المركز الوطني للتصديق الرقمي
NATIONAL CENTER FOR DIGITAL CERTIFICATION

NATIONAL PKI POLICY

Document Classification:

Public

Version Number:2.3

Issue Date: November 30, 2020

Table of Contents

1. SAUDI NATIONAL PKI FRAMEWORK

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 secure, efficient transmission and exchange of information electronically, the Kingdom of Saudi Arabia has created a National Public Key Infrastructure, named National Center for Digital Certification (NCDC). NCDC is created by an act of law and its mandate is stipulated in the Saudi Electronic Transactions Act. NCDC provides trust services to secure exchange of information between key stakeholders. Participants include:

- Government
- Citizens
- Business

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.

NCDC owns and operates the Saudi National Root Certification Authority of the Kingdom of Saudi Arabia. Approved Certification Authorities (CAs) shall be providers of certification services to Subscribers, Relying Parties and Registration Authorities through Certification Service Providers (CSPs). Together all of these components and participants form the “Saudi National PKI.”

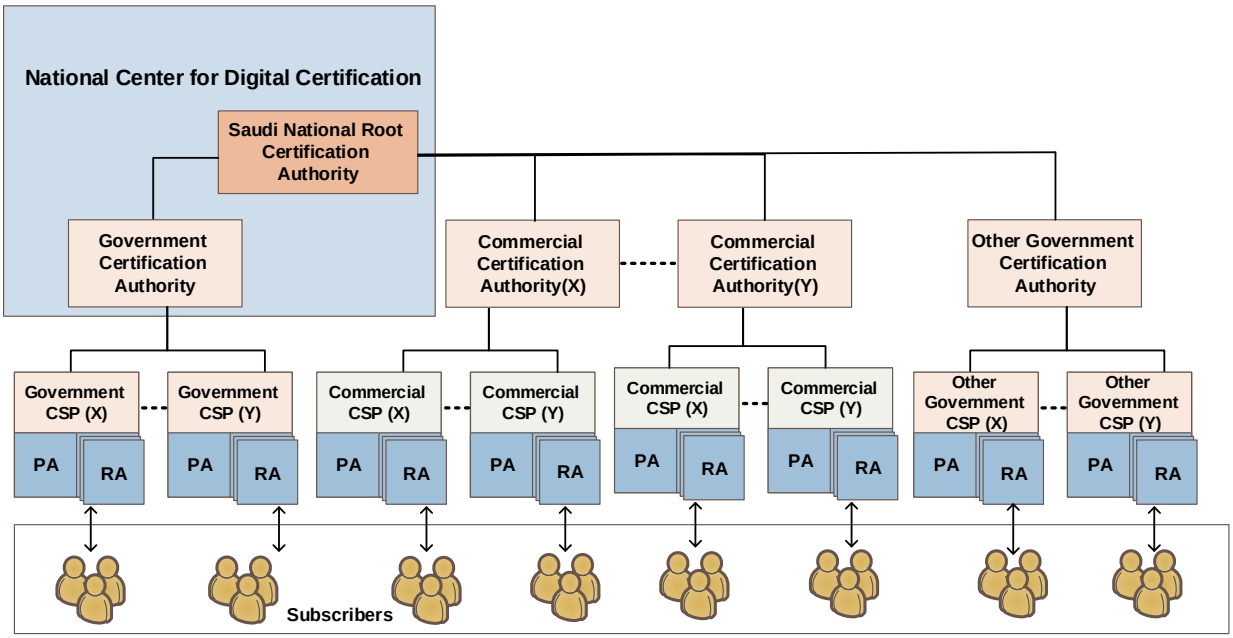

Figure 1: Saudi National PKI framework

2. DEFINITIONS

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

The following verbal forms are used throughout the document to identify and distinguish the requirements that are mandatory from the provisions where there is a certain freedom of choice:

- "**shall**": this verbal form is used to indicate requirements strictly to be followed in order to conform to the present document and from which no deviation is permitted;
- "**should**": this verbal form is used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited;
- "**may**": this verbal form is used to indicate what is permitted by the present document, which can be values, actions, support and /or use of features or presence/absence of optional elements.

3. SCOPE

This document is intended for use by the Certification Authority (CA) wishing to set up operations under the Saudi National Root CA. The aim of this document is to introduce requirements for such CAs and to ensure that such CAs can fit into the Saudi National PKI framework.

4. INTRODUCTION

4.1 GENERAL REQUIREMENTS

This section identifies and introduces the set of provisions and indicates types of entities and applications for which the prospective CA is going to issue certificates. This section can also be used to provide synopsis of the CA PKI business.

- A CA must have Certificate Policy (CP), PKI Disclosure Statement (PDS) and a Certification Practice Statement (CPS) conforming to the CP. The Certification Authority CP and CPS shall adhere to [IETF RFC 3647] with relevant supportive administrative, technical and operational documents.
- The CP shall be a public document published by the CA describing the conditions that are attached to use and application of the certificates it issues. The CPS shall be a public document describing the practices followed by the CA in managing the certificates it issues.
- A CA shall take NCDC approval before adding any new Reliable KYC (Know Your Customer) Agency.
- The Trusted Service Provider(TSP) shall make these documents available on a 24x7 basis to subscribers and relying parties.
- CPS shall include the complete CA hierarchy, including Root and subordinate CA's.
- CPS shall include the signature algorithms and parameters employed.
- CPS shall specify the practice regarding the use of CA keys for signing certificates, CRLs and OCSP.
- Where a CA includes a hierarchy of subordinate CAs chaining up to Saudi National Root CA, the CA shall be responsible for ensuring the subordinate CAs comply with

the applicable policy requirements defined in this policy

- The CA shall publish Public Disclosure Statement that summaries key points of the Certificate Policy for the benefit of Subscribers and Relying Parties.
- Every CA will obtain OID from NCDC under the OID scheme set up for the Saudi National PKI. NCDC has published latest OID Allocation document on https://www.ncdc.gov.sa. OIDs shall be utilized from the OID arc allocated by the Saudi Arabian Standards Organization:

  http://www.oid-info.com/cgi-bin/display?oid=2.16.682.1.101.5000&submit=Tree+display.
- CAs may seek guidance from NCDC for OID allocation for the certificates types it is going to support.
- The CA may issue different types of certificates for the different levels of assurance it supports in accordance with the respective CA policy document. In any case, the CA shall describe the applications or types of applications that are appropriate or inappropriate for the different types of certificates for the different levels of assurance it supports. CA shall take NCDC approval before introducing any new certificate type for its subscriber community.
- For each type of certificate, it issues, the CA shall assign separate OID and describe appropriate policies and practices followed, specific to each certificate type. The description shall cover the following aspects at a minimum:
  - Certificate Subject
  - Assurance Level
  - Assurance Level OID
  - Policy OID
  - Policy Name
  - Certificate Profile
  - Application Usage
  - Verification Process
  - Key Pair Generation and Installation
  - Certificate Issuance Process
  - Key Usage
  - Private Key Protection
  - Certificate Life-time
  - Key Backup
  - Asymmetric Key Length
  - Certificate Re-key / Renewal
  - Obligations
  - Liability
  - Fees
  - Warranties
  - External Auditing
  - Record Maintenance
- The set of policies and practices (incl. CP's, CPS, and PDS's) shall be approved by management, published and communicated to employees and external parties as relevant

- **Terms & conditions**
  - CAs shall make the terms and conditions regarding its services available to all subscribers and relying parties.
  - Before entering into a contractual relationship with a subscriber, the TSP shall inform the subscriber of the terms and conditions regarding use of the certificate, through a durable (i.e. with integrity over time) means of communication, and in a human readable form.
  - The terms and conditions may be transmitted electronically and may use the form of a PKI Disclosure Statement.
  - The terms and conditions shall at least specify for each certificate policy supported by the CA the following:
    a) the certificate policy being applied;
    b) any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations (e.g. the expected life-time of digital certificates);
    c) what is deemed to constitute acceptance of the certificate;
    d) the subscriber's obligations, if any, and where applicable, the subject's obligations;
    e) information for parties relying on the trust service (e.g. how to verify the digital certificate, any possible limitations on the validity period associated with the digital certificate);
    f) the period of time during which
       - CA's event logs are retained;
       - Subscriber’s agreements are recorded;
    g) limitations of liability;
    h) the notice to relying parties (see below);
    i) the ways in which a specific policy adds to or further constrains the requirements of the CP;
    j) the applicable legal system;
    k) procedures for complaints and dispute settlement;
    l) whether the CA’s trust service has been assessed to be conformant with the certificate policy, and if so through which conformity assessment scheme;
    m) the CA's contact information; and
    n) any undertaking regarding availability.
  - Subscribers and parties relying on the trust service shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship.
  - Terms and conditions shall be made available through a durable means of communication.
  - Terms and conditions shall be available in a readily understandable language.
  - The CA, the CSP and the RA(s) it designates, may limit their responsibilities in accordance with the laws of the Kingdom of Saudi Arabia.
- **Subscriber agreement:**
  - The agreement with the subscriber and if the subscriber and subject are two separate entities and the subject is a natural or legal person, with the subject, shall

involve explicit acceptance of the terms and conditions by a willful act which can be later supported by evidence.

- The CSP, or the RA it designates, shall record the subscriber agreement , for the period of time as indicated to the subscriber as part of the terms and conditions.
- Where the subscriber and subject are two separate entities and the subject is a natural or legal person:
  a) the agreement shall be in 2 parts;
  b) the first part of the agreement shall be ratified by the subscriber and shall include:
     - agreement to the subscriber's obligations (see below);
     - if an end-entity hardware secure cryptographic device is used, agreement by the subscriber to use such a device;
     - consent to the keeping of a record by the CSP, or the RA it designates, of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation, the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by the applicable policy in the case of the CA and/or the CSP terminating its services;
     - whether, and under what conditions, the subscriber requires and the subject consents to the publication of the certificate;
     - confirmation that the information to be held in the certificate is correct, which may be achieved by reference (e.g. reference to the CP for the fields of the certificate that are fixed by the CP).
     - obligations applicable to subjects (see below);
  c) the second part of the agreement shall be ratified by the subject and shall include:
     - the agreement by the subject on the obligations applicable to subjects;
     - if an end-entity hardware secure cryptographic device is used, agreement by the subject to use such a device;
     - consent to the keeping of a record by the CSP, or the RA it designates, of information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation, the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the CA and/or the CSP terminating its services.
- Where the subject and subscriber are the same entity or the subject is a device, the agreement shall be in one or two parts, which should include the items listed above;
- The agreement may be in electronic form, which shall be digitally signed (Note: a specific legal type of signature/seal may be recommended here).

- **Subscriber's obligations** shall include:
  - an obligation to provide the CSP, or the RA it designates, with accurate and complete information in accordance with the requirements pursuant to the certificate type and assurance level, particularly with regards to registration;
  - an obligation for the key pair to be only used in accordance with any limitations notified to the subscriber and the subject if the subject is a natural or legal person;

- prohibition of unauthorized use of the subject's private key;
- if the subscriber or subject generates the subject's keys, an obligation to use key length and cryptographic suites as prescribed in the present document;
- an obligation for the subject's private key to be maintained under the subject's (sole) control;
- if an end-entity hardware secure cryptographic device is used, an obligation, when applicable to generate, and to use the subject's private key(s) for cryptographic functions within that device;
- an obligation to notify the CA, the CSP, or the RA it designates, without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
  a) the subject's private key has been lost, stolen, potentially compromised;
  b) control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons;
  c) inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject;
- an obligation, following compromise of the subject's private key, to immediately and permanently discontinue the use of this key, except for key decipherment; and
- an obligation, in the case of being informed that the subject's certificate has been revoked, or that the issuing CA has been compromised, to ensure that the private key is no longer used by the subject.

- **Subject's obligations**: If the subject and subscriber are separate entities and the subject is a natural or legal person, the subject should be informed of his/her obligations, which shall include:
  - an obligation for the key pair to be only used in accordance with any limitations notified;
  - prohibition of unauthorized use of the subject's private key;
  - if the subject generates the subject's keys, an obligation to use key length and cryptographic suites as prescribed in the present document;
  - an obligation to notify the CA, the CSP, or the RA it designates, without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
    a) the subject's private key has been lost, stolen, potentially compromised;
    b) control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons;
    c) inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject;
  - an obligation, following compromise of the subject's private key, to immediately and permanently discontinue the use of this key, except for key decipherment; and
  - an obligation, in the case of being informed that the subject's certificate has been revoked, or that the issuing CA has been compromised, to ensure that the private key is no longer used by the subject.
- **Notice to Relying Parties**: The notice to relying parties shall recommend the relying party to:
  - verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party;
  - take account of any limitations on the usage of the certificate indicated to the relying

party either in the certificate or the terms and conditions supplied;

- take any other precautions prescribed in agreements or elsewhere, including potentially instructions regarding reporting potential problems.

- **Information security policy requirements**: The CA shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security.
- **Personal data protection**:
  - The CSP, or the RA(s) it designates, shall provide evidence of how they meet applicable data protection legislation within their registration process.
  - The verification policy used by the CSP, or the RA(s) it designates, shall only require the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.

4.2 LEVELS OF ASSURANCE

Three levels of assurance (LoAs) are introduced and identified for the issuance of digital certificates under the Saudi National PKI, all of them providing unicity of the digitally certified identity within an intended context but respectively providing low, medium or high confidence in the accuracy or legitimacy of that identity:

- **LOW**

  This level provides little confidence in the accuracy or legitimacy of the claimed identity as it requires no or low assurance of the binding between the identity of the entity named in the certificate and the Subscriber. It is intended for Subscribers handling information of little or no value within minimally secured environments. Identity assertions at this level are appropriate for transactions with minimal consequences to Relying Parties from the registration of a fraudulent identity.

  Digital certificates at this level require no or low assurance of the binding between the identity of the entity named in the certificate and the Subscriber. The keys and certificates may only be generated in a software security module and be stored in a software form factor. Given the limited assurance provided, a Key Usage of non-repudiation is not permitted, nor are Extended Key Usages of smartcard logon or code signing.

- **MEDIUM**

  This level provides medium confidence in the accuracy or legitimacy of the claimed identity. It is intended for Subscribers handling information of medium value within substantially secured environments. Identity assertions at this level are appropriate for transactions with serious (substantial) consequences to Relying Parties from the registration of a fraudulent identity. Digital certificates at this level require medium or high assurance of the binding between the identity of the entity named in the certificate and the certificate holder.

  The keys and certificates at this level can be generated in either at least FIPS 140-2 Level 2 or higher certified hardware or software security module and can be stored in either a software or hardware form factor. User consent is required each time the private key is activated.

- **HIGH**

  This level provides a high confidence in the accuracy or legitimacy of the claimed identity. It is intended for Subscribers handling information of high value within highly secured environments. Identity assertions at this level are appropriate for transactions with catastrophic consequences to Relying Parties from the registration of a fraudulent identity. Digital certificates at this level require very high assurance of the binding between the identity of the entity named in the certificate and the certificate holder. The keys and certificates can only be generated in:

  Case 1: Hardware-based security module and stored in a hardware-based form factor (e.g. Smart Cards or USB Tokens) at least FIPS 140-2 Level 2 validated or equivalent.

  Case 2: Hardware-based solution required when key generated and managed by CA/TSP, at least FIPS 140-2 Level 3 validated or equivalent (this allows key encrypting key or key wrapping based solutions).

  Authenticated-user's consent or PIN unlocks are required each time the private key is activated.

These levels of assurances apply for the issuance of digital certificates to all types of entities, namely natural persons, legal person (e.g. corporations, organizations), and devices. The latter shall always be associated to a person, being natural or legal.

5. PUBLICATION AND REPOSITORY RESPONSIBILITIES

This section defines the provisions regarding the Certification Authority's obligations to publish information regarding its practices, certificates and current status of the certificates. This will also describe the access control on the published information such as Certificate Policy, certificates status and CRLs with the frequency of publication.

- Each CA shall have a repository for its issued certificates and CRLs. The CA repository must be available on a 24x7 basis and replicates certificates issued and revoked.
- Repositories shall be fault tolerant and online with high availability provisions.
- Digital Certificate issued under the Saudi National PKI must be X.509 v3 in accordance to the [RFC 5280] otherwise approved by NCDC.
- The CAs shall implement access restrictions for repository to prevent misuse and unauthorized harvesting of subscriber information.
- Repository information is stored using technology that may support one or more of the following industry standards and schema:
  - LDAP v3 operations
  - LDAP search filters
  - LDAP v3 intelligent referral
  - Relevant LDAP v3 RFCs
  - DSML (Directory Service Markup Language) v2
  - HTTPS
- Upon generation, the complete and accurate certificate shall be available to the subscriber or subject for whom the certificate is being issued.
- Certificates shall be available for retrieval in only those cases for which the subject's

consent has been obtained. If the subject is a device or system, the consent of the natural or legal person responsible for the operating of the device or system needs to be obtained, instead of the subject.

- The CA shall make available to relying parties the terms and conditions regarding the use of the certificate.
- The applicable terms and conditions shall be readily identifiable for a given certificate.
- With regards to the 24x7 availability of the repository, upon system failure, service or other factors which are not under the control of the CA, the CA shall apply best endeavors to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS.
- The repository shall be publicly and internationally available.

6. IDENTIFICATION AND AUTHENTICATION

This section describes procedures used by Certification Authority to authenticate a subscriber prior to certificate issuance. This contains the naming practices adopted by the Certification Authority from name recognition, recognition to name dispute resolution. It also describes how parties requesting re-key or revocation are authenticated.

- CSPs shall setup Registration processes based on the certificate type and assurance level for subscribers prior to issue them with certificates.
- The CSP may request to CA for specific type of certificate based on the new requirements of their user community.
- The CA PA shall take up new requirements with NCDC and based on approval; grant permission for any changes in the current certificate or new certificates types.
- The registration request shall be supported with valid identity documentation.
- The CSPs may designate specific RAs to perform the Subscriber's Identification and Authentication and Certificate life cycle management defined in the respective CA-CP and other relevant documents.
- The RA is obligated to perform certain functions pursuant to an RA Agreement. An RA who performs registration functions represents and warrants that it shall comply with the stipulations of applicable CP, and the associated CPS.
- The CA shall ensure that registration procedure ties the private key whose corresponding public is to be certified with the identity being asserted by the subscriber (proof of possession).
- When the CA designates a third party (e.g. TSP) for generating and/or managing the Subscriber's private key, the CA shall ensure that:
    - The third party is obligated to perform Subscriber device management functions pursuant to an appropriate Agreement.
    - The third party who performs Subscriber device management functions represents and warrants that it shall comply with the stipulations of applicable Agreement, applicable CP, and the associated CPS.
- Pseudonymity may be supported, not anonymity.
- The RA Administrator(s) engaged in Certificate issuance shall be given detailed training to perform their tasks. NCDC or CA shall design examination based on the training which is to be qualified by each RA Administrator.
- Where a Subscriber has already undergone an in-person identity and authentication process by a CSP to receive a certificate, the Subscriber may use that certificate and may obtain further NCDC-issued certificates without having to undertake another face-

to-face registration based upon understanding between CSPs.

- The CSP, or the RA(s) it designates, shall record all the information necessary to verify the subject's identity and if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity. This includes all evidences related to the identification and identity validation of the subscribers, authorizers, and certificate managers when used to verify the subject's identity.
- The TSP shall record the certificate acceptance agreement with the subscriber and if the subscriber and subject are two separate entities and the subject is a natural or legal person, agreement with the subject.

7. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This section will specify requirements imposed upon the Certification Authority or subscribers regarding various operational activities with respect to certificate life cycle management e.g. certificate application, issuance, acceptance, back up, suspension and revocation.

- The prospective CA must follow process defined by NCDC and successfully complete all steps required for setting up Certification Authority business. In addition, for commercial CAs, a license must be obtained from the CITC after an application is approved by NCDC.
- All key backup functionalities shall be governed by CMP protocol in accordance with RFC 4210 and certification request syntax shall be in accordance with PKCS #10.
- CA private keys shall be encrypted and stored in a [FIPS PUB 140-2] Level 3 validated HSM.
- The CA signing keys shall be backed up under the same multi-person control as the original signature keys.
- Access to the CA's private key shall require multiple authorizations and tight security measures.
- The RA's/LRA's private keys shall be encrypted and stored in at least [FIPS PUB 140-2] Level 2 or Higher validated Hardware Cryptographic devices.
- Subscriber key pairs are generated based on the Assurance Level. If subscriber key pairs are generated using cryptographic modules then the cryptographic modules shall be at least compliant to FIPS 140-2 Level 2 or higher.
- NCDC reserves right to revoke and/or to request the revocation of any certificate if deemed necessary.

8. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This section describes the measures relating to non-technical security control to provide reasonable assurance that physical access to the CA is limited to authorized trusted individuals with proper background checks. This section indicates the level of security required to ensure that CA remains trusted and safe for its user communities and those with which it interoperates.

The CA systems shall be hosted in a secured facility and protected from environmental hazards:

- A Threat Risk Assessment shall be performed before establishing the CA facility and operations and subsequently at least once a year.
- The CSP PA shall visit RA facility and review procedures with a contemplation of

environmental factors, technological and operational infrastructures, and the security infrastructure as it relates to the services being offered as per the RA agreement.

- The CAs must perform third party vulnerability assessment at least once a year.
- The CAs shall ensure recording in audit log files all events relating to the security of the CA system.
- The CAs shall retain all system generated (electronic) and manual audit records onsite for a period not less than six months from the date of creation.
- The minimum retention period for archive data is ten years.
- The CAs shall ensure that CSPs shall retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least ten years after any Certificate based on that documentation ceases to be valid.
- All logs must be time stamped and CA must use GPS time synchronization.
- Multiple time servers shall be located in multiple security zones.
- The servers shall synchronize with a predefined set of reliable atomic clock time servers on the internet/using GPS which are secured and governed by a well-known independent authority.
- The CAs shall establish an appropriate separation of duties between key roles.
- All persons filling trusted roles shall be selected on the basis of skills, loyalty, trustworthiness, integrity. 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. Examples of such trusted roles for a CA operation are:
  - CA Master User
  - CA Officer
  - CA Administrator
  - CA Operator
  - CA Auditor
- The CAs must ensure that contingency plans are prepared, tested and regularly updated to address business continuity of operations.

9. TECHNICAL SECURITY CONTROLS

This section defines the security measures taken by the issuing Certification Authority to protect its cryptographic keys and activation data (e.g. PINs, password). Secure key management is critical component for any PKI and the issuing CA shall ensure that all keys and activation data are protected and used by authorized personnel only. Also, this section defines technical controls implemented by the CA for performing functions such as certificate life cycle management, audit and archival. The technical security controls shall include life-cycle security controls and operational security controls.

- The CA software shall be certified under the Common Criteria or ITSEC to a level equivalent to Common Criteria EAL 4.
- The CA's Hardware Security Modules (HSM's) used for key generation shall meet the requirements of [FIPS PUB 140-2] Level 3.
- Multi-person control of CA private key shall be achieved using an "m-of-n" split key knowledge scheme.
- The CA signing keys shall be backed up under the same multi-person (m of n) control

as the original signature keys.

- The CA shall implement System Security Technical controls and set up procedures according to appropriate standards (e.g. [ISO/IEC 27001:2013] or similar).
- According to [IETF RFC 5280], the Key Identifiers used for CA Certificates shall comply to first option provided and should be as suggested below:

  (1) The key Identifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subject Public Key (excluding the tag, length, and number of unused bits).
- The following algorithms and key lengths are recommended under the Saudi PKI framework:
  - Symmetric Key: AES (minimum 128-bit key strength)
  - Hashing Algorithms: Secure Hash Algorithm version (SHA256)
  - Asymmetric Key: RSA
  - Minimum Public Key sizes:
    - Saudi National Root-CA Key Pair: 2048 bits
    - Subordinate CA Key pair: 2048 bits
    - OCSP Key Pair: 2048 bits
- The maximum certificate lifetime shall be:
  - Saudi National Root-CA Signing Certificate — 240 months or valid not beyond 2030 whichever is earlier
  - Subordinate CA signing Certificate — 120 months valid not beyond 2030 whichever is earlier

10. CERTIFICATE, CRL, AND OCSP PROFILES

This section defines X.509 certificate and CRL format including profile information, versions and extensions used.

- CA's shall issue, update and sign Certificates and CRLs as per RFC 5280. The CRL profile shall be compliant with X.509 CRL v2 profile and X.509 v3 CRL extensions which is specified by RFC 5280. OCSP requests and responses shall be in accordance with RFC 6960.
- The CA shall include Assurance Level OID in each issued certificate profile.
- The CA shall support complete certificate life cycle management comprise of following functions:
  - The Initialization is composed of the following functions: registration, key pair generation, certificate creation, certificate publication, and key/certificate delivery.
  - The Operation services can be summarized as following: Certificate Retrieval, Certificate Validation, Key Recovery, key/certificates Update/Renewal, Key History.
  - The termination service is composed of the following functions: Certificate Expiration, Certificates Suspension , Certificate Revocation and Certificate Destruction.

11. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This section covers frequency of the compliance audit or other assessment, auditor qualification, auditor relationship with the entity being audited, scope of the audit and action taken on the deficiencies found during the audit.

- CAs shall be subject to periodic compliance audits which are no less frequent than twelve (12) months. However, NCDC reserves right to conduct ad-hoc compliance audits of CAs operations.
- The compliance audits will verify whether the CA PKI operations environment is in compliance with the applicable CP, CPS and supporting operational policies and procedures. The term CA PKI Operations environment defines the total environment and includes, but is not limited to:
  - all documentation, records,
  - contracts/agreements,
  - compliance with applicable Law,
  - physical and logical controls,
  - personnel and approved roles/tasks,
  - hardware (e.g. servers, desktops, hardware security modules, network devices and security devices),
  - software and information.
- The CSP or an entity designated by it shall have the right to carry out annual as well as periodic audits and investigations in accordance with the contractual agreement, of the records, operations and services provision of the RA. The RA is also required in its contract with any LRA's and any relevant outsourced services, to provide equivalent access to auditors and investigators representing the CSP.
- 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;
  - Bound by law, government regulation, or professional code of ethics; and
- The auditor shall perform such compliance audits as a primary responsibility. NCDC will appoint Qualified Auditor which is Licensed WebTrust Practitioner.
- An Audit Compliance Report, including identification of corrective measures taken or being taken by the audited party, shall be provided to the respective PA and/or NCDC as applicable.
- The CAs shall make the Audit Report publicly available no later than three months after the end of the audit period.
- CAs shall also performing internal audit at least on a quarterly basis against a randomly selected sample for monitor adherence and service quality.

The following audit schemes and auditors are deemed to be recognized (qualified):

- WebTrust for CA audits conducted by Licensed WebTrust Practitioner, provided that the CP/CPS of the CA has been assessed to be in compliance with and abide by the requirements of the present document;

- Audits confirming the CA compliance with the requirements of the present document, conducted by a conformity assessment body that has been accredited under the framework of [ISO/IEC 17065] supplemented by [ETSI EN 319 403] by a national accreditation body signatory of the International Accreditation Forum[1] multilateral agreement. The attestation and conformity assessment report issued by such a conformity assessment body must confirm that the assessed CA and its trust services issuing digital certificates are conformant to the requirements of the present document.

12. OTHER BUSINESS AND LEGAL MATTERS

This section covers general business and legal matters. The subsections cover provision relating to the fees charged by the CA and repositories for the various services provided and to the financial responsibility of the participants.

- The CAs shall cover the fees for the services and refund policy.
- The CAs shall cover provisions relating to Governing law, Severability, merger, survival and dispute resolution.
- The CA shall cover the confidentiality of business requirements in the Privacy Policy and the applicable agreements.
- The CA shall cover provisions regarding apportionment of liability for each type of entity, insurance coverage, warranties and limitation of warranties.
- The CA shall describe the financial responsibilities of CA and repository.