المركز الوطني
للتصديق الرقمي
NATIONAL CENTER FOR DIGITAL CERTIFICATION

SAUDI NATIONAL ROOT-CA

CERTIFICATE POLICY

Document Classification:

Public

Version Number: 3.1

Issue Date: April 16, 2020

Signed by: مشعل محمد عبدالله الشهراني - مدير عام
Signed at: 2020-08-20 05:14:37 +03:00
Reason: أوافق على هذا المستند

Table of Contents

1. INTRODUCTION 8

1.1 Overview 8
1.1.1 Certificate Policy 9
1.1.2 Relationship between the CP and the CPS 9
1.1.3 Interaction with other PKI's 10
1.1.4 Scope 10
1.2 Document Name and Identification 10
1.3 Saudi National PKI Participants 10
1.3.1 NCDC 10
1.3.2 Saudi National Root Certification Authority 11
1.3.3 CA Policy Authority 11
1.3.4 Certification Authority 11
1.3.5 Registration Authority 12
1.3.6 Subscribers 12
1.3.7 Relying Parties 13
1.3.8 Online Certificate Status Protocol Responder 13
1.4 Certificate Usage 13
1.4.1 Appropriate Certificate Uses 13
1.4.2 Prohibited Certificate Uses 13
1.5 Policy Administration 13
1.5.1 Organization Administering the Document 13
1.5.2 Contact Person 14
1.5.3 Person Determining CPS Suitability for the Policy 14
1.5.4 CPS Approval Procedures 14
1.6 Definitions and Acronyms 14

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 15

2.1 Repositories 15
2.1.1 Repository Obligations 15
2.2 Publication of Certification Information 15
2.2.1 Publication of Certificates and Certificate Status 15
2.2.2 Publication of CA Information 15
2.2.3 Interoperability 15
2.3 Time or Frequency of Publication 15
2.4 Access Controls on Repositories 16

3. IDENTIFICATION AND AUTHENTICATION 17

3.1 Naming 17
3.1.1 Types of Names 17
3.1.2 Need for Names to be Meaningful 17
3.1.3 Anonymity or Pseudonymity of Subscribers 17
3.1.4 Rules for Interpreting Various Name Forms 17
3.1.5 Uniqueness of Names 17
3.1.6 Recognition, Authentication and Role of Trademarks 17
3.2 Initial Identity Validation 18
3.2.1 Method to Prove Possession of Private Key 18
3.2.2 Authentication of Organization Identity 18
3.2.3 Authentication of Individual Identity 18
3.2.4 Non-verified Subscriber Information 18
3.2.5 Criteria for Interoperation 18
3.3 Identification and Authentication for Re-key Requests 18
3.3.1 Identification and Authentication for Routine Re-Key 18

3.3.2 Identification and Authentication for Re-key after Revocation 18
3.4 Identification and Authentication for Revocation Request 18

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 19

4.1 Certificate Application 19
4.1.1 Who Can Submit a Certificate Application 19
4.1.2 Enrolment Process and Responsibilities 19
4.2 Certificate Application Processing 19
4.2.1 Performing Identification and Authentication Functions 19
4.2.2 Approval or Rejection of Certificate Applications 19
4.2.3 Time to Process Certificate Applications 19
4.3 Certificate Issuance 19
4.3.1 CA Actions during Certificate Issuance 19
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 20
4.4 Certificate Acceptance 20
4.4.1 Conduct Constituting Certificate Acceptance 20
4.4.2 Publication of the Certificate by the CA 20
4.4.3 Notification of Certificate Issuance by the CA to other Entities 20
4.5 Key Pair and Certificate Usage 20
4.5.1 Subscriber Private Key and Certificate Usage 20
4.5.2 Relying Party Public Key and Certificate Usage 20
4.6 Certificate Renewal 20
4.7 Certificate Re-Key 21
4.7.1 Circumstance for Certificate Re-key 21
4.7.2 Who May Request Certification of a New Public Key 21
4.7.3 Processing Certificate Re-keying Requests 21
4.7.4 Notification of Re-Keyed Certificate Issuance to Subscriber 21
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 21
4.7.6 Publication of the Re-keyed Certificate by the CA 21
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 21
4.8 Certificate Modification 21
4.9 Certificate Revocation and Suspension 22
4.9.1 Circumstances for Revocation 22
4.9.2 Who Can Request Revocation 22
4.9.3 Procedure for Revocation Request 23
4.9.4 Revocation Request Grace Period 23
4.9.5 Time within which CA must Process the Revocation Request 23
4.9.6 Revocation Checking Requirement for Relying Parties 23
4.9.7 CRL Issuance Frequency 23
4.9.8 Maximum Latency of CRLs 23
4.9.9 Online Revocation Checking/Status Availability 23
4.9.10 Online Revocation Checking Requirements 24
4.9.11 Other Forms of Revocation Advertisements Available 24
4.9.12 Special Requirements Related To Key Compromise 24
4.9.13 Circumstances for Suspension 24
4.9.14 Who can Request Suspension 24
4.9.15 Procedure for Suspension Request 24
4.9.16 Limits on Suspension Period 24
4.9.17 Circumstances for Terminating Suspended Certificates 25
4.9.18 Procedure for Terminating the Suspension of a Certificate 25
4.10 Certificate Status Services 25
4.11 End of Subscription 25
4.12 Key Escrow and Recovery 25

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS 26

5.1 Physical Controls 26
5.1.1 Site Location and Construction 26

5.1.2 Physical Access 27
5.1.3 Power and Air Conditioning 27
5.1.4 Water Exposure 27
5.1.5 Fire Prevention and Protection 27
5.1.6 Media Storage 27
5.1.7 Waste Disposal 27
5.1.8 Off-site Backup 28
5.2 Procedural Controls 28
5.2.1 Trusted Roles 28
5.2.2 Number of Persons Required per Task 28
5.2.3 Identification and authentication for Each Role 28
5.2.4 Roles Requiring Separation of Duties 28
5.3 Personnel Controls 28
5.3.1 Background, Qualifications and Experience Requirements 28
5.3.2 Background Check and Clearance Procedures 29
5.3.3 Training Requirements 29
5.3.4 Retraining Frequency and Requirements 29
5.3.5 Job Rotation Frequency and Sequence 29
5.3.6 Sanctions for Unauthorized Actions 29
5.3.7 Independent Contractor Requirements 29
5.3.8 Documentation Supplied to Personnel 30
5.4 Audit Logging Procedures 30
5.4.1 Types of Events Recorded 30
5.4.2 Frequency of Processing Log 31
5.4.3 Retention Period for Audit Log 31
5.4.4 Protection of Audit log 31
5.4.5 Audit Log Backup Procedures 31
5.4.6 Audit Collection System (Internal vs. External) 31
5.4.7 Notification to Event-Causing Subject 31
5.4.8 Vulnerability Assessments 32
5.5 Records Archival 32
5.5.1 Types of Events Archived 32
5.5.2 Retention Period for Archive 32
5.5.3 Protection of Archive 32
5.5.4 Archive Backup Procedures 32
5.5.5 Requirements for Time-Stamping of Records 32
5.5.6 Archive Collection System (Internal or External) 32
5.5.7 Procedures to Obtain and Verify Archive Information 33
5.6 Key Changeover 33
5.7 Compromise and Disaster Recovery 33
5.7.1 Incident and Compromise Handling Procedures 33
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 33
5.7.3 Entity Private Key Compromise Procedures 33
5.7.4 Business Continuity Capabilities after a Disaster 33
5.8 CA or RA Termination 34
5.8.1 CA Termination 34
5.8.2 RA Termination 34

6. TECHNICAL SECURITY CONTROLS 36

6.1 Key Pair Generation and Installation 36
6.1.1 Key Pair Generation 36
6.1.2 Private Key Delivery to Subscriber 36
6.1.3 Public Key Delivery to Certificate Issuer 36
6.1.4 CA Public Key Delivery to Relying Parties 36
6.1.5 Key Sizes 36
6.1.6 Public Key Parameters Generation and Quality Checking 37
6.1.7 Key Usage Purposes 37

6.2 Private Key Protection and Cryptographic-Module Engineering Controls 37
6.2.1 Cryptographic Module Standards and Controls *37*
6.2.2 Private Key Multi-Person Control *37*
6.2.3 Private Key Escrow *37*
6.2.4 Private Key Backup *37*
6.2.5 Private Key Archival *38*
6.2.6 Private Key Transfer into or from a Cryptographic Module *38*
6.2.7 Private Key Storage on Cryptographic Module *38*
6.2.8 Method of Activating Private Key *38*
6.2.9 Methods of Deactivating Private Key *39*
6.2.10 Methods of Destroying Private Key *39*
6.2.11 Cryptographic Module Rating *39*
6.3 Other Aspects of Key Pair Management 39
6.3.1 Public Key Archival *39*
6.3.2 Certificate Operational Periods and Key Pair Usage Periods *39*
6.4 Activation Data 39
6.4.1 Activation Data Generation and Installation *39*
6.4.2 Activation Data Protection *40*
6.4.3 Other Aspects of Activation Data *40*
6.5 Computer Security Controls 40
6.5.1 Specific Computer Security Technical Requirements *40*
6.5.2 Computer Security Rating *40*
6.6 Life Cycle Technical Controls 40
6.6.1 System Development Controls *40*
6.6.2 Security Management Controls *40*
6.6.3 Life Cycle Security Controls *40*
6.7 Network Security Controls 41
6.8 Time Stamping 41

7. CERTIFICATE, CRL, AND OCSP PROFILES **42**

7.1 Certificate Profile 42
7.1.1 Version Numbers *42*
7.1.2 Certificate Extensions *42*
7.1.3 Algorithm Object Identifiers *42*
7.1.4 Name Forms *42*
7.1.5 Name Constraints *42*
7.1.6 Certificate Policy Object Identifier *42*
7.1.7 Usage of Policy Constraints Extension *43*
7.1.8 Policy Qualifiers Syntax and Semantics *43*
7.1.9 Processing Semantics for the Critical Certificate Policies Extension *43*
7.2 CRL Profile 43
7.2.1 Version Numbers *43*
7.2.2 CRL and CRL Entry Extensions *43*
7.3 OCSP Profile 43
7.3.1 Version Numbers *43*
7.3.2 OCSP Extensions *44*

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS **45**

8.1 Frequency or Circumstances of Assessments 45
8.2 Identity and Qualifications of Assessor 45
8.3 Assessor's Relationship to Assessed Entity 45
8.4 Topics Covered By Assessment 45
8.5 Actions Taken As A Result of Deficiency 46
8.6 Communication of Results 46

9. OTHER BUSINESS AND LEGAL MATTERS **47**

9.1 Fees 47

9.1.1 Certificate Issuance or Renewal Fee 47
9.1.2 Certificate Access Fees 47
9.1.3 Revocation or Status Information Access Fee 47
9.1.4 Fees for Other Services 47
9.1.5 Refund Policy 47
9.2 Financial Responsibility 47
9.2.1 Insurance Coverage 47
9.2.2 Other Assets 47
9.2.3 Insurance or warranty Coverage for End-Entities 47
9.3 Confidentiality of Business Information 48
9.3.1 Scope of Confidential Information 48
9.3.2 Information not within the Scope of Confidential Information 48
9.3.3 Responsibility to Protect Confidential Information 48
9.4 Privacy of Personal Information 48
9.4.1 Privacy Plan 48
9.4.2 Information treated as Private 48
9.4.3 Information not deemed Private 48
9.4.4 Responsibility to Protect Private Information 48
9.4.5 Notice and Consent to Use Private Information 49
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 49
9.4.7 Other Information Disclosure Circumstances 49
9.5 Intellectual Property Rights 49
9.6 Representations and Warranties 49
9.6.1 Saudi National Root-CA Representations and Warranties 49
9.6.2 CA Representations and Warranties 50
9.6.3 RA Representations and Warranties 50
9.6.4 Subscriber Representations and Warranties 50
9.6.5 Relying Parties Representations and Warranties 51
9.7 Disclaimers of Warranties 51
9.8 Limitations of Liability 51
9.9 Indemnities 52
9.10 Term and Termination 52
9.10.1 Term 52
9.10.2 Termination 52
9.10.3 Effect of Termination and Survival 53
9.11 Individual Notices and Communications with Participants 53
9.12 Amendments 53
9.12.1 Procedure for Amendment 53
9.12.2 Notification Mechanism and Period 53
9.12.3 Circumstances under which OID must be Changed 53
9.13 Dispute Resolution Provisions 53
9.14 Governing Law 53
9.15 Compliance with Applicable Law 54
9.16 Miscellaneous Provisions 54
9.16.1 Entire Agreement 54
9.16.2 Assignment 54
9.16.3 Severability 54
9.16.4 Enforcement (Attorney Fees and Waiver of Rights) 54
9.16.5 Force Majeure 54
9.17 Other Provisions 54
9.17.1 Fiduciary Relationships 54
9.17.2 Administrative Processes 54

APPENDIX - A: CERTIFICATE TYPES 55

1. EXTENSION DEFINITIONS – ROOT CA CERTIFICATE 56

2. EXTENSION DEFINITIONS – GOVERNMENT CA CERTIFICATE 57

3. EXTENSION DEFINITIONS – BTC LICENSED CA CERTIFICATE 58
4. EXTENSION DEFINITIONS – STCS INTERMEDIARY CA CERTIFICATE.....59

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.

NCDC provides trust services to secure the exchange of information between key stakeholders. Participants include:

- Government
- Citizens
- Business

NCDC owns and operates the Saudi National Root-CA of the Kingdom of Saudi Arabia. Approved Certification Authorities (CAs) shall be issuers of Digital Certificates to Subscribers, Relying parties and Registration Authorities through Certification Service Providers (CSPs) if expressly approved by NCDC. Together all of these components and participants form the “Saudi National PKI”.

NCDC operates as a closed business system model. NCDC Digital Certificates support Authentication, Digital Signature, Encryption and Non-Repudiation services for access and processing of electronic information, documents and transactions. Moreover, this CP shall be used to cross-certify the Saudi National Root-CA with other CAs as per NCDC Cross Certification Policy.

A new service delivery model has been created whereby a shared National PKI Center has been created. The National Center for Digital Certification Shared Services Center (NCDC-SSC) hosts Saudi National Root CA and Government CA and manages operations for the hosted CAs. National Root CA and Government CA are segregated through physical and logical controls. Commercial CAs under the Saudi National Root CA are hosted outside NCDC-SSC and managing their operations.

This CP shall define the policies by which the Saudi National Root-CA operates. This CP complies with the Saudi National PKI Policy and in line with Internet Request for Comment (RFC) 3647 [RFC 3647]. The terms used in this document shall have the meanings as defined in NCDC Glossary section which can be found at https://www.ncdc.gov.sa.

Saudi National Root-CA conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at https://www.cabforum.org. In the event of any inconsistency between this document and those requirements, those requirements take precedence over this document.

1.1 OVERVIEW

This CP defines level of trust and assurance for use by all Saudi National PKI participants.

Assurance level is defined as the:

- Strength of the binding between a Public Key and the individual whose Subject name is cited in the Certificate,
- Mechanisms used to control the use of the Private Key,
- Security provided by the PKI itself.

This CP defines high assurance level for use by Saudi National Root-CA participants which include NCDC approved CAs and supportive functions for the Saudi National Root-CA operations. This includes:

- A stringent Identity proofing process through Registration Authority before issuance of certificate,
- The Digital Certificates issued to Subscribers (CAs or Saudi National Root-CA supporting functions) are on hardware,

The assurance level Certificates defined in this CP apply to the following entities:

- Relying Parties (RPs) who are permitted to rely upon Digital Certificates meeting NCDC standards for purposes set forth by this CP,
- Other authorities (e.g., Subordinate CAs expressly approved by NCDC, Registration Authorities (RAs) or OCSP Responders) certified or used by the CSP operated by the Issuer.

This CP has been developed under the direction of NCDC and has the responsibility for directing the development, approval and update of the Saudi National Root-CA CP.

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

As described in this CP, PDS and supporting Certification Practice Statement (CPS), NCDC will establish a self-signed off-line Root CA.

It is the responsibility of all parties applying for or using a Digital Certificate issued under this CP, to read the Saudi National Root-CA CP and to understand the practices established for the lifecycle management of the Certificates. Any application for Digital Certificates or reliance on OCSP validation of NCDC issued Certificates signifies understanding and acceptance of this CP and its supporting policy documents.

1.1.1 CERTIFICATE POLICY

X.509 certificates will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party to decide whether a Certificate is trusted for a particular purpose. Certificates issued by the Saudi National Root-CA will identify the applicable policy in the certificate policies extension by including applicable OID(s).

1.1.2 RELATIONSHIP BETWEEN THE CP AND THE CPS

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

1.1.3 INTERACTION WITH OTHER PKI'S

NCDC will decide on issues related to cross-certification with other Certification Authorities as per NCDC Cross Certification Policy.

1.1.4 SCOPE

This CP applies to all certificates issued by the Saudi National Root-CA. The Saudi National Root-CA shall issues certificates and Certificate Revocation Lists (CRLs) only to NCDC approved CAs and supportive functions for the Saudi National Root-CA operations within Saudi National PKI. The Saudi National Root-CA also cross-certifies with CAs at international level as per NCDC Cross Certification Policy.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the Saudi National Root-CA Certificate Policy (CP), and is identified by the object identifier (OID): 2.16.682.1.101.5000.1.2.1.1

NCDC will also issue OIDs to the approved CAs. The approved CAs (Level-One CAs) will then choose to assign OIDs for different purposes under this scheme. Please refer to the latest OID Allocation document available on https://www.ncdc.gov.sa.

1.3 SAUDI NATIONAL PKI PARTICIPANTS

The following are roles relevant to the administration and operation of the Saudi National Root-CA.

1.3.1 NCDC

NCDC approves and maintains the practices, policies and procedures under which the entire Saudi National PKI operates. NCDC is also responsible for the governance and enforcement of the policies. Regarding the CP, NCDC approves the Saudi National Root-CA Certificate Policy (CP), PKI Disclosure Statement (PDS) and Certification Practice Statement (CPS), including their revisions.

NCDC is responsible for establishing and administering the requirements and procedures for entities wishing to become a Certification Service Provider (CSP) within the Saudi National PKI. CITC license is required for commercial, non-governmental CSPs.

NCDC tasks include:

- Establishment and maintenance of the Saudi National Root-CA CP,
- Review and approval of the Saudi National Root-CA CPS as being in conformance with this CP,
- Review and approval of the Saudi National Root-CA PDS as being in conformance with this CP,
- Ensuring the operation of the Saudi National Root-CA comply with the requirements of the Saudi National Root-CA CP, CPS and the NCDC Operations Policies and Procedures,
- Decision on the admittance of new CAs,
- Decision on the admittance of new CSPs,

- Establish and approve Cross-Certification criteria and entities, and
- Arbitration on all claims or disputes between all Saudi National PKI participants as per the NCDC Dispute Resolution Policy.

1.3.2 SAUDI NATIONAL ROOT CERTIFICATION AUTHORITY

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

- Generation and issuance of cross certified CA certificates,
- Publication of cross certified CA Certificates,
- Revocation of cross certified CA Certificates,
- Re-key of the Saudi National Root-CA and NCDC approved CAs signing keys,
- Establishment and maintenance of the CPS in accordance with the Saudi National Root-CA CP,
- Performance of all aspects of the services, operations and infrastructure related to Certificates issued under this CP, in accordance with the requirements, representations, and warranties of the Saudi National Root-CA CP and CPS, and
- Issuance of certificates to approved entities wishing to cross certify with the Saudi National PKI as per NCDC Cross Certification Policy.

1.3.3 CA POLICY AUTHORITY

The CA Policy Authority (PA) is responsible for the governance of CA. CA Policy Authority members are appointed by NCDC. Its tasks include:

- Ensuring the operation of the CA comply with the requirements of the Saudi National PKI Policy, CA CP,PDS, CPS and relevant Operations Policies and Procedures,
- Customize the Subscriber Agreement, Relying Party Agreement and Registration Authority based on the CA's specific business requirements,
- Seeking resolution of disputes between participants operating in its domain,
- Establishing and implement their own CP, PDS and CPS in conjunction with the Saudi National PKI Policy, and
- Act as liaison with NCDC.

1.3.4 CERTIFICATION AUTHORITY

The term CA refers to any entity approved by NCDC to join the Saudi National PKI, directly under the Saudi National Root-CA. On successfully joining the Saudi National PKI ; CA is entitle to issue certificates after mapping to one of the policy OIDs listed in the NCDC OID Allocation document, which can be found at https://www.ncdc.gov.sa. CAs will issue subscriber certificates, OCSP responder certificates and other certificates required by PKI components. CAs, acting on behalf of CSPs, will issue certificates to Subscribers in accordance with their CSP Agreement, Subscriber Agreement, Relying party Agreement, their respective CP/CPS, and the Saudi National PKI Policy. The CAs will describe which subscriber types they will support, which certificate types they will issue and determine the level of warranties and liabilities.

A CA is responsible for:

- Control over the designation of RAs,
- Control over the designation of CSPs,
- The Certificate generation process,
- Publication of Subscriber Certificates,
- Revocation of Subscriber Certificates,
- Publication of revocation information,
- Re-key of Subscribers,
- Conduct regular internal security audits,
- Conduct compliance reviews of its CSPs,
- Assist in audits conducted by or on behalf of NCDC, and
- Performance of all aspects of the services, operations and infrastructure related to the respective CA.

1.3.5 REGISTRATION AUTHORITY

Saudi National Root-CA may, subject to the approval of NCDC, designate specific RAs to perform the Subscriber Identification and Authentication and Certificate request and revocation functions defined in the Saudi National Root-CA CP and related documents.

RA is obligated to perform certain functions pursuant to an RA Agreement including the following:

- Process Certificate application requests in accordance with the Saudi National Root-CA CP and applicable RA Agreement, and other policies and procedures with regard to the Certificates issued,
- Maintain and process all supporting documentation related to the Certificate application process,
- Process Certificate Revocation requests in accordance with this CP, applicable RA Agreement, and other relevant operational policies and procedures with respect to the Certificates issued. Without limitation to the generality of the foregoing, the RA shall request the revocation of any Certificate that it has approved for issuance according to the conditions described later in section 4.9.1,
- Comply with the provisions of its RA Agreement and the provisions of the Saudi National Root-CA CP including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements, and
- Follow Privacy policy in accordance with the Saudi National Root-CA CP and applicable RA Agreement.

1.3.6 SUBSCRIBERS

Subscribers are individuals (end users), entities (organizations) or devices to whom certificates are issued.

The subscribers of Saudi National Root-CA would be the approved CAs by NCDC. However, the subscribers and relying parties who use the certificates issued by approved CA under

Saudi National PKI need to be assured that the CA is licensed by the Saudi National Root-CA.

1.3.7 RELYING PARTIES

A Relying Party is any entity that places comfort on information provided by Certificate Service Providers regarding a specific electronic transaction that the Relying Party uses to accept or reject its participation in the transaction.

The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.8 ONLINE CERTIFICATE STATUS PROTOCOL RESPONDER

Online Certificate Status Protocol (OCSP) Responders and Simple Certificate Validation Protocol (SCVP) status providers may provide revocation status information or full certification path validation services respectively. The Saudi National Root-CA may make their certificate status information available through an OCSP responder in addition to any other mechanisms they wish to employ. The Saudi National Root-CA shall publish status information for the certificates it issues in a Certificate Revocation List (CRL).

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The use of Certificates supported by the Saudi National PKI is restricted to parties authorized by contract to do so. Entities and persons other than those authorized by contract may not use certificates for any purpose.

The Saudi National Root-CA shall issue certificates and Certificate Revocation Lists (CRLs) only to NCDC approved CAs under Saudi National Root-CA, cross certified CAs outside Saudi Arabia and certificates required by the PKI components and supportive functions for the Saudi National Root-CA operations within Saudi National PKI.

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 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 the Saudi National Root-CA 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 NCDC (see Section 1.3.1).

1.5.2 CONTACT PERSON

Queries regarding the Saudi National Root-CA CP shall be directed at:

Email: info@ncdc.gov.sa

Telephone: +966 11 4522197

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

NCDC is responsible for approving the Saudi National Root-CA CPS and establishing that the Saudi National Root-CA conforms to the requirements of this CP in accordance with NCDC policies and procedures.

1.5.4 CPS APPROVAL PROCEDURES

Changes or updates to the Saudi National Root-CA CPS 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 NCDC approval.

1.6 DEFINITIONS AND ACRONYMS

The terms and acronyms used in this document shall have the meanings as defined in NCDC Glossary section which can be found at https://www.ncdc.gov.sa.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The NCDC shall operate Repositories to support the Saudi National Root-CA operations. The repositories shall be directories that provide access through an appropriate standard-based access protocol.

2.1.1 REPOSITORY OBLIGATIONS

Repositories shall support:

- An appropriate standard-based access protocol,
- Availability of the information as required by the certificate information posting and retrieval stipulations of the Saudi National Root-CA CP , and
- Access control mechanisms, when necessary to protect the repository availability and information as described in later sections.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

The Saudi National Root-CA shall publish in the appropriate repository, the Saudi National Root-CA Certificate, cross certified CA certificates, supportive functions certificates and CRLs as described under same section in the CPS.

2.2.2 PUBLICATION OF CA INFORMATION

This CP shall be made available to all Saudi National PKI participants at NCDC website https://www.ncdc.gov.sa. This web site is the only source for up-to-date documentation and NCDC reserves the right to publish newer versions of the documentation without prior notice.

Additionally, Saudi National Root-CA shall publish an approved, current and digitally signed version of the Saudi National Root-CA CP , CPS and its PDS.

NCDC Public LDAP directory and NCDC website (https://www.ncdc.gov.sa) are the only authoritative sources for:

- All publicly accessible certificates issued by Saudi National Root-CA; and
- The certificate revocation list (CRL) for Saudi National Root-CA.

2.2.3 INTEROPERABILITY

Repositories used to publish CA certificates and CRLs, shall employ standard-based scheme for directory objects and attributes, at least LDAPv3.

2.3 TIME OR FREQUENCY OF PUBLICATION

Saudi National Root-CA shall publish certificate promptly following their generation and issuance. CRL information shall be published as set in section 4.9.7.

This CP and any subsequent changes should be made available to the Saudi National PKI participants as set forth in section 2.2.2 within two weeks of approval by NCDC.

2.4 ACCESS CONTROLS ON REPOSITORIES

Certificates and certificate status information in the repository shall be made available to Saudi National PKI participants and other parties on a 24X7 basis as determined by the applicable agreements and NCDC Privacy Policy, and subject to routine maintenance.

The Saudi National Root-CA will protect repository information not intended for public dissemination or modification through the use of strong authentication, access controls, and an overall Information Security Management System that prevents unauthorized access to information.

The controls employed by NCDC 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.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

Each CA certificate must have a unique and readily identifiable Distinguished Name (DN) according to the X.500 standard. Naming conventions for CAs are approved by the Saudi National Root-CA.

Details of these are found in the Certificate Types under Appendix-A in this CP.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The CAs certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates are understood and used by Relying Parties. Names used in the certificates must identify the CA in a meaningful way to which they are assigned.

The subject name contained in a CA certificate must be meaningful in the sense that the Saudi National Root-CA is provided with proper evidence of the association existing between the name and the entity to which it belongs.

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

OU=Saudi National Root CA, O=National Center for Digital Certification, C=SA

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

Saudi National Root-CA does not support issuing anonymous certificates.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

The naming convention used by the Saudi National Root-CA is ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.5 UNIQUENESS OF NAMES

All distinguished names shall be unique across the Saudi National Root-CA.

3.1.6 RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

Where permitted or required, the use of a trademark is reserved to the holder of that trademark.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

The Certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the certificate. The method to prove possession of a private key shall be established by NCDC.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

Applicants wishing to join or cross certify with the Saudi National PKI are authenticated in accordance with NCDC specifications as described in NCDC Cross Certification Policy and Saudi National PKI Policy.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

The Saudi National Root-CA does not issue end-entity certificates.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Non-verified information shall not be included in certificates issued by Saudi National Root-CA.

3.2.5 CRITERIA FOR INTEROPERATION

Any CA wishing to cross certify with the Saudi National Root-CA, shall adhere to the following requirements:

- Issue Certificates compliant with the Certificate profile described later in this CP,
- Make Certificate information and CRL available within the Saudi National PKI community in accordance with the Saudi National Root-CA CP, and
- Provide an accessible directory that interoperates with the NCDC Repository defined forth in this CP.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

An authorized representative should request re-key of CA, in compliance with the Saudi National Root-CA Operations Policy.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

If a CA certificate is revoked, an authorized representative of the CA shall provide sufficient information before Saudi National Root-CA initiates generation of the new CA certificate.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests shall be authenticated to verify that the revocation has been requested by an authorized entity. 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 NCDC.

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

For CA licensing process, an application must be submitted and approved by NCDC. In addition, for commercial CAs, a license must be obtained from CITC after an application is approved by NCDC.

Entities wishing to cross certify with the Saudi National PKI apply to NCDC and receive approval before the Saudi National Root-CA proceeds with exchanging certificates.

4.1.2 ENROLMENT PROCESS AND RESPONSIBILITIES

All applicants shall agree to the terms and conditions of the applicable Agreements which may include, but are not limited to, Subscriber Agreement, CSP Agreement, Relying Party or RA Agreement.

NCDC shall set up enrolment process for the certificates issued under the Saudi National Root-CA.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The identity-proofing of the CA and cross certifying entity shall meet the requirements specified in Saudi National PKI Policy and NCDC Cross Certification Policy.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

NCDC may accept or reject a Certificate application of the CA or cross certifying entity as described in the CA Licensing Process.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

The time to process certificate applications is specified in the relevant Agreement between the PKI participants.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

The Saudi National Root-CA Certificate has been self-generated and self-signed. When the Saudi National Root-CA receives a request for a CA Certificate or an entity wishing to cross certify with the Saudi National PKI, the Saudi National Root-CA does not issue a Certificate before the applicant accepts the terms of an Agreement (for CAs), agrees to adapt to the Saudi National PKI Policy, successfully completes the CA or Cross Certifying Entity

application form, obtains the required license from the CITC (for commercial CAs), and gets final approval from NCDC.

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

Saudi National Root-CA must notify the CA Applicant of Certificate issuance using secure mechanisms as defined in Saudi National Root-CA Operations Policy.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Certificate acceptance is governed by the Agreements set out between the Saudi National Root-CA and CA's. The use of a Certificate or the reliance upon a Certificate signifies acceptance by the CA of the terms and conditions of the Saudi National Root-CA CP by which they irrevocably agree to be bound.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

Once Saudi National Root-CA accepts and generates CA certificate it shall be published in the appropriate repository.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

NCDC and CA PA shall be informed when a CA has been cross certified with the Saudi National Root-CA.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

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

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Relying parties shall use public key certificates and associated public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates. The Relying Party is solely responsible for deciding whether or not to rely on the information in a certificate provided to accept or reject their participation in the transaction.

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.

The Saudi National Root-CA CP does not support certificate renewal.

4.7 CERTIFICATE RE-KEY

Re-keying (key update) a certificate consists of creating new certificates with a different Key pair while retaining other Subject information from old certificate.

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

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

Certificate re-key shall take place after a certificate is revoked and the subscriber information is still accountable or after a certificate has expired or nearing expiry.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

In accordance with the conditions specified in section 4.7.1, an authorized representative of the CA may request re-key of its CA certificate.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

Only after verifying re-key request from authorized representative of CA, processing of certificate re-keying request shall be initiated.

4.7.4 NOTIFICATION OF RE-KEYED CERTIFICATE ISSUANCE TO SUBSCRIBER

Notification of issuance of a re-keyed certificate to the Subscriber shall be using secure mechanisms as defined in Saudi National Root-CA Operations Policy.

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

After successful completion of the re-key process, certificate shall be published in appropriate repositories.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Generally, Saudi National Root-CA does not notify other entities of a re-keyed certificate apart from requesting CA.

4.8 CERTIFICATE MODIFICATION

Certificate modification for all applicants will be accomplished through Certificate re-key as specified in section 4.7.

The Saudi National Root-CA CP does not support other forms of Certificate modification.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

A Certificate shall be revoked/ suspended when the binding between the Subject and the Subject's Public Key defined within a Certificate is no longer considered valid.

4.9.1 CIRCUMSTANCES FOR REVOCATION

The Saudi National Root-CA shall maintain controls to provide reasonable assurance that Subordinate CA Certificate is revoked within 7 days; whenever:

- Failed to comply with the terms and conditions subject to which the licence was granted;
- Contravened any provisions of the Electronic Transactions (e-Transactions) Act and Bylaws made there under;
- The Subject has failed to meet its obligations under its agreements with the Saudi National Root-CA, those of any applicable CP,PDS and CPS or any other applicable Agreements;
- NCDC suspects or determines that revocation of a Certificate is in the best interest of the integrity of the NCDC;
- The Subordinate CA requests revocation in writing;
- The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6,
- The Issuing CA obtains evidence that the Certificate was misused;
- The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with these 4.9.1.2, 6.1.5, 6.1.6 Baseline Requirements or the applicable Certificate Policy or Certification Practice Statement;
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
- Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on a CRL and specified as revoked by an OCSP Responder. The Saudi National Root-CA publishes a revocation notice on its Web Site if any issuing CA certificate is revoked.

4.9.2 WHO CAN REQUEST REVOCATION

The following entities can request revocation of a Certificate:

- NCDC can request the revocation of any certificates issued by any CA participating in the Saudi National PKI;
- The authorized signatory of the CA; or
- A legal, judicial or regulatory agency in Saudi Arabia.

The authority to revoke the Saudi National Root-CA certificate rests with NCDC.

If any request for revocation cannot be resolved, the request is subject to the Dispute Resolution process described in the NCDC Dispute Resolution Policy.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

A request to revoke certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The Saudi National Root-CA 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

The Saudi National Root-CA shall maintain controls to provide reasonable assurance that the revocation process for the Subordinate CA Certificate be completed within 7 days.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

Authorized Certificate revocation should be processed within 24 hours.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

Relying Parties should comply with the signature validation requirements defined in the Relying Party Agreement.

4.9.7 CRL ISSUANCE FREQUENCY

The Saudi National Root-CA will publish its CRL no less frequently than once every twelve months and at the time of any Certificate revocation of certificate issued by it.

4.9.8 MAXIMUM LATENCY OF CRLS

CRLs shall be published in the Repositories within 10 minutes of Certificate revocation. Certificate status information is updated within 30 minutes of certificate revocation.

4.9.9 ONLINE REVOCATION CHECKING/STATUS AVAILABILITY

Saudi National Root-CA may provide access to an OCSP Responder covering the certificates it issues.

4.9.10 ONLINE REVOCATION CHECKING REQUIREMENTS

The Saudi National Root-CA may make its Certificate status information available through an OCSP responder. OCSP requests and responses comply with the profiles specified later in this CP.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

No stipulation.

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

If NCDC discovers, or has a reason to believe, that there has been a compromise of the private key of the Saudi National Root-CA or any other approved CA, NCDC will immediately declare a disaster and invoke NCDC business continuity plan. NCDC will (1) determine the scope of certificates that must be revoked, (2) publish a new CRL at the earliest feasible time, (3) use reasonable efforts to notify CSPs, subscribers and potential relying parties that there has been a key compromise, and (4) generate new CA key pair as per NCDC operations policies and procedures.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

The Saudi National Root-CA has the option to suspend certificates under the circumstances described in section 4.9.1.

4.9.14 WHO CAN REQUEST SUSPENSION

The following entities can request suspension of a Certificate:

- NCDC can request the suspension of any certificates issued by any CA participating in the Saudi National PKI;
- The authorized signatory of the CA; or
- A legal, judicial or regulatory agency in Saudi Arabia.

If any request for suspension cannot be resolved, the request is subject to the Dispute Resolution process described in the Dispute Resolution Policy.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

A request to suspend a certificate shall identify the certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated (e.g., digitally or manually signed). The Saudi National Root-CA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements.

4.9.16 LIMITS ON SUSPENSION PERIOD

The maximum period for which a certificate can be suspended will be defined by the Policy Authority but shall not exceed ninety (90) days.

4.9.17 CIRCUMSTANCES FOR TERMINATING SUSPENDED CERTIFICATES

A suspended certificate is reactivated when the entity which requested the suspension of a certificate is satisfied that the circumstances leading to the suspension are no longer valid. Once reactivated, the certificate will be valid for the remainder of its initial life time.

A suspended certificate is revoked when the entity which requested the suspension of a certificate is satisfied that the circumstances leading to the suspension are indeed valid.

When the period for suspension has reached its maximum duration without resolution, the certificate will be revoked.

4.9.18 PROCEDURE FOR TERMINATING THE SUSPENSION OF A CERTIFICATE

A request to unsuspend a certificate shall identify the certificate to be unsuspended, explain the reason for unsuspension, and allow the request to be authenticated (e.g., digitally or manually signed). The CA or RA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements.

4.10 CERTIFICATE STATUS SERVICES

The status of public certificates is available from CRL's in the repositories and via an OCSP responder, if supported.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW AND RECOVERY

No keys shall be escrowed for the Saudi National Root-CA and Level-One CAs under Saudi National Root CA..

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

The Saudi National Root-CA is collocated in the NCDC-SSC and follows the physical security requirements specified as below:

The NCDC-SSC systems are protected by seven 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 CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of two factor biometric authentication. Unescorted personnel, including un-trusted employees or visitors, are not allowed into such secured areas.

The NCDC has implemented policies and procedures to ensure that the physical environments in which the CA systems are installed maintain a high level of security:

- NCDC-SSC systems are installed in a secure facility that is isolated from outside networks, with all access controlled;
- The NCDC-SSC is separated into a series of progressively secure areas; and
- The entrances and exits from the secure areas are under constant video surveillance and all systems that provide authentication, as well as those that record entry, exit and network activity, are in secured areas.

The security techniques employed are designed to resist a large number and combination of different forms of attack. The mechanisms the NCDC-SSC uses include:

- Perimeter alarms;
- Closed circuit television;
- Two-factor authentication using Biometrics and dual mechanical rotary locks;
- Mantraps;
- Radio frequency attenuation shielding and reinforced walls;
- Motion detectors;
- Human guards; and
- All the Networking and systems components including the certification components are installed in secure Data cabinets with pin locks from both sides.

To prevent tampering, cryptographic hardware is stored in a most secure area of the NCDC-SSC, with access limited to authorized personnel.

The NCDC uses human guards to continually monitor the facility housing the CA equipment on a 7x24x365 basis. The NCDC-SSC facility is never left unattended.

5.1.1 SITE LOCATION AND CONSTRUCTION

The location and construction of the facility housing the Saudi National Root-CA and other CAs, the NCDC-SSC, 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, provide robust protection against unauthorized access to the Saudi National Root-CA equipment and records.

5.1.2 PHYSICAL ACCESS

The CA equipment shall always be protected from unauthorized access. The physical security mechanisms for Saudi National Root-CA at a minimum shall be in place to:

- Permit no unauthorized access to the hardware;
- Store all removable media and paper containing sensitive plain-text information in secure containers;
- Monitor, either manually or electronically, for unauthorized intrusion at all times, and
- Maintain and periodically inspect an access log.

A security check of the facility housing the CAs equipment shall be on a regular basis. The NCDC-SSC facility shall never leave unattended.

5.1.3 POWER AND AIR CONDITIONING

The CAs 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 CA on-line servers (e.g., CAs hosting directories) shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power, to support a smooth shutdown of the CA operations.

5.1.4 WATER EXPOSURE

The Saudi National Root-CA shall ensure that CA equipment is installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

5.1.5 FIRE PREVENTION AND PROTECTION

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

5.1.6 MEDIA STORAGE

Saudi National Root-CA shall ensure that CA media is stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive, or backup information is duplicated and stored in a location separate from the primary site.

5.1.7 WASTE DISPOSAL

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

5.1.8 OFF-SITE BACKUP

Full system backups of CAs, sufficient to recover from system failure, shall be made on a periodic schedule as described in the NCDC 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 NCDC. The following are the trusted roles for a CA:

- CA Master
- CA Officer
- CA Administrator
- CA Operator
- CA Auditor

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

The NCDC-SSC 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 individuals shall fill each of the roles specified in NCDC Trusted Roles 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 Saudi National Root-CA certificate signing Private Key. Activation of the Saudi National Root-CA certificate signing Private Key shall require actions by at least two individuals.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

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

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

The Saudi National Root-CA will ensure that no individual shall be assigned more than one Trusted Role.

5.3 PERSONNEL CONTROLS

5.3.1 BACKGROUND, QUALIFICATIONS AND EXPERIENCE REQUIREMENTS

All persons filling trusted roles are selected on the basis of skills, experience, loyalty, trustworthiness, and integrity. CA Master trusted roles must be held by citizens of the

Kingdom of Saudi Arabia. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA are set forth in the NCDC Trusted Roles document and NCDC Organization Structure document. While performing any critical operation one of the trusted roles should be held by the Saudi citizen.

5.3.2 BACKGROUND CHECK AND CLEARANCE PROCEDURES

NCDC conducts background investigations for all NCDC personnel including trusted roles and management positions. Background check shall take into account the following:

- Availability of satisfactory character reference, i.e. one business and one personal;
- A check (for completeness and accuracy) of the applicant's CV;
- Confirmation of claimed academic and professional qualifications;
- Independent identity check (National ID card, Passport or similar document);
- Interviews with references shall be done as required; and
- More detailed checks, such as security clearance.

Security clearance shall be repeated every 3 years for personnel holding trusted roles.

5.3.3 TRAINING REQUIREMENTS

The Saudi National Root-CA shall ensure that all personnel receive appropriate training. Such training shall address relevant topics such as security requirements, operational responsibilities and associated procedures.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

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

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

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

The Saudi National Root-CA shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions (i.e., not permitted by the Saudi National Root-CA CP, CPS, NCDC Policies and Operational Procedures) involving the CA or its repository.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

Contractor personnel employed to perform functions pertaining to the CA shall be subject to the same sanctions as other personnel as set forth in Section 5.3.6.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

Saudi National Root-CA will make available to its personnel its CP, CPS, and any relevant documents required to perform their jobs.

5.4 AUDIT LOGGING PROCEDURES

Audit log files are generated for all events relating to the security of the Saudi National Root-CA and its RA. The security audit logs for each auditable event defined in this section are maintained in accordance with onsite retention period and for archive.

5.4.1 TYPES OF EVENTS RECORDED

The Saudi National Root-CA shall ensure recording of all events in audit log files relating to the security of the CA system hosted in NCDC-SSC, including but not limited to, routers, firewalls, directories and servers hosting CA, RA and other software. 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. CA and Subscriber 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 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 and OCSP entries.
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 CA facility.

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, as defined in the CPS;
- CA personnel changes;
- Discrepancy and 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 LOG

Audit logs are required to be processed in accordance with the NCDC Audit and Compliance Policy.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

The Saudi National Root-CA shall retain all system generated (electronic) and manual audit records onsite for a period not less than six months from the date of creation.

5.4.4 PROTECTION OF AUDIT LOG

The Saudi National Root-CA 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

Saudi National Root-CA shall back up all audit logs and audit summaries.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

The audit collection system is detailed in the NCDC Audit and Compliance Policy.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

Event-causing subject are not notified.

5.4.8 VULNERABILITY ASSESSMENTS

Routine vulnerability assessments of security controls shall be performed by the Saudi National Root-CA. The security program must 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.

Based on the Risk Assessment exercise, NCDC 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

Saudi National Root-CA archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA. The CA shall make these audit logs available to its Qualified Auditor upon request.

5.5.2 RETENTION PERIOD FOR ARCHIVE

The minimum retention periods for archive data shall be established in accordance with applicable regulatory guidance, laws, Agreements, and as specified by NCDC.

NCDC has established minimum retention period for archive data at ten years.

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, CA PA, or as required by law. Records and material information relevant to use of, and reliance on, a certificate shall be archived. Archive media shall be stored in a secure storage facility separate from the component itself. Any secondary site must provide equivalent protection and access controls as the primary site.

5.5.4 ARCHIVE BACKUP PROCEDURES

As specified in the NCDC Backup Policies and Procedures.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Certificates, CRLs, and other revocation database entries shall contain time and date information obtained from the Time Server.

Also all the System logs shall be time stamped.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

As specified in NCDC Archival Policy.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

As specified in NCDC Archival Policy.

5.6 KEY CHANGEOVER

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

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

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

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

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

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

As specified in the Saudi National Root-CA Operations Policy.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

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

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

NCDC Business Continuity Management System (BCMS) demonstrates the capability to restore or recover critical PKI services at the primary site within twenty four (24) hours in the event of service(s) non-availability.

Business Continuity Management components at NCDC are being regularly tested, verified, and updated to be operational to address crisis situation in the event of a disruption. For security reasons details of these plans are not publicly available.

NCDC business continuity plan includes:

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

NCDC has developed recovery plans to mitigate the effects of any kind of natural, man-made or equipment failure related disaster.

NCDC has implemented an alternate recovery site as per industry standards to provide full recovery of critical PKI services within five days following a disaster at the primary site. NCDC Business Continuity Policy contains further details.

5.8 CA OR RA TERMINATION

5.8.1 CA TERMINATION

If any CA terminates operation for convenience, contract expiration, re-organization, or other non-security related reason, the Agreement between the Saudi National Root-CA and the CA shall set forth what actions are to be taken to ensure continued support for certificates previously issued by the CA. At a minimum, such actions shall include preservation of the CA information archive described in the Saudi National Root-CA CP and CPS. NCDC will be the custodian of CA archival records in case of termination.

5.8.2 RA TERMINATION

Upon termination of the RA Agreement, the RA certificate shall be revoked and the tasks performed by the RA must be handled by another RA.

NCDC will be the custodian of RA archival records in case of termination.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

Saudi National Root-CA Key generation procedures shall be documented.

Saudi National Root-CA Key pair generation shall be witnessed and attested by a party separate from the CA trusted roles as mentioned in NCDC Root-CA Key Generation Ceremony Policy.

Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. Saudi National Root-CA shall use Hardware Security Modules (HSMs) for CA key generation and storage. The Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the CA keys.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

No end-subscriber certificates are issued from the Saudi National Root-CA except for the supportive operational roles.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Applicant public keys must be delivered for certificate issuance using industry standard secure protocol.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The Saudi National Root-CA and other CAs will ensure that their Subscribers and Relying Parties receive and maintain the trust anchor in a trustworthy fashion. Methods for trust anchor delivery may include:

- A trusted role loading the trust anchor onto Tokens delivered to Subscribers via secure mechanisms,
- Distribution of trust anchor through secure out-of-band mechanisms,
- Calculation and comparison of trust anchor hash or fingerprint against the hash made available via authenticated out-of-band sources, or
- Downloading trust anchor from web sites secured with a currently valid certificate of equal or greater assurance level than the Certificate being downloaded and the site trust anchor already on the Subscriber system via secure means.

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 in section 6.3.2. All FIPS-approved signature algorithms shall be

considered acceptable. If NCDC determines that the security of a particular algorithm may be compromised, it may propose schedule for transition to the other stronger algorithms.

All certificates issued shall use at least 2048 bit RSA, with Secure Hash Algorithm version (SHA-256), Elliptical Curve Digital Signature Algorithm (ECDSA), or RSA digital signature in accordance with FIPS 186-2 or equivalent.

TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall use triple-DES or AES (minimum 128 bit key strength) for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

Public key parameters prescribed shall be generated in accordance with industry best practices. RSA keys shall be generated according to ANSI X9.31 and primality testing of prime numbers shall be done according to ANSI X9.80 standards. However no end-subscriber certificates are issued from the Saudi National Root-CA.

6.1.7 KEY USAGE PURPOSES

Public keys that are bound into certificates shall be certified for use in authenticating, signing or encrypting, but not all, except as specified by the issuing CA. The use of a specific key is determined by the key usage extension in the X.509 certificate.

Saudi National Root-CA and other CAs keys are used for certificate signing and CRL signing.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC-MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

Cryptographic modules employed in the NCDC shall comply with FIPS-PUB 140-2 “Security Requirements for Cryptographic Modules”.

6.2.2 PRIVATE KEY MULTI-PERSON CONTROL

Using of Saudi National Root-CA Private signing key shall require action by multiple persons as described in same section of Saudi National Root-CA CPS and Saudi National Root-CA Operations Policy.

6.2.3 PRIVATE KEY ESCROW

Saudi National Root-CA shall not escrow CA private keys.

6.2.4 PRIVATE KEY BACKUP

Saudi National Root-CA signing Private Key shall be backed up under the same multi-person control as the original Signing Key. A single copy of the signing key may be stored at the CA location. A second copy may be kept at the CA backup location identified as business continuity location. A third copy may be kept at the CA backup location identified as

disaster recovery location. Procedures for Saudi National Root-CA signing Private Key backup shall be detailed in the Saudi National Root-CA Backup and Restore Policy.

Saudi National Root-CA private keys that are physically transported from one facility to another shall remain confidential and maintain their integrity.

Saudi National Root-CA hardware containing CA private keys, and associated activation materials, shall be transported in a physically secure environment by authorized personnel in trusted roles, using multiple person controls, and using sealed tamper evident packaging.

Saudi National Root-CA keys and associated activation materials shall be transported in a manner that prevents the key from being activated or accessed during the transportation event; and CA key transportation events shall be logged.

6.2.5 PRIVATE KEY ARCHIVAL

A complete history of all encryption private keys and certificates issued must be maintained for Saudi National Root-CA supporting functions, such as RA Administrators.

Saudi National Root-CA shall maintain controls to provide reasonable assurance that archived CA keys remain confidential, secured, and shall never be put back into production.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

Saudi National Root-CA Private Keys shall be generated in and remain in the same hardware cryptographic module.

The Saudi National Root-CA keys shall be cloned for secure backup from the master hardware cryptographic module, directly to the backup hardware cryptographic module(s) using secure mechanisms. The Saudi National Root-CA Key should not be temporarily or permanently saved in software for any purpose.

The Saudi National Root-CA keys migrated from one secure cryptographic device to another, other than for the purposes of routine backup and restoration shall be completed in a physically secure environment by those in trusted roles under multi-person control.

The hardware and software tools used during the Saudi National Root-CA key migration process shall be tested by the CA prior to the migration event. The Saudi National Root-CA keys migration event shall follow a documented script and logged.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The Saudi National Root-CA Private Keys shall be stored on FIPS 140-2 Level 3 cryptographic module, in encrypted form.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

A CA's private key shall be activated by the main stakeholders and authorized personnel, as defined in Saudi National Root-CA Operations Policy, supplying their activation data. Such activation data shall be held on secure media and shall require the successful completion of an authentication process using a password or PIN.

6.2.9 METHODS OF DEACTIVATING PRIVATE KEY

A CA's private keys shall be deactivated by the main stakeholders and authorized personnel, as defined in Saudi National Root-CA Operations Policy by removing their secure media and storing it in a secure container or environment when not in use.

6.2.10 METHODS OF DESTROYING PRIVATE KEY

The copies of Saudi National Root-CA keys that no longer serve a valid business purposes or copies of CA keys that are at the end of the key pair life cycle shall be destroyed as per NCDC Cryptographic Devices Lifecycle Management Policy and Procedure.

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 ARCHIVAL

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

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

The table below shows key usage, length and certificate lifetime:

Key/Certificate	Minimum Key Length in Bits	Maximum Validity Period
Saudi National Root CA signing Key and certificate	2048	240 months or valid not beyond 2030, whichever is earlier.
CA signing key and certificate	2048	120 months or valid not beyond 2030, whichever is earlier.
End Entity signing and non-repudiation key and Certificate	2048	36 months
End Entity Encryption Certificate	2048	36 months
End Entity Decryption Key	2048	No Expiry

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

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

6.4.2 ACTIVATION DATA PROTECTION

If written down, it will be secured at the level of the data that the associated cryptographic module is used to protect, and will not be stored with the cryptographic module.

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.

6.5.2 COMPUTER SECURITY RATING

The CA software shall be certified under the Common Criteria or ITSEC to a level equivalent to Common Criteria EAL 4.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

The Saudi National Root-CA shall maintain controls to provide reasonable assurance that CA systems development, maintenance activities, patching, and changes to CA systems shall be documented, tested, authorized, and properly implemented to maintain CA system integrity.

The Saudi National Root-CA design, installation, and operation will be documented by qualified personnel. The NCDC-SSC operational personnel, with oversight by NCDC, will develop and produce appropriate qualification documentation establishing that Saudi National Root-CA components are properly installed and configured, and operate in accordance with the technical specifications.

6.6.2 SECURITY MANAGEMENT CONTROLS

The Saudi National Root-CA shall maintain controls to provide reasonable assurance that changes to CA systems operating systems, databases, applications, network devices, and hardware shall be documented, tested, authorized, and properly implemented to maintain CA system integrity.

The configuration of the NCDC-SSC 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 ongoing maintenance of the system.

6.6.3 LIFE CYCLE SECURITY CONTROLS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

RAs shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. These network security controls include effective firewall management, including port restrictions and IP address filtering.

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 will be supported as detailed in the same section of the Saudi National Root-CA CPS.

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 Certificate profile for the Saudi National Root-CA is described in this section. The Certificate profiles of all subordinated issuing CAs of the Saudi National Root-CA and the issued subscriber certificates are described in the CP/CPS of the according issuing CA.

Certificate profiles are covered in Appendix–A.

7.1.1 VERSION NUMBERS

The Saudi National Root-CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 CERTIFICATE EXTENSIONS

NCDC critical private extensions shall be interoperable in their intended community of use.

Subordinate and Subscriber certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

Saudi National Root-CA shall sign Certificates using:

sha256WithRSAEncryption algorithm (1.2.840.113549.1.1.11).

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 Saudi National Root-CA shall contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names are in the form of an X.501 printable string.

7.1.5 NAME CONSTRAINTS

No stipulation.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

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

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

It is expected that all members of the Saudi National PKI apply to this policy.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

No stipulation.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION

No stipulation.

7.2 CRL PROFILE

The Saudi National Root-CA CRL Profile is as below:

Field	Content	Comment
Version	1	
Algorithm	SHA256withRSA	
Issuer	OU=Saudi National Root CA O=National Center for Digital Certification C=SA	
This update	*<issue date>*	
Next update	*<issue date + 12 months>*	*When a certificate is revoked or any material change is required.*
AuthorityKeyIdentifier	*<Issuing CA's Subject Key Identifier>*	
CRL number	<number>	

7.2.1 VERSION NUMBERS

Saudi National Root-CA shall issue X.509 version two (v2) CRLs (populate version field with integer "1").

7.2.2 CRL AND CRL ENTRY EXTENSIONS

Critical private extensions shall be interoperable in their intended community of use.

7.3 OCSP PROFILE

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

7.3.1 VERSION NUMBERS

The version number for request and responses shall be v1.

7.3.2 OCSP EXTENSIONS

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

NCDC shall be responsible for overseeing compliance of the Saudi National Root-CA. The NCDC-SSC shall ensure that the requirements of the Saudi National Root-CA CP, PDS and CPS and the provisions of applicable Agreements with operational policies and procedures shall be implemented and enforced.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENTS

The Saudi National Root-CA shall be subjected to periodic compliance audits which are no less frequent than once a year and after each significant change to the deployed procedures and techniques. NCDC also performing internal audit at least a quarterly basis against a randomly selected sample for monitor adherence and service quality. Moreover, NCDC may require ad-hoc compliance audits of Saudi National Root-CA to validate that it is operating in accordance with the respective CP, PDS, CPS, and other supporting operational policies and procedures.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

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

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

NCDC will appoint Qualified Auditor who shall be Licensed WebTrust Practitioner to perform such compliance audits as a primary responsibility.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4 TOPICS COVERED BY ASSESSMENT

The compliance audits will verify whether the CA PKI operations environment is in compliance with the Saudi National Root-CA CP, CPS and supporting operational policies and procedures. The term CA PKI operations environment defines the total environment and includes:

- All documentation and records;
- Contracts and agreements;

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

The auditor shall provide NCDC with a compliance report highlighting any discrepancies.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

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

8.6 COMMUNICATION OF RESULTS

An Audit Compliance Report, including identification of corrective measures taken or being taken by the audited party, shall be provided to NCDC.

The Saudi National Root-CA Audit Report shall be 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

Currently, no fees are charged by Saudi National Root-CA for Digital Certificates, although NCDC reserves the right to change this in the future.

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEE

Saudi National Root-CA may not charge for certificate issuance and renewal.

9.1.2 CERTIFICATE ACCESS FEES

Saudi National Root-CA may not charge for access to any certificates.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEE

No fee is charged for Digital Certificate revocation or status information access.

9.1.4 FEES FOR OTHER SERVICES

Saudi National Root-CA may not charge for other services.

9.1.5 REFUND POLICY

Refunds are not possible for the Digital Certificates for which no fees are charged.

9.2 FINANCIAL RESPONSIBILITY

The Saudi National Root-CA disclaims all liability implicit or explicit due to the use of any certificates issued by the Saudi National Root-CA which certify public keys of CAs.

9.2.1 INSURANCE COVERAGE

Insurance coverage for any CA shall be in accordance with the applicable Agreement between the contracting party and the CA.

9.2.2 OTHER ASSETS

The Saudi National Root-CA maintains sufficient financial resources to maintain operations and fulfill duties. Other approved CAs shall also maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to participants under the Saudi National PKI.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

Insurance and/or warranty coverage for end-entities shall be in accordance with the respective Agreement with the CSP.

It is in the sole responsibility of subscribers and relying parties to ensure an adequate insurance, to cover risks using the certificate or rendering respective services.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Information pertaining to the CA and not requiring protection may be made publicly available at the discretion of NCDC or CA PA. Specific confidentiality requirements for business information are defined in the NCDC Privacy Policy and the applicable Agreements.

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

Any corporate or personal information held by the NCDC, CAs or 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 the Privacy policy. Information contained in certificates and related certificate status is not confidential.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

Such information which is not within the scope of confidential information will be as specified by NCDC Privacy Policy, NCDC Operations Policies and procedures and applicable Agreements.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

All Saudi National PKI participants shall be responsible for protecting the confidential information they possess in accordance with the NCDC Privacy Policy and applicable laws and Agreements.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

All Subscribers identifying information as defined by NCDC Privacy Policy shall be protected from unauthorized disclosure.

9.4.2 INFORMATION TREATED AS PRIVATE

Information to be treated as private is defined in the NCDC Privacy Policy.

9.4.3 INFORMATION NOT DEEMED PRIVATE

NCDC 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

Any sensitive information shall be explicitly identified in the Agreement with the contracting party.

Access to this information shall be restricted to those with an official need-to-know in order to perform their official duties.

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 NCDC Privacy Policy.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

Any disclosure shall be handled in accordance with the NCDC Privacy Policy.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Any disclosure shall be handled in accordance with the NCDC Privacy Policy.

9.5 INTELLECTUAL PROPERTY RIGHTS

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

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 SAUDI NATIONAL ROOT-CA REPRESENTATIONS AND WARRANTIES

NCDC, acting as the Saudi National Root-CA, will warrant and promise to:

- Provide the operational infrastructure and certification services;
- Provide certification and repository services consistent with this CP, CPS and NCDC Operations Policies and Procedures;
- 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 NCDC Operations Policies and Procedures;
- Provide certificate and key management services including certificate issuance, publication, revocation and key renewal and update in accordance with the Saudi National Root-CA CP and CPS;
- Ensure that CA personnel use private keys issued for the purpose of conducting CA duties only for such purposes;
- Maintaining 24 x 7 publicly-accessible repositories with current information and replicates Saudi National Root-CA issued certificates and CRLs;
- All Application Software Suppliers with whom the Saudi National Root-CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
- Ensure for the performance and warranties of the subordinate CAs that CAs operations will comply with all stipulated requirements, liabilities and obligations.

The representations and warranties that each CA provides will be described in the corresponding Agreement.

9.6.2 CA REPRESENTATIONS AND WARRANTIES

- At the time of Certificate issuance, CA shall implement procedure for verifying accuracy of the information contained within it before installation and first use;
- Implemented a procedure for reducing the likelihood that the information contained in the Certificate is not misleading;
- Implemented procedures for verifying Device Sponsor requesting the Secure Site Certificate on behalf of the Device as authorized representative and to verify that the applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension;
- Maintaining 24 x 7 publicly-accessible repositories with current information and replicates issued certificates, CRLs;
- For the CA's, the Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the CA keys and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;
- CA private key is generated using multi-person control "m-of-n" split key knowledge scheme;
- Backing up of the CA signing Private Key is under the same multi-person control as the original Signing Key; and
- 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.

9.6.3 RA REPRESENTATIONS AND WARRANTIES

An RA who performs registration functions represents and warrants that it shall comply with the stipulations of this CP, and the associated CPS. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

9.6.4 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

1. Subscriber is obligated to:
   - 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 Subscriber Certificate only for its intended uses as specified by the CSPs;
   - Notify the CSP 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 that does not violate applicable laws in the Kingdom of Saudi Arabia; and
   - Immediately cease use of the Subscriber Certificate upon termination of Subscriber Agreement, revocation or expiration of 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.

9.6.5 RELYING PARTIES REPRESENTATIONS AND WARRANTIES

Relying Parties who rely upon the certificates issued under Saudi National 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 suspended or revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon; and
- Determine that such Certificate provides adequate assurances for its intended use.

9.7 DISCLAIMERS OF WARRANTIES

NCDC, 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.

The Saudi National Root-CA 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 Saudi National PKI or for the legal validity, acceptance or any other type of recognition of its own certificates, those issued by it or by other Subordinate entity, any digital signature backed by such certificates, and any products provided by the NCDC. The NCDC 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:

- The Saudi National Root-CA will not incur any liability to Subscribers or any person to the extent that such liability results from their negligence, fraud or willful misconduct;
- The Saudi National Root-CA assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under this policy for any use other than in accordance with this policy. Subscribers will immediately indemnify the Saudi National Root-CA from and against any such liability and costs and claims arising there from;
- The Saudi National Root-CA 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;
- End-Users, RAs, CSPs are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by CSPs or Saudi National Root-CA;
- Subscribers to compensate a Relying Party which incurs a loss as a result of the Subscriber's breach of Subscriber agreement;

- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations;
- Registration Authorities shall bear the consequences of their failure to perform the Registration Authorities obligations described in the Registration Authorities agreement and
- Saudi National Root-CA denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

9.9 INDEMNITIES

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, the CA SHALL defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

The CSPs shall indemnify, defend and hold harmless:

- NCDC, its CEO,, officers, employees, agents, consultants, and subsidiaries from any and all claims, damages, costs (including, without limitation, attorney's fees), judgments, awards or liability;
- The CSP's own employees, arising from any of the CSP's operations and activities as a CSP , of any entity or services subordinated or outsourced by the CSP; and
- Any parties relying on the CSP's Certificates, or arising as a result of an infringement or violation of any patents, copyrights, trade secrets, licenses, or other property rights of any third party.

9.10 TERM AND TERMINATION

9.10.1 TERM

The CP becomes effective upon publication in the repository. Amendments to this CP become effective upon publication of approved 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 the Saudi National Root-CA CP can be found at: https://www.ncdc.gov.sa/.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this CP, 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 the NCDC, PA, Saudi National Root-CA, other CAs, Cross certifying entities, RAs and LRAs 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 Certificate assurance level.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

NCDC shall review this CP at least once per year. Errors, updates, or suggested changes to this CP shall be communicated to the Saudi National PKI participants and Subscribers. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change. Any technical changes in the Saudi National PKI shall be managed as per the NCDC Change Management Policy.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

This CP and any subsequent changes shall be made available to the Saudi National PKI participants within two weeks from approval. NCDC 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 Saudi National PKI participants and other parties designated by NCDC shall provide their comments to NCDC in accordance with NCDC rules.

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 NCDC, in its sole discretion.

9.13 DISPUTE RESOLUTION PROVISIONS

The use of certificates issued by the NCDC is governed by contracts, agreements, and standards set forth by the NCDC. 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 the NCDC 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 NCDC.

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 AND WAIVER OF RIGHTS)

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

9.16.5 FORCE MAJEURE

The Saudi National Root-CA 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

The Saudi National Root-CA is not the agent, fiduciary, trustee or any other representative of any of the approved CAs and must not be represented by the approved CAs in that form. The approved CAs have no authority to bind the Saudi National Root-CA, by contract or otherwise of any obligation or financial implication.

9.17.2 ADMINISTRATIVE PROCESSES

No Stipulation.

APPENDIX - A: CERTIFICATE TYPES

This section details Root, Government and Commercial CAs certificates issued by the Saudi National Root-CA.

1. EXTENSION DEFINITIONS – ROOT CA CERTIFICATE

Field / x.509 extension	Value or Value Constant	Critical
Subject	OU=Saudi National Root CA O = National Center for Digital Certification C = SA (Encoding should be in UTF8 only)	V1 Field
CRL Distribution Points	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/CRL/nrcapart<n>.crl Directory Address: CN=CRL1 OU=Saudi National Root CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/CRL/nrcacomb<n>.crl	NO
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Saudi National Root CA (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	<same data as in Authority Key Identifier above>	NO
Basic Constraints	Subject Type=CA Path Length Constraint=None	YES
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ncdc.gov.sa	NO
Key Usage	Certificate Signing; CRL Signing	YES

2. EXTENSION DEFINITIONS – GOVERNMENT CA CERTIFICATE

Field / x.509 extension	Value or Value Constant	Critical
Subject	OU=Government CA O = National Center for Digital Certification C = SA (Encoding should be in UTF8 only)	V1 Field
CRL Distribution Points	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/CRL/nrcapart<n>.crl Directory Address: CN=CRL1 OU=Saudi National Root CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/CRL/nrcacomb<n>.crl	NO
Authority Key Identifier	<Same as the SubjectKeyIdentifier of the National Root CA>	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Government CA (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=CA Path Length Constraint=None	YES
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ncdc.gov.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://web.ncdc.gov.sa/certs/snrcasha256.crt	NO
Key Usage	Certificate Signing; CRL Signing	YES

3. EXTENSION DEFINITIONS – BTC LICENSED CA CERTIFICATE

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = BTC LICENSED CA O = BAUD Telecom Company C = SA (Encoding should be in UTF8 only)	V1 Field
CRL Distribution Points	e.g. [1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/CRL/nrcapart<n>.crl Directory Address: CN=CRL1 OU=Saudi National Root CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/CRL/nrcacomb<n>.crl	NO
Authority Key Identifier	<Same as the SubjectKeyIdentifier of the Saudi National Root CA>	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the BTC Licensed CA (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=CA Path Length Constraint=None	YES
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ncdc.gov.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://web.ncdc.gov.sa/certs/snrcasha256.crt	NO
Key Usage	Certificate Signing; CRL Signing	YES

4. EXTENSION DEFINITIONS – STCS INTERMEDIARY CA CERTIFICATE

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = STCS Intermediary CA O = STCS C = SA (Encoding should be in UTF8 only)	V1 Field
CRL Distribution Points	e.g. [1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/CRL/nrcapart<n>.crl Directory Address: CN=CRL1 OU=Saudi National Root CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/CRL/nrcacomb<n>.crl	NO
Authority Key Identifier	<Same as the SubjectKeyIdentifier of the Saudi National Root CA>	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the STCS Intermediary CA (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=CA Path Length Constraint=None	YES
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ncdc.gov.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://web.ncdc.gov.sa/certs/snrcasha256.crt	NO
Key Usage	Certificate Signing; CRL Signing	YES