QUALIFIED CA (QUCA) CERTIFICATE POLICY

Document Classification:

Public

Version Number: 2.3

Issue Date: 03 Jul 2023

Document Reference

Item	Description
Document Title:	Sirar Qualified CA (QUCA) Certificate Policy
Custodian Department:	Sirar's Product Management
Owner:	Sirar's Policy Authority
Version Number:	2.3
Document Status:	Final

Document Author:	Sirar's Policy authority	
	PKI Consultant	Signature/Date
Approved by:	Fahad I. Aljutaily	Signed by:Fahad Aljutaily Signed at:2023-09-10 11:35:55 +03:00 Reason:I approve this document Fahad Aljutaily
	Sirar CEO	Signature/Date

HA

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	27/11/2019	K Hlabathi	Final incorporating reviews
1.1	18/12/2019	K Hlabathi	Final for NCDC approval and publishing after Deloitte review
1.2	23/12/2019	K Hlabathi	Added signatory. For final approval and publishing
1.3	04/01/2020	Katekani Hlabathi	Updates after Deloitte Readiness Assessment review. For approval and repository update
1.4	16/07/2020	STCS Policy Authority	Updates based on regular review
1.5	16/08/2020	STCS Policy Authority	Addressing the comments received during the period of time audit
1.6	30/09/2021	Solutions' Policy Authority	Annual review
2.0	15/06/2022	Sirar's Policy Authority	Document issuance under Sirar's name
2.1	07/11/2022	Sirar's Policy Authority	Add the support of ECDSA keys for subscriber certificates
2.2	08/01/2023	Sirar's Policy Authority	Update identify verification methods under section 3.2.3 Re-key process updated under section 4.7.1
2.3	03/07/2023	Sirar's Policy Authority	- Annual review - Added definitions and acronyms

Document Control

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

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

Table of Contents

1. INTRODUCTION

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:

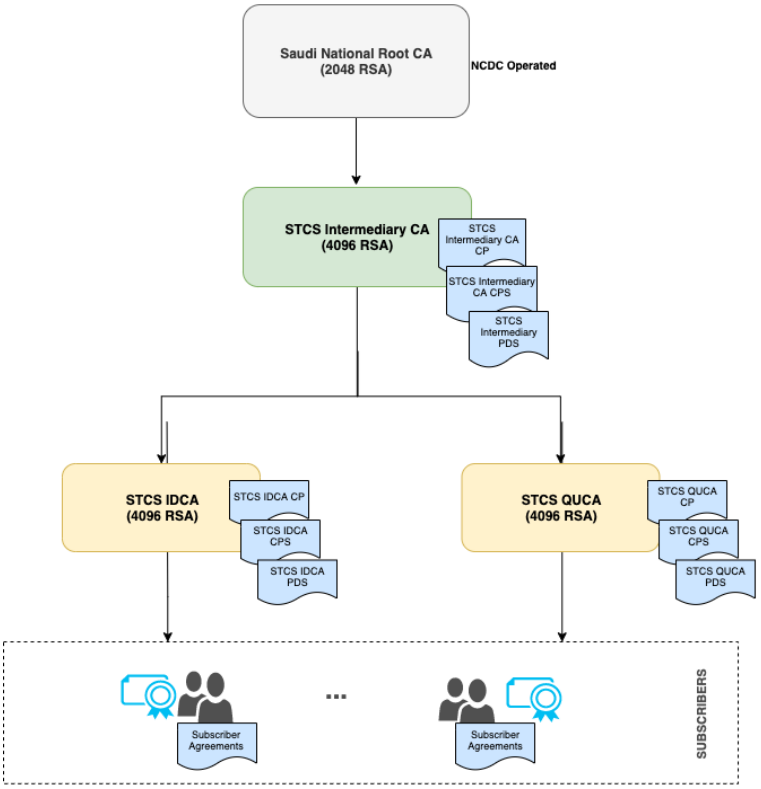

Figure 1-Sirar's PKI and Governance Hierarchy

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

- Saudi National PKI Policy,
- Sirar Intermediary CA 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

The QUCA is an Issuing CA that issues certificates to subscribers and signs Certificate Revocation Lists (CRLs) containing revoked certificates for those end users.

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

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

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

1.1.1 CERTIFICATE POLICY

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

1.1.2 RELATIONSHIP BETWEEN THE CP AND THE CPS

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

The CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by the QUCA as governed by this CP and related documents which describe the Sirar’s PKI 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 CP 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 Certificate Policy (CP), and is identified by the object identifier (OID):

OID: 2.16.682.1.101.5000.1.4.1.2.1.11

1.3 PKI PARTICIPANTS

The following are subcomponents of the QUCA that are governed by this CP.

Several parties constitute the participants of the QUCA. The parties mentioned hereunder including the Certification Authorities, the Sirar's PKI committee, subscribers and relying parties are collectively called PKI participants.

1.3.1 CERTIFICATION AUTHORITIES

The Sirar's PKI is an umbrella term referring to the Sirar as an organization that runs PKI services under the Saudi National Root CA. The 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, timestamping certificates and other certificates required by the internal PKI components. The Issuing CAs issue certificates to Subscribers in accordance with each respective CP and the CPS, their RA Agreement, Subscriber Agreement, Relying Party Agreement, and the Saudi National PKI Policy.

Sirar as an entity is responsible for:

- Control over the designation of 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 the 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 this CP, the CPS as well as the related documents.

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

- Process Certificate application requests in accordance with this CP, the CPS 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 CP, the CPS, 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 CP;
- Comply with the provisions of its RA Agreement and the provisions of this CP 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 CP, the CPS 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 this CP and the 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 CP,

requirements for reliance, and limitations thereon, are governed by the terms of this CP and the Relying Party Agreement.

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

- The certificate has been used for the purpose for which it has been issued, as described in this CP
- The Relying Party has verified the validity of the digital certificate, using procedures described in the Relying Party Agreement;
- The Relying Party has accepted and agreed to the Relying Party Agreement at the time of relying on the certificate; it shall be deemed to have done so by relying on the certificate; and
- The relying party accepts in totality, the certificate policy applicable to the certificate, which can be identified by reference of the certificate policy OID mentioned in the certificate.

1.3.5 OTHER PARTICIPANTS

1.3.5.1 Sirar's PKI Committee

Sirar's PKI Committee (hereinafter, PKI Committee) operates as the governance function for the Sirar's PKI. It groups the necessary functions for this purpose including the policy, compliance and design functions. The PKI Committee provides strategic direction and continuously supervises the PKI operations team. This committee is appointed by Sirar.

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

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

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

the QUCA issues Subscriber, Registration Authority, Timestamping certificate andOnline Certificate Status Protocol (OCSP) responder certificates. The subscriber certificates are used to digitally sign documents, data and transactions. The RA certificates are used to identify the RA to the QUCA when the RA Application interacts with the CA.

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

Timestamping certificates for signing timestamps issued for Sirar's TimeStamping Authority.

The QUCA issues certificates under this CP 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 levels of assurance are offered to subscribers in the form of end entity certificates issued by the QUCA. The Levels of Assurance is in line with levels described in the Saudi National PKI Policy.

Assurance Level	Description of Assurance Level
Medium Assurance Certificates	The certificates issued at this level provide medium confidence in the accuracy or legitimacy of the claimed identity. Identity assertions at this level are appropriate for transactions with serious or substantial consequences to Relying Parties. Identity at this level is verified with authoritative sources.
High Assurance Certificates	The certificates issued at this level provide high confidence in the accuracy or legitimacy of the claimed identity. It is intended of subscribers handling information of high value and that can have catastrophic consequences to Relying Parties. Identities at this level is verified with authoritative sources on the basis of a face to face or equivalent method.

1.4.2 PROHIBITED CERTIFICATE USES

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

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

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

1.5.2 CONTACT PERSON

Queries regarding this CP shall be directed to:

Email: PolicyAuthority@sirar.com.sa

Telephone: 909

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

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

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

1.5.4 CPS APPROVAL PROCEDURES

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

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

1.6 DEFINITIONS AND ACRONYMS

1.6.1 DEFINITIONS

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

Applicant Representative: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant. As far as Sirar's PKI is concerned, the applicant representative is in charge of submitting certificate requests and certificate revocation requests on behalf of the applicant.

Attestation Letter: A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA).

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

CA Key Pair: A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

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

Certificate Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List: A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the CA's CPS or a certificate template file used by CA software.

Cryptographic Token: A USB cryptographic device certified as conformant with FIPS 140 Level 2 or equivalent.

CSPRNG: A random number generator intended for use in cryptographic system.

Delegated Third Party: A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Generation Script: A documented plan of procedures for the generation of a CA Key Pair.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Object Identifier: A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol (OCSP): An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

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

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

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

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Sirar's Remote Signing Platform: Hosted and operated by Sirar for offering Remote Signing service to its customers. The Remote Signing Platform handles the following:

- Generates end user key pairs inside the HSM connected to the remote signing server. Private Keys are always generated at the request of the end users, cannot be exported

from the HSM in an unencrypted form and cannot be used for signing operations without the consent of the legitimate end users.

- Stores securely the generated key-pair in an encrypted form using an HSM.
- Enables remote generation of digital signature only when this operation is authorized by the end user himself.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

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

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

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists (Or Verification Officers): Someone who performs the information verification duties specified by these Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

1.6.2 ACRONYMS

CA	Certification Authority
CCTV	Closed Circuit TV
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request

DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
FIPS	Federal Information Processing Standards
EID	Electronic Identity Card
EIDAS	Electronic IDentification, Authentication and trust Services
ETSI	European Telecommunications Standards Institute
PKCS#1	Public Key Cryptography Standards (PKCS) #1
PKCS#7	Cryptographic Message Syntax
PKCS#10	Certification Request Syntax Specification
PKI	Public Key Infrastructure
PA	Policy Authority
RA	Registration Authority
RSA	Rivest-Shamir-Adelman (The names of the inventors of the RSA algorithm)
RTO	Recovery Time Objective
SSL	Secure Sockets Layer
TSA	Timestamping Authority
TLS	Transport Layer Security
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier, a URL, FTP address, email address, etc.
URL	Universal Resource Locator
VO	Verification Officer

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

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

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

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

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

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

The QUCA shall publishes 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 of the CPS, as part of the certificate profile of each certificate file.

2.2.2 PUBLICATION OF CA INFORMATION

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

2.2.3 INTEROPERABILITY

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

2.3 TIME OR FREQUENCY OF PUBLICATION

CRLs for the Subscriber Certificates are issued within 24 hours after revocation. Each CRL includes a monotonically increasing sequence number for each CRL issued.

This CP,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 the PKI Committee.

2.4 ACCESS CONTROLS ON REPOSITORIES

Certificates and certificate status information at the Sirar's PKI repository shall be made available to the 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's shall protect repository information that is not intended for public dissemination or modification using strong authentication, access controls, and an overall Information Security Management System that prevents unauthorized access to information.

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

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

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

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

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

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

CN=STCS QUCA, O=STCS, C=SA

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The QUCA may not issue anonymous or pseudonymous certificates.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

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

3.1.5 UNIQUENESS OF NAMES

All distinguished names shall be unique across the QUCA.

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

The QUCA may perform identification of the Applicant using any legal means of communication or investigation as necessary to validate the identity of the applicant.

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

The QUCA shall verify that the certificate applicant possesses the private key corresponding to the public key being certified by performing signature verification on the certificate request received. The QUCA shall always expect the certificate request to be signed by the private key associated to the public key being certified.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

If the Certificate subject is an organizational entity, then an authorized representative of the entity applies for a certificate. The QUCA shall authenticate, through an approved RA or directly, the identity and authorization of this representative.

For Organizational certificates the applicant must provide the following documents at minimum:

- Organization documents, such as registration documents, issued by a government entity responsible for company registrations.
- A document showing the association of the applicant to the organization

For RA certificates, the request shall contain the following information as a minimum:

- 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

The request shall be supported with an Identity Proof.

The CPS document shall document acceptable methods of performing identity proofing on Organizational entities for the different Levels of Assurance.

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. The QUCA issues three types of certificates:

1) **Medium Level of Assurance Certificates –** the individual's identity shall be verified based on one of the following methods:
   a) A Trusted KYC database shall fulfill one of the following requirements:
      i) Owned and operated by a licensee of Saudi Central Bank (SAMA) or/and Capital Markets Authority (CMA) in Kingdom of Saudi Arabia,
      ii) Owned and operated by an organization that relies on a National Data Owner or a Government ID issuing agency such as those mentioned under point 3.b below.

      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

b) Recorded videos or video calls where person's face is visually verified by an officer against a government issued photo ID.

2) **High Level of Assurance Certificates –** in addition to the requirements apply for Medium Level, the individual's identity shall be verified based on one of the following methods:
   a) In-person verification where person's face is visually matched by an officer against a photo on a government issued photo ID,
   b) Strong 2-factor authentication offered by:
      i) A national data owner such as the Saudi Data & AI Authority (SDAIA), its subsidiaries/affiliates, Service Delivery arms or Agencies,
      ii) A Saudi Government agency that issues a government ID such as passport, driving license, residence permit etc.
   c) Biometric varication, such as face verification or fingerprint verification, or
   d) Receive a digitally signed certificate from by the requestor using a high assurance certificate, issued by a CA participating in the Saudi National PKI.

The respective verification process applicable to specific certificate types and levels of assurance shall be detailed in the CPS document.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Non-verified information shall not be included in high assurance certificates issued by the QUCA, unless specifically mentioned in this CP and the CPS.

3.2.5 VALIDATION OF AUTHORITY

The QUCA shall, before certificate issuance, ensure that the applicant has specific rights, entitlements or permissions to request the certificate.

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 shall use a new key pair at least once every three years. During the Re-keying process the QUCA shall 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.

Subscribers may identify themselves to the QUCA using the currently valid certificate. Otherwise, the identification and authentication steps for Re-Key shall be the same as applied during initial certification.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

If a Subscriber Certificate is revoked, the Subscriber shall go 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 are described in the CPS.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

This section specifies the requirements for initial application for certificate issuance by the QUCA through its Registration Authorities. The RA shall perform 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 will perform the following steps when it receives the confirmation and certificate information from the RA:

- Verify that the transmission is from an authorized RA;
- Private key ownership verification to be performed by CA or RA;
- Generate the Certificate relating to that Applicant; and
- Transmits the Certificate to the Applicant and/or to the requesting RA.

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

Either the Applicant or an individual authorized to request certificates on behalf of the Applicant may 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

For any requested certificate, the subscriber shall ratify a dedicated subscriber agreement. Further details on the enrolment process shall be specified in the CPS.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

Refer to section 3.2 of this CP. More details on the verification process shall be specified in the CPS for the different certificate types.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

An application for a subscriber certificate shall be approved if the following criteria are met:

- Successful identification and authentication of all required Subscriber information as described in Appendix-A of the QUCA CPS, for each respective certificate type.

Certificate application shall be rejected 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 RA believes that issuing a certificate to the Subscriber may bring Sirar into disrepute.
- The applicant fails to prove private key ownership

Policies specific to each certificate type have been detailed in the CPS.

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

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

When RAs receive a request for Certificate, it is not issued before the applicant accepts the terms of a Subscriber Agreement, successfully completes the application form and the RA request has been successfully validated using mechanisms such as validating the digital signature of the RA.

Following successfully completion of the registration process, the QUCA will create and sign the certificate if all certificate requirements have been met and make the certificate available to the subscriber.

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

The QUCA shall notify Subscribers, either directly or through the RA, that they have created the Subscribers Certificate and provide Subscribers with access to the Certificates by notifying them that their Certificates are available as defined in Appendix-A of the CPS.

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 this CP and the CPS together with 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 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 shall use their Certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of the Subscriber Agreement, this CP, and applicable laws. Subscribers shall protect their Private Keys from access by any other party and shall notify the RA upon the compromise of the private key or any reasonable suspicion of compromise.

Subscribers 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

When using a subscriber's public key and corresponding certificate, a relying party shall adhere to the following obligations:

- Ensure that the key is appropriate for the intended use as set forth in this CP and that such use is consistent with the applicable certificate content including, but not limited to, the key usage, extended key usage and certificate policies extension fields
- Check the status of the certificate against the appropriate and current CRLs or through the OCSP service offered by the QUCA.

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 the QUCA issued certificates to end users.

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

Certificate renewal is supported 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 or any other acceptable mechanisms as defined in the CPS. The request for renewal may originate from the following:

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

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

The QUCA may only process the certificate renewal after confirming the authenticity of such a request. The validation may reuse the original documentation used during first issuance. 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 shall notify 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, the 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 the old certificate.

The new Certificate shall 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, after a revocation, or when the user forgets the password protecting the private key corresponding to the subject certificate.

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

4.7.2 WHO CAN REQUEST A CERTIFICATE RE-KEY

In accordance with the conditions specified in previous section, 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
- A subscriber for his own individual certificate
- An authorized representative for an Organizational certificate.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

Only after verifying re-key request from subscriber or authorized representative; processing of certificate re-keying request shall be initiated.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

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

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Conduct constituting acceptance of a re-keyed certificate is same as listed in section 4.4.1.

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 shall not notify other entities of a re-keyed certificate apart from the requesting party.

4.8 CERTIFICATE MODIFICATION

The QUCA shall not support any other form of Subscriber certificate modification. Modification shall be supported only through revoking existing certificate then either issuing a new certificate or follow 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 CA and/or RA will notify subscribers of certificate revocation using any of the below methods:

- Access to the CRL at 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 shall 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 shall revoke 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 CP or any other applicable Agreements, regulations, or laws;
- The QUCA suspects or determines that revocation of a Certificate is in the best interest of the integrity of Sirar;
- The QUCA determines that a Certificate was not issued correctly in accordance with this CP;
- 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 Certificate is known, or reasonably believed, to be false.
- The subscriber of the Certificate asks for his 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.
- The QUCA shall revoke the certificate of the subscriber, if the subscriber is no longer part of the organization; and
- The Registration Authority's Agreement has been terminated.

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

4.9.2 WHO CAN REQUEST REVOCATION OF A CERTIFICATE

The following entities can request revocation of a certificate:

- NCDC can request the revocation of any certificates issued by any CA participating in the Saudi National PKI;
- Sirar itself may initiate revocation of a certificate in the cases described in section 4.9.1;
- The PKI Committee can request the revocation of any certificates issued under its authority;
- An RA can request the revocation of any of their Subscribers Certificate;
- 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 the revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The QUCA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements.

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

The QUCA shall process authorized revocation requests within a commercially reasonable time.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

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

4.9.7 CRL ISSUANCE FREQUENCY

The QUCA shall issue CRLS within 24 hours after revocation a Subscriber certificate.

4.9.8 MAXIMUM LATENCY OF CRLS

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

4.9.9 ONLINE REVOCATION CHECKING AVAILABILITY

The QUCA shall provide access to an OCSP Responder covering the certificates they issue. The OCSP responses shall conform to RFC 6960 and the OCSP responder's certificate must be signed by the QUCA. 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 shall provide 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 shall not exceed an expiration time of 25 hours.

The QUCA shall require OCSP requests to contain the following data:

- Protocol Version
- Service request
- Target certificate identifier

4.9.11 Other Forms of Revocation Advertisements Available

The QUCA will not provide other forms of revocation advertisements, other than OCSP and CRL.

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

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

4.10.2 Service Availability

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

4.10.3 Optional Features

No stipulation — this section is intentionally left blank.

4.11 END OF SUBSCRIPTION

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. Access to functions critical to registration and certification is limited to personnel in Trusted Roles.

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

5.1.1 SITE LOCATION AND CONSTRUCTION

The location and construction of the facility hosting the 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

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

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

The QUCA equipment shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Any of the 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 shall ensure that the QUCA systems are protected from exposure to water sources

5.1.5 FIRE PREVENTION AND PROTECTION

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

5.1.6 MEDIA STORAGE

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

5.1.7 WASTE DISPOSAL

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

5.1.8 OFF-SITE BACKUP

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

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the QUCA. The following are the trusted roles for Sirar's PKI:

- CA Administrator – general CA administration and approval of the generation, and 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 shall ensure separation of duties for critical CA functions to prevent one person from maliciously using the PKI systems without detection. Each user's system access is limited to those actions for which they are required to perform in fulfilling their responsibilities. Separate individual shall fill each of the roles specified in Sirar's PKI 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 section 5.2.1 of this CP and Sirar's PKI Governance and Operating Model document. Sirar shall ensure that no individual shall be assigned more than one Trusted Role.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE AND CLEARANCE REQUIREMENTS

All persons filling trusted roles shall be selected on the basis of skills, experience, loyalty, trustworthiness, and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the 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 shall be repeated every 3 years for personnel holding trusted roles. All persons filling the Trusted Roles shall only be granted access to the Sirar PKI systems once the background clearance procedures detailed above have been completed and confirmed.

5.3.3 TRAINING REQUIREMENTS

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

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

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

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

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

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

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

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

5.3.7 CONTRACTING PERSONNEL REQUIREMENTS

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

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

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

5.4 AUDIT LOGGING PROCEDURES

Audit log files are generated for all events relating to the security of the 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

Sirar 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 the Sirar 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 OF PROCESSING DATA

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

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

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

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

All log entries include the following elements:

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

5.4.3 RETENTION PERIOD FOR AUDIT LOG

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

5.4.4 PROTECTION OF AUDIT LOG

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

5.4.5 AUDIT LOG BACKUP PROCEDURES

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

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

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

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

Event-causing subject are not notified.

5.4.8 VULNERABILITY ASSESSMENTS

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

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

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

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF EVENTS ARCHIVED

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

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

Sirar 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.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

If STSC detects a potential hacking attempt or other form of compromise to the QUCA, 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.

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

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

5.7.3 CA PRIVATE KEY COMPROMISE RECOVERY PROCEDURES

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

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

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

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

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

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

During a disaster, the primary site shall be physically secured to prevent unauthorized access to the CA facilities.

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

The 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 shall deliver 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 shall be delivered securely using secure standards such as PKCS#12 file format.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Public keys shall be delivered to the QUCA through the use of 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 shall be delivered to the Relying Parties by making it available as set forth in section 2.2.1.

6.1.5 KEY SIZES

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. Key sizes are described as below for 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.

The key lengths of certificates issued by the QUCA are at least 2048-bit RSA, recommended 4096-bit RSA or at least 256-bit ECDSA, recommended 521-bit ECDSA.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The QUCA shall generate 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

Public keys that are bound with Subscribers' certificates shall be certified for use in Digital Signing, as specified by the QUCA. The use of a specific key is determined by the key usage extension in the X.509 certificate.

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 subscribers, timestamping, OCSP Responder and RA private key protection issued by the QUCA shall comply with FIPS-PUB 140-2 "Security Requirements for Cryptographic Modules", Level 2 and above.

6.2.2 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 RA, Subscriber, OCSP Responder, Timestamping Private keys.

6.2.4 PRIVATE KEY BACKUP

The QUCA does not backup RA, Subscriber or OCSP Responder, Timestamping private keys.

6.2.5 PRIVATE KEY ARCHIVAL

The QUCA does not archive the Subscribers' Private Keys.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

The QUCA does not permit RAs, OCSP Responder, Timestamping or subscriber key transfer into and out of cryptographic modules or devices. RAs, OCSP Responder and Subscriber keys that 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 RAs, Timestamping and OCSP Responder and subscriber keys for High Level of Assurance certificates, keys shall be stored in FIPS 140-2 level 2 devices.

6.2.8 METHOD OF ACTIVATING PRIVATE KEYS

Subscriber Private keys shall be 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

Refer to the CPS.

6.2.11 CRYPTOGRAPHIC MODULE RATING

As described in section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVE

The subscriber public key is archived as part of the certificate archive process.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY USAGE PERIODS

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

Key/Certificate	Maximum Validity Period
Subscriber keys	36 months
RA keys	36 months
OCSP Signing Key	36 months
Timestamping signing Key	60 months

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

The activation data used to unlock RA, OCSP responder, Timestamping or 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 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 shall comply with at least Common Criteria EAL2 or an equivalent security profile from other applicable standards.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

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

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

6.6.2 SECURITY MANAGEMENT CONTROLS

The configuration of the QUCA systems as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to software or configuration. A formal configuration management methodology shall be used for installation and on-going maintenance of the system. During initial installation the CA software is checked to ensure that it is the same software that came from the vendor (e.g., by comparing checksums)

6.6.3 LIFE CYCLE SECURITY RATINGS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

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

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

6.8 TIME STAMPING

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

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

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

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 certificate profiles specified in the CPS.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

The 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).

The algorithm identifier of the subject Public Key shall be:

rsaEncryption (OID: = 1.2.840.113549.1.1.1).

7.1.4 NAME FORMS

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

7.1.5 NAME CONSTRAINTS

No Stipulation.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

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

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

No stipulation

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

No stipulation.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION

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

7.2 CRL PROFILE

The CRL Profile for all CRLs issued by the QUCA is as below:

Field	Content	Comment
Version	1 (Version 2)	
Algorithm	SHA256withRSA	
Issuer	CN= STCS QUCA O=STCS C=SA	
This update	*<issue date>*	Date the 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

7.2.1 VERSION NUMBERS

The QUCA shall issue X.509 version two (v2) CRLs (populate version field with integer “1”)

7.2.2 CRL AND CRL ENTRY EXTENSIONS

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

7.3 OCSP PROFILE

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

7.3.1 VERSION NUMBER

The version number for request and OCSP responses shall be v1

7.3.2 OCSP EXTENSIONS

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The PKI Committee shall be responsible for overseeing compliance of the QUCA to the CP and CPS. The PKI Committee shall ensure that the requirements of this CP and CPS 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 this CP and the 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.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The annual audit of the QUCA shall be performed by an external 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 (i.e., external to the Sirar's PKI);
- 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.

An external 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 and not requiring protection may be made publicly available at the discretion of Sirar or the PKI Committee. Specific confidentiality requirements for business information are defined in Sirar's Privacy Policy and the applicable Agreements.

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

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

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

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

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 subscriber's name, and public key will not be deemed private. Sirar's Privacy Policy identifies the personally identifiable information that can be collected to enable issuance of a certificate.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

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

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

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

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL/ADMINISTRATIVE PROCESS

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

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

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

9.5 INTELLECTUAL PROPERTY RIGHTS

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

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

Sirar provides representations and warranties in accordance with this CP and the 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 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 this CP and the relevant CPS and may choose to include additional representations within its CPS or RA agreement.

9.6.3 RELYING PARTIES REPRESENTATIONS AND WARRANTIES

Relying Parties who rely upon the certificates issued under 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 CA/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 this CP and the CPS;
   - Notify the CA/RA in the event that any information in the Certificate is, or becomes, incorrect or inaccurate;
   - Notify the CA/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 CP and the CPS;
   - A Subscriber Certificate being tampered with by the Subscriber; or
   - Inaccuracies or misrepresentations contained within the Application. A Subscriber shall indemnify and hold the CA/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 CP, the CPS 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's. 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 CP shall be effective upon approval by the PKI Committee. The NCDC shall be notified of all changes to this document. Once the CP becomes effective it is published in the repository. Amendments to this CP upon approval become effective and replace the older version in the repository.

9.10.2 TERMINATION

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

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this CP, all 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 CP's Certificate assurance level.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

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

9.12.2 NOTIFICATION MECHANISM AND PERIOD

This CP and any subsequent changes shall be made available to the QUCA participants within two weeks of approval. Sirar reserves the right to amend this CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URL's, and changes to contact information. All 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 CP 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 CP. Dispute Resolution mechanism is described in Sirar's Dispute Resolution Policy.

9.14 GOVERNING LAW

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

9.15 COMPLIANCE WITH APPLICABLE LAW

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

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

No stipulation.

9.16.2 ASSIGNMENT

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

9.16.3 SEVERABILITY

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

9.16.4 ENFORCEMENT (ATTORNEY FEES/WAIVER OF RIGHTS)

This document shall be treated according to laws of Kingdom of Saudi Arabia. Legal disputes arising from the operation of the 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 CP 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 CP shall be deemed to constitute either Sirar, or any of its subcontractors, agents, officers, suppliers, employees, partners, principals, or directors to be a partner, Affiliate, trustee, of any Relying Party or any third party, or to create any fiduciary relationship between Sirar and any Relying party, or any third party, for any purpose whatsoever.

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

9.17.2 ADMINISTRATIVE PROCESSES

Administrative process shall be specified in corresponding agreements and any Sirar Operational policies.