificates from the original holder of the certificate. Such requests shall be validated using mechanisms such as challenge response. The request for renewal may originate from the following:

- An RA for its own RA certificate
- An RA on behalf of a subscriber
- A subscriber for his own individual certificate
- An authorized representative for an Organizational certificate.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

The QUCA processes the certificate renewal after confirming the authenticity of such a request. The validation may reuse the original documentation used during first issuance. QUCA may request additional information before the certificate renewal request may be performed. Such request will be processed as soon as is commercially reasonable to do so.

Should the validation fail, the certificate shall not be renewed. The subscriber has the option to apply for a new certificate, and such application shall follow the applicable procedures for a new certificate application.

4.6.4 NOTIFICATION OF RENEWED CERTIFICATE ISSUANCE

The QUCA notifies the subscriber of the renewed certificate using the same method as that of original issuance.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Acceptance procedures for renewed certificate shall follow the same conditions as the original certificate acceptance.

4.6.6 PUBLICATION OF A RENEWAL CERTIFICATE

Refer to section 4.4.2.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Generally, QUCA does not notify other entities of a renewed certificate apart from the requesting party.

4.7 CERTIFICATE RE-KEY

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

The new Certificate may have the same expiry date as the old certificate and may be signed using a different Issuing CA private key.

4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

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.

4.7.2 WHO CAN REQUEST A CERTIFICATE RE-KEY

Certificate re-key may be requested by:

- The PKI Committee for any corrective action (Subscriber to be notified)
- An RA for its own RA certificate
- An RA on behalf of a subscriber, if requested by the subscriber
- A subscriber for his own individual certificate
- An authorized representative for an Organizational certificate.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

The QUCA follows procedures to ensure that the person or organization seeking to update an end-user Subscriber Certificate is in fact the Subscriber, a sponsor of a device or a representative of an entity. Acceptable procedures are through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key.

Other than the above mentioned procedures, the QUCA/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 QUCA does not notify other entities of a re-keyed certificate apart from the requesting party.

4.8 Certificate Modification

The QUCA 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
- 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 QUCA/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 QUCA to the subscriber's registered email address); or
- Telephonic notification to subscriber.

The QUCA 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 QUCA 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;
- QUCA suspects or determines that revocation of a Certificate is in the best interest of the integrity of the CA;

- The QUCA determines that a 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 of the certificate 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.
- Subscriber or another authorized agent asks for his/her certificate to be revoked;
- If the Subscriber is no longer part of the organization, i.e. affiliation to the organization is no longer valid; and
- The Subscriber agreement, or Registration Authority's Agreement in the case of an RA, 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:

- NCDC can request the revocation of any certificates issued by any CA participating in the Saudi National PKI;
- The PKI Committee can request the revocation of any certificates issued under its authority;
- An RA can request the revocation of any of their Subscribers Certificate;
- The RA for their own certificate, if any suspected misuse has been attributed to their given Certificates;
- Subscribers, 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 NCDC.

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 QUCA 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.

4.9.3.2 Procedure for Requesting the Revocation of an RA Certificate

An RA requesting revocation of its RA certificate is required to communicate the request to the PKI Committee. The Committee – after following provisions in the relevant RA Agreement, Operations Policies or Procedures – approve the revocation. The Committee may also initiate the revocation of an RA certificate if it is deemed to be necessary or in the best interest of the QUCA.

Upon approval, the RA 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

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

- 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 QUCA 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 QUCA provides an Online revocation and status checking to its relying parties. The QUCA 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 QUCA.

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 QUCA 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, with appropriate physical and procedural access controls for all hardware and software sub-systems used in the issuance and revocation of certificates. Sirar limits 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 QUCA and Sirar's Data Center equipment is consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, provides robust protection against unauthorized access to the QUCA equipment and records.

5.1.2 PHYSICAL ACCESS

QUCA 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 QUCA 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 un-trusted employees or visitors, should not be allowed into such secured areas. Sirar employ Security Personnel that continually monitor the facility hosting CA equipment on a 24x7 basis. Sirar shall provide normal and emergency lighting to the CA facilities.

Sirar 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 QUCA equipment have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Any of the QUCA 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's ensures that the QUCA 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 QUCA equipment is housed in a facility with appropriate fire suppression and protection systems.

5.1.6 MEDIA STORAGE

Sirar's ensures that QUCA 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 extraordinarily responsible or the integrity of the PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the QUCA. 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 individual 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 QUCA certificate signing Private Key. Activation of the QUCA 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 QUCA will ensure that no individual is assigned more than one Trusted Role.

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 QUCA 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 check shall take into account the following:

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

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

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:

- QUCA 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 QUCA 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 QUCA 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 QUCA shall determine whether to suspend or continue with operations.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

Event-causing subject are not notified.

5.4.8 VULNERABILITY ASSESSMENTS

Routine vulnerability assessments of security controls shall be performed by Sirar for its Issuing CAs and other PKI supporting systems hosted in Sirar's data centre. Such assessments shall be held 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 QUCA 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 QUCA 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. QUCA's minimum retention period for archive data is established at ten (10) years.

The QUCA shall retain all documentation relating to the QUCA 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 NCDC, the PKI Committee, or as required by law. Records and material information relevant to use of, and reliance on, a certificate shall be archived. Archive media shall be stored in a secure storage facility separate from the 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 QUCA 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 QUCA may periodically perform key rollover, allowing CA keys to be changed periodically as required to minimize risk to the integrity of the QUCA. 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 QUCA 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 QUCA 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 QUCA maintains backup copies of hardware, system, databases, and private keys in order to rebuild the QUCA 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 QUCA 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 QUCA, the impact of the termination must be minimized as much as possible in light of the prevailing circumstances and is subject to the applicable QUCA Agreements. Procedures to be followed for the termination of the QUCA 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 NCDC
- Ensure certificate status information services are provided and maintained for the duration of the termination
- Ensure process for revoking certificates are maintained

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

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

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 QUCA is witnessed and attested to by a party separate from the QUCA operator or the CA administrator as mentioned in the Key Generation Script for each CA.

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.

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

For Subscriber and RA Private 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 2 or higher. Keypairs generated in Software shall be generated using trustworthy computer systems.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBERS

For local signing certificates, Sirar delivers subscriber private keys in a secure format, such as in cryptographic tokens or smartcards when those keys are generated in cryptographic hardware.

Subscriber and RA keys generated in Software is delivered securely using secure standards such as PKCS#12 file format, where the following requirements are met:

- Anyone who generates a private signing key for a Subscriber does not retain any copy of the key after delivery of the private key to the Subscriber (in case of local signing where the subscriber keys are stored on smartcards or tokens);
- The private key is protected from activation, compromise, or modification during the delivery process;
- The Subscriber acknowledges receipt of the private key (in case of local signing where the subscriber keys are stored on smartcards or tokens);
- Delivery is accomplished in a way that ensures that the correct smartcard or token and activation data are provided to the correct Subscriber.
    - For cryptographic modules, accountability by the RA for the location and state of the module is maintained until the Subscriber accepts possession of it.

- For electronic delivery of private keys, the key material is encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data is delivered using a separate secure channel.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Public keys can be delivered to the QUCA 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 QUCA 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 as below for all subscriber certificates issued by the QUCA. All FIPS-approved signature algorithms shall be considered acceptable. If NCDC determines that the security of a particular algorithm may be compromised, it shall direct Sirar to revoke the affected certificates.

All certificates issued to subscribers shall use at least 2048-bit RSA, with Secure Hash Algorithm version 2 (SHA-256) in accordance with FIPS 186-2 or equivalent.

The key lengths of certificates issued by the QUCA are as follows:

- Subscriber Key Pairs: 2048 bits RSA
- RA Key Pairs: 2048 bits RSA
- OCSP Key Pair: 2048 bits RSA
- Timestamping Key Pair: 2048 bits RSA

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The QUCA generates key pairs that comply with FIPS 186-4. The QUCA 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 depending on their intended business usage 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

Cryptographic modules, smartcards or tokens employed for subscriber, OCSP Responder and RA private key protection issued by the QUCA shall comply with FIPS-PUB 140-2 “Security Requirements for Cryptographic Modules”, Level 3 and above.

6.2.2 SUBSCRIBER PRIVATE KEY MULTI-PERSON CONTROL

No stipulation. RAs, OCSP Responder and subscribers’ private keys are not under multi-person control.

6.2.3 PRIVATE KEY ESCROW

The QUCA does not escrow Subscriber Private keys as it does not issue encryption certificates.

6.2.4 PRIVATE KEY BACKUP

The QUCA does not backup Subscriber private keys.

6.2.5 PRIVATE KEY ARCHIVAL

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

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The subscriber keys are allowed to be stored in at least FIPS 140-2 level 2 compliant devices in encrypted form except for the low-assurance certificates where key is stored in software-based containers.

6.2.8 METHOD OF ACTIVATING PRIVATE KEYS

Subscriber Private keys is activated by providing a passphrase set on initial certificate generation by the subscriber.

6.2.9 METHODS OF DEACTIVATING PRIVATE KEYS

Subscriber private keys that have been activated shall not be left unattended. Subscribers are obliged to deactivate the private key by “logging out” of the cryptographic device or automatically after a period of inactivity as configured.

6.2.10 METHODS OF DESTROYING PRIVATE KEYS

For the Subscribers keys stored on hardware security device like smart card / tokens:

The subscriber shall delete their keys and certificates from the device using the appropriate vendor's provided software. Alternatively, the subscribe can re-initialize their hardware token to destroy all its contents.

For the Subscribers keys stored on software-based containers:

The subscriber shall delete the content of the software-based container using the vendor's provided instructions. Alternatively, the subscribe can securely delete the files storing the data of the software-based container.

For the Subscribers keys used for remote signing keys:

The remote signing private key of a subscriber is automatically deleted by the Sirar's remote signing service after the revocation or expiry of the corresponding remote signing certificate.

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	Key Length in Bits	Maximum Validity Period
Subscriber keys	2048	36 months
RA keys	2048	36 months
OCSP Signing Key	2048	36 months
Timestamping signing Key	2048	60 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 RA, OCSP responder, Timestamping or 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 QUCA 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 QUCA 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 QUCA systems configuration, modification and upgrades are documented and controlled by the PKI operations management. A vulnerability management process is enforced to ensure that the QUCA 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

QUCA LOCAL Signing Certificate (High Assurance)

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	[1]At least 64 bits of entropy validated on duplicates.	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = STCS QUCA O = STCS 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=<English Full Name and/or Arabic Full Name>, surName = <optional English-Lastname> <optional Arabic-Lastname>, E = <emailaddress>, SN = <optional SerialNumber>, OU=<High Assurance >,OU=<optional RA Name>, OU=<optional Name of Customer Base>, OU=<optional Subject organization name>, O = STCS, C = SA”.	V1 Field
SubjectPublicKeyInfo	Public Key Key length: 2048 (RSA)	V1 Field
SubjectAltName	RFC822[2] Name=<emailaddress>	No
CRL Distribution Points	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sirar.com.sa/CRL/stcs_quca_stcs_sa_crlfile.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 Qualified 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 =< **2.16.682.1.101.5000.1.4.1.2.1.12** > [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sirar.com.sa/repository [2]Certificate Policy: Policy Identifier =<**2.16.682.1.101.5000.1.4.1.2.1.11.5.1.3**>	NO

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

[2] Exists only when the email address is included in the Subject

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

MEDIUM Assurance Digital Signing Certificate

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 = STCS QUCA O = STCS 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=<English Full Name and/or Arabic Full Name>, givenName = <optional English-Firstname> < optional Arabic-FirstName>, surName = <optional English-Lastname> <optional Arabic-Lastname>, E = <Optional emailaddress>, SN = <optional SerialNumber>, OU=Medium Assurance, OU=<optional RA Name>, OU=<optional Name of Customer Base>, OU=<optional Subject organization name>, O = STCS, C = SA".	V1 Field
SubjectPublic KeyInfo	Public Key Key length: 2048 (RSA)	V1 Field
SubjectAltName	[4]RFC822 Name=<emailaddress>	No
CRL Distribution Points	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: http://crl.sirar.com.sa/CRL/stcs_quca_stcs_sa_crlfile.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 Qualified 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 =< **2.16.682.1.101.5000.1.4.1.2.1.12** > [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sirar.com.sa/repository [2]Certificate Policy: Policy Identifier =<**2.16.682.1.101.5000.1.4.1.2.1.11.5.2.2**>	NO

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

[4] Exists only when the email address is included in the Subject

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

HIGH Assurance Digital Signing Certificate

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	[5]At least 64 bits of entropy validated on duplicates.	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = STCS QUCA O = STCS 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=< English Full Name and/or Arabic Full Name>, givenName = <optional English-Firstname> < optional Arabic-FirstName>, surName = <optional English-Lastname> <optional Arabic-Lastname>, E = <Optional emailaddress>, SN = <optional SerialNumber>, OU=High Assurance, OU=<optional RA Name>, OU=<optional Name of Customer Base>, OU=<optional Subject organization name>, O = STCS, C = SA"	V1 Field
SubjectPublic KeyInfo	Public Key Key length: 2048 (RSA)	V1 Field
SubjectAltName	[6]RFC822 Name=<emailaddress>	No
CRL Distribution Points	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.sirar.com.sa/CRL/stcs_quca_stcs_sa_crlfile.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 Qualified 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 =< **2.16.682.1.101.5000.1.4.1.2.1.12** > [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sirar.com.sa/repository [2]Certificate Policy:	NO

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

[6] Exists only when the email address is included in the Subject

Field / x.509 extension	Value or Value Constant	Critical
	Policy Identifier =<**2.16.682.1.101.5000.1.4.1.2.1.11.5.2.3**>	
Authority Information Access	[1]Authority Info Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sirar.com.sa [2]Authority Info Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl.sirar.com.sa/certs/stcs_quca.crt	NO
Key Usage	Nonrepudiation	YES

STCS QUCA RA Certificate Profile

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	[7]At least 64 bits of entropy validated on duplicates.	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = STCS QUCA O = STCS 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 = < Organization name> OU = <Organization RA_id name> OU = <optional search bases> O = STCS C = SA	V1 Field
SubjectPublicKeyInfo	Public Key Key length: 2048 (RSA)	V1 Field
CRL Distribution Points	e.g [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sirar.com.sa/CRL/stcs_quca_stcs_sa_crlfile.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 Qualified CA** (excluding the tag, length, and number of unused bits).	Yes
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=<**2.16.682.1.101.5000.1.4.1.2.1.12**> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sirar.com.sa/repository [2]Certificate Policy: Policy Identifier=<**2.16.682.1.101.5000.1.4.1.2.1.11.7.1**>	NO
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	NO

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

Field / x.509 extension	Value or Value Constant	Critical
	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl.sirar.com.sa/certs/stcs_quca.crt	
Key Usage	Digital Signature, keyEncipherment	YES

eSEAL Medium LOA Digital Signing Certificate

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	[8]At least 64 bits of entropy validated on duplicates.	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = STCS QUCA O = STCS 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 = <Organization Name/Trade Name> <Arabic Organization Name/Trade Name> , OrganizationIdentifier=<National Unique Identifier e.g. VATSA-[VAT NUMBER]> , OU=<Full registered name of the organization> O = STCS OU=<Medium Assurance> OU = <Optional RA Name> C = SA”	V1 Field
SubjectPublic KeyInfo	Public Key Key length: 2048 (RSA)	V1 Field
CRL Distribution Points	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sirar.com.sa/CRL/stcs_quca_stcs_sa_crlfile.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 Qualified 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 =< **2.16.682.1.101.5000.1.4.1.2.1.12** > [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sirar.com.sa/repository	NO

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

Field / x.509 extension	Value or Value Constant	Critical
	[2]Certificate Policy: Policy Identifier =< **2.16.682.1.101.5000.1.4.1.2.1.11.6.1** >	
Authority Information Access	[1]Authority Info Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sirar.com.sa [2]Authority Info Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl.sirar.com.sa/certs/stcs_quca.crt	NO
Key Usage	digitalSignature	YES

eSEAL HIGH LOA Digital Signing Certificate

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	[9]At least 64 bits of entropy validated on duplicates.	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = STCS QUCA O = STCS 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 = <Organization Name/Trade Name> <Arabic Organization Name/Trade Name> , OrganizationIdentifier=<National Unique Identifier e.g. VATSA-[VAT NUMBER]> , OU=<Full registered name of the organization> O = STCS OU=<High Assurance> OU = <Optional RA Name> C = SA”	V1 Field
SubjectPublic KeyInfo	Public Key Key length: 2048 (RSA)	V1 Field
CRL Distribution Points	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.sirar.com.sa/CRL/stcs_quca_stcs_sa_crlfile.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 Qualified CA (excluding the tag, length, and number of unused bits).	NO

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

Field / x.509 extension	Value or Value Constant	Critical
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 =< **2.16.682.1.101.5000.1.4.1.2.1.12** > [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sirar.com.sa/repository [2]Certificate Policy: Policy Identifier =<**2.16.682.1.101.5000.1.4.1.2.1.11.6.2**>	NO
Authority Information Access	[1]Authority Info Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.sirar.com.sa [2]Authority Info Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://crl.sirar.com.sa/certs/stcs_quca.crt	NO
Key Usage	digitalSignature	YES

TIMESTAMPING Authority Certificate Profile

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	[10]At least 64 bits of entropy validated on duplicates.	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = STCS QUCA O = STCS C = SA	V1 Field
NotBefore	Certificate generation process date/time.	V1 Field
NotAfter	Certificate generation process date/time + Up to 60 months (5 years)	V1 Field
Subject	CN = STCS TimeStamping Authority O = STCS C = SA	V1 Field
SubjectPublic KeyInfo	Public Key Key length: 2048 (RSA)	V1 Field
CRL Distribution Points	e.g. [1] CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.sirar.com.sa/CRL/stcs_quca_stcs_sa_crlfile.crl	NO

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

Field / x.509 extension	Value or Value Constant	Critical
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=< **2.16.682.1.101.5000.1.4.1.2.1.12**> [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=<**2.16.682.1.101.5000.1.4.1.2.1.11.7.3**>	NO
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/stcs_quca.crt	NO
Key Usage	digitalSignature	YES
Extended keyUsage	timeStamping	YES

7.1.1 VERSION NUMBERS

The QUCA 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

QUCA 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 QUCA 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 QUCA 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 QUCA CRL Profile is shown below:

7.2.1 QUCA CRL PROFILE

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

7.2.2 VERSION NUMBERS

The QUCA 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

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

The OCSP response signing certificate profile is as follows:

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	[11]At least 64 bits of entropy validated on duplicates.	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = STCS QUCA O = STCS 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

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

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = STCS QUCA OCSP Service O = STCS C = SA	V1 Field
SubjectPublicKeyInfo	Public Key Key length: 2048 (RSA)	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 **QUCA** (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=<**2.16.682.1.101.5000.1.4.1.2.1.12**> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.sirar.com.sa/repository [2]Certificate Policy: Policy Identifier=<**2.16.682.1.101.5000.1.4.1.2.1.11.7.2**>	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 QUCA 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 QUCA to 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 QUCA shall undergo annual WebTrust audits whose results shall be submitted to NCDC 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 QUCA shall be subjected 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 QUCA 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 QUCA is audited for compliance to the AICPA/CICA Trust Service Principles and Criteria for Certification Authorities.

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

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If irregularities are found by the auditor, Sirar shall be informed in writing of the findings. Sirar shall submit a report to the auditor or directly to NCDC, as determined by NCDC, 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 NCDC as appropriate.

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

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 NCDC 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 re-key.

9.1.2 CERTIFICATE ACCESS FEES

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

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEE

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

9.1.4 FEES FOR OTHER SERVICES

Sirar may charge fees for other services such as timestamping.

9.1.5 REFUND POLICY

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

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

9.2.1 INSURANCE COVERAGE

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

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

9.2.2 OTHER ASSETS

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

9.2.3 INSURANCE/WARRANTY COVERAGE FOR END-ENTITIES

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Information pertaining to the QUCA 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 CP, 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 QUCA due to:

- The compromise of their private key, in which case a disclosure may be made that the private key has been compromised; or
- The termination of the QUCA 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 QUCA 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 the Sirar's contractual obligations that at least as protective as the terms specified in section 9.4.1.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

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

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL/ADMINISTRATIVE PROCESS

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

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

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

9.5 INTELLECTUAL PROPERTY RIGHTS

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 it conducts an efficient and trustworthy operation. "Reasonable efforts" include but are not limited to operating in compliance with:
  - Documented CP and CPS;
  - Documented Sirar's Operations Policies and Procedures; and
  - Within applicable agreements, Saudi Law and regulations.
- At the time of Certificate issuance; Sirar 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's, the Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the CA keys and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key CA private key is generated using multi-person control "m-of-n" split key knowledge scheme;
- Backing up of the CA signing Private Key is under the same multi-person control as the original Signing Key;
- Keep confidential, any passwords, PINs or other personal secrets used in obtaining authenticated access to PKI facilities and maintain proper control procedures for all such personal secrets;
- Use its private signing key only to sign certificates and CRLs and for no other purpose;
- Perform authentication and identification procedures in accordance with applicable Agreement and Sirar's Operations Policies and Procedures;
- Provide certificate and key management services in accordance with the CP and CPS; and
- Ensure that CA personnel use private keys issued for the purpose of conducting CA duties only for such purposes.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

Sirar 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 human 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 QUCA/RA for specific Certificate type to be issued by the QUCA;
   - 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 password, 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 QUCA/RA in the event that any information in the Certificate is, or becomes, incorrect or inaccurate;
   - Notify the QUCA/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 the 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 QUCA/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 warranty, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of the QUCA 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 their negligence, fraud or willful misconduct;
- Sirar assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under Certificate Policy for any use other than in accordance with Certificate Policy. Relying Parties will immediately indemnify Sirar from and against any such liability and costs and claims arising there from;
- Sirar will not be liable to any party whosoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services;
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations described in the Relying Party agreement;
- Sirar denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 TERM

This CPS shall be effective upon approval by the PKI Committee. The NCDC 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 QUCA participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

All communication between NCDC, Saudi National Root CA, and Sirar, the QUCA 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 NCDC. The final agreed amendments are approved and applied by the PKI Committee.

Sirar's 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 QUCA 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 URL's, 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 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 QUCA 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 Kingdom of Saudi Arabia. Legal disputes arising from the operation of the QUCA 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 process shall be specified in corresponding agreements and any Sirar Operational policies.

APPENDIX-A: CERTIFICATE TYPES & POLICIES

A.1 CERTIFICATE TYPES SUPPORTED

A.1.1 DIGITAL SIGNING CERTIFICATE SERVICE (IDS)

A.1.1.1 Digital Signing Certificate issuance requirements And Usage : MEDIUM Assurance Certificate (MAC)

S. No.	Attribute	Digital Signing Certificate
1	Policy Name	Sirar Medium Assurance Digital Signing Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.11.5.2.2**
3	Application Usage	Intended for digitally signing transactions and documents by individuals. These certificates are issued under the STCS Qualified CA (QUCA) in compliance with the requirements of **Medium Assurance Level** certificates as per Saudi National PKI Policy. These certificates are general purpose certificates that are not tied to any specific application or function. The applications using the QUCA issued Digital Identity Certificates should honour Key Usage set in the certificates The Digital Signing certificate may also be used for other general or specific QUCA purposes which are not covered explicitly above, provided that a Relying Party is able to reasonably rely on that certificate and the usage is as per the QUCA practices, Subscriber's agreement and not otherwise prohibited by law of Saudi Arabia.

4	Verification Process	• Applicant's identity data is retrieved from one of the following sources:
		  ○ a government issued ID, in which case, the authenticity of document(s) is verified beforehand; or
		  ○ an existing identity provider such as IAM/NAFATH/ELM; or
		  ○ trusted KYC database such as a bank KYC
		• The QUCA/RA checks that the applicant is the sole claimant of the identity
		• A binding of the claimed identity shall be performed by checking the link between the applicant and the claimed identity using strong 2-factor authentication. That authentication is done leveraging the applicant's existing account at the trusted KYC database
		• The QUCA/RA checks the existence of the email address supplied and that the subscriber has control over it
		
		If the certificate subject includes an organization's name:
		• Company or legal documents from a company registration authority shall be provided and verified
		• Identity document of the applicant and the authorization that confirms the permission to apply the certificate on behalf of the organization to be provided, and that the applicant is a member of the organization
		• RA shall verify the existence of the email address provided and that the subscriber/applicant has control over the email address
		• RA shall verify the existence of the organization by using a public register

5	Key Pair Generation and Protection	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. Subscriber may use Hardware Security device like smart card / tokens for key generation and storage. Software generated keys are also supported, provided the process complies with the requirements of FIPS 186. **If generated in Cryptographic device, the device must be certified to at least FIPS 140-2 Level 2.**

S. No.	Attribute	Digital Signing Certificate
6	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber is authenticated remotely as explained in row 5 above • The applicant's identity information is retrieved from the sources described at row 5 above • The QUCA or the RA proceed with the certificate issuance as follows: • **Local signing certificates:** o The subscriber will go to QUCA/RA service centre (or remotely for software generated keys) o The Subscriber will plug his smart card / USB token into the customization device. o The Subscriber will enter the PIN of the smart card / USB token o The Subscriber will enter reference number and an authorization code to generate keys and download certificates. o The Client Software will generate the Subscriber's keys securely on his smart card / USB token. o The RA will authenticate the Subscriber using the reference number and authorization code and receive the certificate signing request using a secure protocol such as PKIX-CMP. Upon successful authentication, the RA shall request for the creating of the Subscribers certificates and transport them securely onto the Subscriber's smart cards / USB tokens once approved by the CA. Software generated keys shall follow the same process, except there will be no cryptographic device for key generation or storage. Instead, the certificate shall be made available via a PKCS#12 formatted file. • **Remote signing certificates:** o The QUCA/RA creates an account for the applicant in the remote signing service o The user keys are generated inside the remote signing service o A certificate request is sent to the CA then the certificate is issued and returned to the remote signing service o The remote signing account is activated and the subscriber is notified.
7	Asymmetric Key Length	Minimum 2048 bits RSA
8	Certificate Re-key	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. • 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.

A.1.1.2 Digital Signing Certificate issuance requirements And Usage: HIGH Assurance Certificate (HAC)

S. No.	Attribute	Digital Identity Certificate
1	Policy Name	Sirar Digital Signing Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.11.5.2.3**

S. No.	Attribute	Digital Identity Certificate
3	Application Usage	The Sirar High Assurance Digital Signing certificate is intended to produce legally binding signatures. They are issued under the STCS Qualified CA (QUCA). These Digital Signing certificates comply with the requirements of **High Assurance Level** certificates as per Saudi National PKI Policy.
4	Verification Process	• Applicant's identity data is retrieved from one of the following sources: o a government issued ID, in which case, the authenticity of document(s) is verified beforehand; or o an existing identity provider such as IAM/NAFATH/ELM. • The QUCA/RA checks that the applicant is the sole claimant of the identity • A binding of the claimed identity shall be performed by checking the link between the applicant and the claimed identity through one of the following methods: o In-person verification where person's face is visually matched by an officer against a photo on a government issued photo ID, or; o Strong 2-factor authentication offered by IAM/NAFATH/ELM , or; o Biometric varication, such as the fingerprint verification service offered by IAM/NAFATH/ELM. • The QUCA/RA checks the existence of the email address supplied and that the subscriber has control over it **If the certificate subject includes an organization's name:** • Company or legal documents from a company registration authority shall be provided and verified • Identity document of the applicant and the authorization that confirms the permission to apply the certificate on behalf of the organization to be provided, and that the applicant is a member of the organization • QUCA/RA shall verify the existence of the email address provided and that the subscriber/applicant has control over the email address • QUCA/RA shall verify the existence of the organization by using a public register
5	Key Pair Generation and Protection	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, subscriber shall use Hardware Security device like smart card / tokens for key generation and storage. **Keys for High Level Assurance certificates MUST be generated and stored on the secured hardware meeting the minimum requirements as mentioned in the CP.** The Digital Signing Private keys must be generated and stored on FIPS 140-2 Level 2 or higher certified hardware. The QUCA/RA shall not retain any copy of the subscriber Private Keys.
6	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The applicant' identity verification process is done as explained in row 5 above. • The applicant's identity information is retrieved from the sources described at row 5 above • The QUCA/RA proceed with the certificate issuance as follows: • **Local signing certificates:** o The subscriber will go to QUCA/RA service centre o The Subscriber will plug his smart card / USB token into the customization device. o The Subscriber will enter the PIN of the smart card / USB token o The Subscriber will enter reference number and an authorization code to generate keys and download certificates. o The Client Software will generate the Subscriber's keys securely on his smart card / USB token. o The QUCA/RA will authenticate the Subscriber using the reference number and authorization code and receive the certificate signing request using a secure protocol such as PKIX-CMP. Upon successful authentication, the QUCA/RA shall request for the creating of the

S. No.	Attribute	Digital Identity Certificate
		Subscribers certificates and transport them securely onto the Subscriber's smart cards / USB tokens once approved by the CA. • **Remote signing certificates:** o The QUCA/RA creates an account for the applicant in the remote signing service o The user keys are generated inside the remote signing service A certificate request is sent to the CA then the certificate is issued and returned to the remote signing service o The remote signing account is activated, and the subscriber is notified.
7	Asymmetric Key Length	Minimum 2048 bits RSA
8	Certificate Re-key	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. • 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.

A.1.2 E-SEAL CERTIFICATES

A.1.2.1 eSeal Certificate issuance requirements And Usage: Medium Assurance Certificate (MAC)

S. No.	Attribute	Digital Identity Certificate
1	Policy Name	Sirar Medium Assurance eSeal Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.11.6.1**
3	Application Usage	Used to add an eSeal on a document issued\attested by an organization. These certificates comply with the requirements of **Medium Assurance Level** certificates as per Saudi National PKI Policy.
4	Verification Process	• The following data is verified by QUCA based on STC KYC Database: 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 • The QUCA 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) • The QUCA verifies the Organizations existence as mentioned in section 3.2.2 • The QUCA verifies the organization's address to confirm if it is the same address where the organization conducts its operation. • The QUCA verifies the identity of the certificate requester according to the submitted identity documents.

S. No.	Attribute	Digital Identity Certificate
5	Key Pair Generation and Protection	The keys will be generated and stored using Hardware Security Module of Sirar remote signing service.
6	Certificate Issuance Process	Certificates shall only be issued to Organization with valid legal standing in Saudi as follows: • The QUCA/RA creates an account for the organization's certificate in the remote signing service • The signing keys are generated inside the remote signing service • A certificate request is sent to the CA then the certificate is issued and returned to the remote signing service • The remote signing account is activated • Handover the account's credentials securely to the certificate requester
7	Asymmetric Key Length	Minimum 2048 bits RSA
8	Certificate Re-key	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. • 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.

A.1.2.2 eSeal Certificate issuance requirements And Usage: High Assurance Certificate (HAC)

S. No.	Attribute	Digital Identity Certificate
1	Policy Name	Sirar High Assurance eSeal Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.11.6.2**
3	Application Usage	Used to add an eSeal on a document issued\attested by an organization. These certificates comply with the requirements of **High Assurance Level** certificates as per Saudi National PKI Policy.
4	Verification Process	• The following validation data is verified by QUCA 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 • The QUCA reviews all the submitted documents and validate the filled information • The QUCA 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) • The QUCA verifies the Organizations existence as mentioned in section 3.2.2 • The QUCA verifies the organization's address to confirm if it is the same address where the organization conducts its operation

S. No.	Attribute	Digital Identity Certificate
		• The QUCA 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. • The QUCA verifies the identity of the certificate requester according to the submitted identity documents.
5	Key Pair Generation and Protection	The keys will be generated and stored using Hardware Security Module of Sirar remote signing service.
6	Certificate Issuance Process	Certificates shall only be issued to Organization with valid legal standing in Saudi as follows: • The QUCA/RA creates an account for the organization's certificate in the remote signing service • The signing keys are generated inside the remote signing service • A certificate request is sent to the CA then the certificate is issued and returned to the remote signing service • The remote signing account is activated • Handover the account's credentials securely to the certificate requester
7	Asymmetric Key Length	Minimum 2048 bits RSA
8	Certificate Re-key	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. • 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.

A.1.3 RA IDENTITY CERTIFICATE (RA CERTIFICATE)

This is the Registration Authority (RA) Certificate Issued by the QUCA. The RA certificate is used to authenticate RA application requests to the CA if so implemented.

A.1.3.1 RA Certificate issuance requirements And Usage

S. No.	Attribute	RA Certificate
1	Policy Name	QUCA RA Identity Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.11.7.1**
3	Application Usage	QUCA RA Certificates are RA Identity Certificates. They are specifically issued to identify and authenticate RA requests to the CA, such as requesting subscriber certificates. They will be used by the RA applications that are authorized to manage subscribers and the corresponding lifecycle of their certificates. The RA applications using the QUCA issued RA Certificate should honour the Key Usage and any Extensions set in the certificate. The RA certificates shall comply with the requirements for a **Medium (or Substantial)** Level of Assurance (LoA) as described in the Saudi National PKI Policy.

4	Verification Process	The process of verifying the Sirar RA Identity certificate request is done as part of the RA Take on process or contract renewal process. The following process shall apply: • The Request for an RA certificate shall be requested by the PKI Committee or authorized RA representative • The request shall be accompanied by a signed RA Agreement. • The request shall also be accompanied by documented evidence of the RA approval • The Identity of the requesting party shall be verified. If the applicant is an external party, the applicant shall produce a government issued identity document.
5	Key Pair Generation and Installation	Keypair 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. Where Cryptographic devices are used, the Sirar RA Keypairs shall be generated using devices meeting the stipulated FIPS 140-2 Level.
6	Certificate Issuance Process	The certificate is issued as part of the Key Ceremony Process A signed PKCS#10 formatted CSR is provided to the QUCA that shall in turn sign the request. The signed certificate shall be returned to complete the process of the QUCA configuration
7	Private Key Protection	The Sirar RA Certificate Private Keys shall be protected using a trustworthy key storage mechanisms or Hardware Security Module meeting FIPS140-2 Level 2 requirements.
8	Asymmetric Key Length	Minimum 2048 bits RSA
9	Certificate Re-key	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. • 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.

A.1.3 ONLINE CERTIFICATE STATUS PROTOCOL CERTIFICATE (OCSP CERTIFICATE)

The OCSP certificate is issued to the OCSP responder service. The certificate is used to sign OCSP requests.

A.1.3.1 OCSP Certificate issuance requirements And Usage

S. No.	Attribute	OCSP Certificate
1	Policy Name	QUCA OCSP Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.11.7.2**
3	Application Usage	QUCA OCSP Certificates are used for signing of OCSP responses. They are specifically issued to sign responses from an OCSP responder service. The OCSP Responder applications using the QUCA issued OCSP Certificate should honour the Key Usage and any Extensions set in the certificate.
4	Verification Process	The process of verifying the Sirar OCSP certificate request is done as part of setting up the CA services (immediately after a Key Ceremony). The following process shall apply:

		• The Request for the OCSP certificate shall be requested by the PKI Committee or authorized CA representative • The request shall be accompanied by documented evidence of the OCSP Responder service approval • The Identity of the requesting party shall be verified.
5	Key Pair Generation and Installation	Keypair 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. Where Cryptographic devices are used, the OCSP Keypairs shall be generated using devices meeting the stipulated FIPS 140-2 Level.
6	Certificate Issuance Process	A signed PKCS#10 formatted CSR is provided to the QUCA that shall in turn sign the request. The signed certificate shall be returned to complete the process of the QUCA OCSP Responder configuration
7	Private Key Protection	The QUCA OCSP Certificate Private Keys shall be protected using a Hardware Security Module meeting FIPS140-2 Level 2 requirements.
8	Asymmetric Key Length	Minimum 2048 bits RSA
9	Certificate Re-key	Certificate re-key may happen while the certificate is still active or after it has expired. The routine re-key of the OCSP certificates is done according Sirar internal Operations Policies and Procedures.

A.1.4 LOCAL SIGNING SERVICES (LSS)

This service uses cryptographic keys stored locally to create a signature and allows the user to sign documents/data using a certificate stored on their ID card, USB Token, etc. The service will be integrated with the PKI platform.

A.1.4.1 LOCAL SIGNING CERTIFICATE ISSUANCE REQUIREMENTS AND USAGE

S. No.	Attribute	Local Signing Certificate
1	Policy Name	Local Signing Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.11.5.1.3**
3	Application Usage	QUCA issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the QUCA issued Local Signing Certificate should honour Key Usage. The Local Signing certificate should be used for local signing using a secure token or Smartcard and may also be used to verify data integrity. Following are some of the common usage of the certificate • Digital Signatures • Electronic Transaction signing • Digital submission of forms • B2B or B2C correspondence. The Local signing certificate may also be used for other general or specific QUCA purposes which are not covered explicitly above, provided that a Relying Party is able to reasonably rely on that certificate and the usage is as per the QUCA practices, Subscriber's agreement and not otherwise prohibited by law of Saudi Arabia.
4	Verification Process	1. Subscriber shall be required to attend to the QUCA/RA for face-to-face identity validation (or an equivalent electronic process) and submission of supporting documents. 2. The following will be considered valid identity documents:

S. No.	Attribute	Local Signing Certificate
		• National ID / passport for citizens. • Residence permit / passport for residents. 3. Letter from an authorized party (as prescribed by the QUCA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process 4. During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics 5. Where a Subscriber/approver have already undergone face-to-face identity and authentication process by the QUCA/RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by a valid High-Assurance Sirar Certificate Type.
5	Key Pair Generation and Installation	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, subscriber shall use Hardware Security device like smart card / tokens for key generation and storage. **All Local Signing certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the CP.** The Local Signing Private keys must be generated and stored on FIPS 140-2 Level 2 or higher certified hardware token or smart card, and the QUCA/RA shall not retain any copy of the subscriber Private Keys. In addition, the Subscriber shall acknowledge receipt of the private key(s).
6	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber will be present at the QUCA/RA for face-to-face identity verification or an equivalent electronic identity verification process • The QUCA/RA will validate the documents submitted by the subscriber • The QUCA/RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner. • The subscriber will go to the QUCA/RA customization centre • The Subscriber will plug his smart card / USB token into the customization device. • The Subscriber will enter the PIN of the smart card / USB token • The Subscriber will enter reference number and an authorization code to generate keys and download certificates. • The Client Software will generate the Subscriber's keys securely on his smart card / USB token. • The QUCA/RA will authenticate the Subscriber using the reference number and authorization code and receive the certificate signing request using a secure protocol such as PKIX-CMP. Upon successful authentication, the QUCA/RA shall create the Subscribers certificates and transport them securely onto the Subscriber's smart cards / USB tokens.
7	Private Key Protection	Subscribers shall protect their private keys in a FIPS 140-2 Level 2 or higher certified smart card or other hardware token/module. Subscriber is obligated to secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key. Generation and/or Storage of name authentication private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.
8	Asymmetric Key Length	Minimum 2048 bits RSA
9	Certificate Re-key	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	Local Signing 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.

A.1.5 TRUSTED TIMESTAMPING SERVICES (TTS)

This service allows parties to bind electronic data to a particular time establishing evidence that these data existed before that time. Part of TTS is an internet facing Webservice allowing parties to request and receive timestamps. The timestamps themselves will be based on Digital Signature certificates issued by QUCA. Access to timestamp requests are controlled through using authentication mechanisms such as certificates. Other forms of access control shall also be possible. Timestamps are also used for validation (crl, oscp services), PDF signing with timestamp and PDF signing with long-term validation (LTV) online services.

S. No.	Attribute	TTS Certificate
1	Policy Name	QUCA TTS Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.11.7.3**
3	Application Usage	QUCA TTS Certificates are used for signing time stamp transactions. The trusted time source uses an accurate time source and shall comply with RFC 3161. The TTS applications using the QUCA issued TTS Certificate should honour the Key Usage and any Extensions set in the certificate.
4	Verification Process	The process of verifying the Sirar TTS certificate request is done as part of setting up the CA services. The following process shall apply: • The Request for the TTS certificate shall be requested by the PKI Committee or authorized CA representative • The request shall be accompanied by documented evidence of the TTS service approval • The Identity of the requesting party shall be verified.
5	Key Pair Generation and Installation	Keypair 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. Where Cryptographic devices are used, the Sirar TTS Keypairs shall be generated using devices meeting the stipulated FIPS 140-2 Level.
6	Certificate Issuance Process	A signed PKCS#10 formatted CSR is provided to the QUCA that shall in turn sign the request. The signed certificate shall be returned to complete the process of the QUCA TTS configuration
7	Private Key Protection	The QUCA TTS Certificate Private Keys shall be protected using a Hardware Security Module meeting FIPS140-2 Level 2 requirements.
8	Asymmetric Key Length	Minimum 2048 bits RSA
9	Certificate Re-key	Certificate re-key may happen while the certificate is still active or after it has expired. The routine re-key of the TTS certificates is done according Sirar internal Operations Policies and Procedures.