SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority

SAUDI NATIONAL ROOT-CA

CERTIFICATION PRACTICE STATEMENT

Document Classification:

Public

Version Number: 3.4

Issue Date: May 22, 2023

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	2006	E & Y	NCDC CPS
1.2	21/09/2008	Dr Deoraj	Revision of the CPS document for Saudi National Root-CA
1.3	8/10/2008	Dr Deoraj	Incorporated comments of Mohammed & Jaser after discussion
1.31	15/10/2008	Dr Deoraj	Audit log and Archival Period , CRL Frequency timeframe assigned
1.4	17/01/2009	Dr Deoraj	Copyright statement modified , comments in respect of new latest model
1.41	30/01/2009	Dr Deoraj	Liability, warranties added based on comments from Dr Fahad and Mohammed
1.5	06/03/2009	Dr Deoraj	Changes incorporated on the review comments from team and added certificate profile received from Parag, Phani & Chirag
2.0	1/06/2010	Dr Deoraj	NPA is replaced with NCDC , NCDC Hierarchy, Glossary link, Gov CA Profile added and other agreed changes
2.1	9/8/2011	Dr Deoraj	Changes made as per WebTrust Observations along with other suggested changes
2.2	27/03/2012	Dr. Deoraj and Naif	Updated as per CAB Forum recommendations and SHA-2 upgrade.
2.3	04/12/2012	Naif	Updated section 5.7.4 to include implementation of NCDC DR site. And update section 4.9.12 to include key compromise.
2.4	4/12/2013	Naif	Annual review, no changes
2.5	15/4/2015	Dr. Deoraj and Naif	Annual review
2.6	16/05/2016	Dr. Deoraj and Naif	Annual review
2.7	23/05/2017	Dr. Deoraj and Naif	Annual review, CAB Forum compliance statement added, Trust model drawing changed
2.8	23/05/2018	Dr. Deoraj and Khalid Bin Kulaib	Annual review ,changes as per WebTrust Principles and Criteria 2.1 added
2.9	04/07/2019	Dr. Deoraj and Meshal M. Al-shahrani	Annual review, Changes as per the WebTrust Baseline 2.4,removed fax

3.0	04/11/2019	Dr. Deoraj and Meshal M. Al-shahrani	Key escrow and Commercial CA related text updated
3.1	16/04/2020	Dr. Deoraj and Abdullah Aldhuwayhi	Annual review
3.2	20/06/2021	Abdullah Aldhuwayhi and Dr. Deoraj	Annual review
3.3	17/05/2022	Dr. Deoraj	Annual review
3.4	22/05/2023	Ammar Alsofyani	Update the CPS with NIC policies

Table of Contents

1. INTRODUCTION

This Certification Practice Statement (CPS) establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by the Saudi National Root Certification Authority (Root-CA) of the Government of Saudi Arabia and its approved Certification Authorities (CAs). In particular, this CPS establishes the processes and procedures the Saudi National Root-CA follow to:

- Issue National Information Center (NIC) compliant cross certificates to CA at national level,
- Issue cross certificates to other peer CAs at international level upon NIC approval,
- Certificate issuance to supportive administrative roles for the Saudi National Root-CA operations,
- Maintenance, revoke certificates issued by the Saudi National Root-CA,
- Directory management of the certificate related items, and
- Operate the OCSP Responder.

It is the responsibility of all parties under the Saudi National Root-CA CPS to understand the practices established for the lifecycle management of certificates issued to the approved CAs, other cross certified CAs at international level and to the supportive administrative roles for Saudi National Root-CA operations.

NIC 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 Digital Trust Service Providers (DTSPs) if expressly approved by NIC. The Digital Government Authority (DGA) is the regulator of Digital Trust Services in the Kingdom of Saudi Arabia. Together all of these components and participants form the “Saudi National PKI”.

A new service delivery model has been created whereby a shared National PKI Center has been created. The PKI Center at National Information Center (NIC-PKIC) 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 NIC-PKIC and managing their operations.

This CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) request for comments (RFC) 3647, Certificate Policy and Certification Practices Framework.

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 CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by the Saudi National Root-CA as governed by the Saudi National Root-CA Certificate Policy (Saudi National Root-CA CP).

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

- Securely managing the core infrastructure that supports the PKI, and
- Issuing, managing, revoking and renewing certificates to CAs , other peer cross certified CAs internationally and supportive administrative roles for the PKI operations

in accordance with the requirements of the Saudi National Root-CA CP.

Saudi National Root CA issued Digital Certificates provide a high level of assurance in accordance with Section 1.1 of the Saudi National Root-CA CP.

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

1.1.1 CERTIFICATE POLICY

Certificates issued in accordance with the Saudi National Root-CA CP will assert the Object Identifier (OID) that is set within the Saudi National Root-CA CP.

1.1.2 RELATIONSHIP BETWEEN THE CP AND THE CPS

This CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by the Saudi National Root-CA as governed by the Saudi National Root-CA CP and related documents which describe NIC requirements, and use of certificates.

1.1.3 INTERACTION WITH OTHER PKI'S

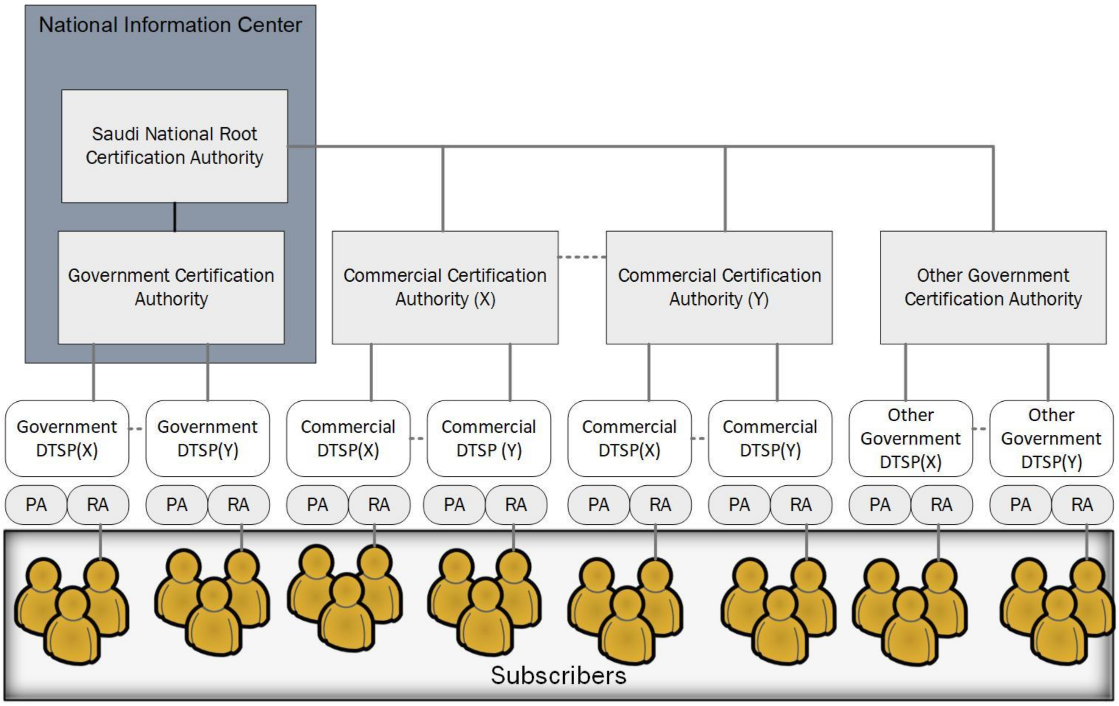
NIC will set the requirements for entities, within and outside the Kingdom of Saudi Arabia, wishing to cross-certify with the Saudi National Root-CA. Cross-certification will only be permitted after approval from NIC.

1.1.4 SCOPE

This CPS applies to all certificates issued by the Saudi National Root-CA, other approved CAs, cross certified peer CAs internationally and supportive functions for the Saudi National Root-CA operations within Saudi National PKI.

The Saudi National PKI hierarchy consists of a self-signed Root CA (Saudi National Root-CA), maintained and operated by NIC in an offline environment, and several CAs for online issuance and management of Subscriber certificates through DTSPs. The Saudi National Root-CA issues and manages the approved CAs certificates and associated Authority Revocation List (ARL). It may also cross-certify with other peer CAs upon approval of NIC.

The approved CAs issue Subscriber (human, device or entity) certificates and certificates for its RAs and LRAs. Saudi National PKI hierarchy is as shown in the following figure.


National Information Center
Saudi National Root Certification Authority
Government Certification Authority
Commercial Certification Authority (X)
Commercial Certification Authority (Y)
Other Government Certification Authority
Government DTSP(X)
Government DTSP(Y)
Commercial DTSP(X)
Commercial DTSP (Y)
Commercial DTSP(X)
Commercial DTSP(Y)
Other Government DTSP(X)
Other Government DTSP(Y)
PA
RA
Subscribers

1.2 DOCUMENT NAME AND IDENTIFICATION

The Object Identifier (OID) assigned to this CPS is 2.16.682.1.101.5000.1.2.1.2. Please refer to the latest OID Allocation document available on https://ca.nic.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 DGA

The Digital Government Authority (DGA) is the regulator of Digital Trust Services in the Kingdom of Saudi Arabia.

1.3.2 NIC

NIC approves and maintains the practices, policies and procedures under which the entire Saudi National PKI operates. NIC is also responsible for the governance and enforcement of the policies. Its specific tasks include:

- Policy Approval Process: Development, approval and revision of all NIC policies, in particular the Saudi National Root-CA CP and CPS;
- Approving Digital Trust Service Providers: Establishment and administration of the requirements and procedures for entities wishing to become a DTSP. It is also responsible for approving DTSP applications;
- Approval of Cross-Certification: It is also responsible for approving cross-certification applications;
- Dispute Resolution: Arbitration on all disputes arising out of or related to the activities of the NIC;

- Governance: Maintaining participant compliance with the requirements of NIC including overseeing the audit of the Saudi National Root-CA, approved CAs, DTSs and NIC-PKIC. NIC is responsible for the determination and execution of remedies and actions for non-compliance and unacceptable risk;
- Interoperability Practices: Coordinating legal, policy, technical, and business practices and issues related to NIC interoperability with other Certificate Authorities; and
- Standards: Establishing compliance with baseline standards for the Saudi National Root-CA and cross certified CAs.

1.3.3 SAUDI NATIONAL ROOT CERTIFICATION AUTHORITY

The Saudi National Root-CA is the trust anchor for the entire Saudi National PKI. It remains offline in a highly secured environment and is activated to perform the following operations:

- The generation, issuance and publication of cross certified CA certificates;
- Revocation of cross certified CA Certificates;
- Re-key of the Saudi National Root-CA and NIC approved CA signing keys;
- Performance of all aspects of the services, operations and infrastructure related to Certificates issued under the Saudi National Root-CA CP, in accordance with the requirements, representations, and warranties of the Saudi National Root-CA CP and this CPS; and
- Certificate signing of approved entities wishing to cross certify with NIC at the national and international level.

1.3.4 CA POLICY AUTHORITY

The CA Policy Authority (PA) is responsible for the governance of a CA. CA Policy Authority members are appointed by NIC. Its jurisdiction is confined to the operations of a CA and its subordinate participants. Its tasks include:

- Enforcement of the CA CP, PDS and CPS and the relevant Operations Policies and Procedures;
- Ensure compliance of issued certificates by the CA with the requirements of NIC;
- Resolution of disputes between entities operating under it;
- Customize Subscriber Agreement, Relying Party Agreement and Registration Authority based on the CA's specific business requirements; and
- Act as liaison with NIC.

1.3.5 CERTIFICATION AUTHORITY

CAs operating under the Saudi National Root-CA shall perform the following functions:

- Issue certificates in accordance with the CA CP and the DTSP Agreement to:
  - Registration Authorities;
  - Local Registration Authorities;
  - Individuals;
  - Government or Business entities;

  - Responsible persons within organizations, in connection with the Identification and Authentication of Devices (Computing and Communications equipment).
- Provide Relying Parties with access to:
  - Certificate information published in a directory;
  - The public keys associated with certificates that are listed in the directory.
- CAs can issue the following:
  - Confidentiality Certificates;
  - Signature Certificates;
  - Authentication Certificates.
- Publish issued certificates in a nominated LDAP directory;
- Investigate compromises and suspected compromises of private keys at any subordinate level they deem warranted in their chain of trust;
- Publish revocation information in a directory;
- Conduct regular internal security audits;
- Conduct compliance reviews of its RAs, LRAs and Relying Parties; and
- Assist in audits conducted by or on behalf of NIC.

1.3.6 REGISTRATION AUTHORITY

Registration Authority (RA) is the entity that collects and verifies each subscriber's identity and the information that is to be entered into the subscriber's public key certificate. RA performs its function in accordance with the Saudi National Root-CA CP, this CPS and any documented Operations Policies and Procedures. RA performs following functions:

- Registers Subscribers including:
  - Processing certificate application information and documentation as part of the identification and authentication process;
  - Confirming that an applicant's name does not appear in their list of compromised subscribers;
  - Optional generation of key pairs and/or issuance of tokens for applicants.
- Submit applicant's public keys together with digitally signed certification requests to their CA;
- Process requests from Subscribers for the renewal or revocation of their certificates and generate digitally signed renewal or revocation requests to their CA; and
- Overall control over the registration process including the activities of any Trusted Agent or Local Registration Authority (LRA).

1.3.7 SUBSCRIBERS

Subscribers are individuals, organizations or devices to whom certificates are issued. Subscribers are bound by the conditions of use of certificates as contained in the Subscribers Agreement. Subscribers are not automatically Relying Parties unless specified in the Subscriber Agreement. In general, the subscriber asserts that he or she uses the key and certificate in accordance with the applicable CP. Depending upon the DTSP and respective CP and CPS, Subscribers are defined as either:

- End users (Residents, business or government employees);
- Entities (Organizations, government departments); or
- Devices (Computing and communications equipment such as Trusted Servers or Firewalls).

Subscribers perform the following tasks:

- Provide complete, full and accurate information during the application process for the issuance of a certificate;
- Comply with all procedures required in connection with the Identification and Authentication requirements applicable to the certificate issued;
- Review any certificate issued to them and ensure the correctness of all information set out therein and notify the DTSP or the LRA/TA immediately in the event that the certificate contains any inaccuracies;
- Request the issue, renewal and if appropriate, revocation of their certificates;
- Comply fully with their respective certificate application process including, without limitation, the provision of all required information and documentation;
- Secure their private key(s); and
- Use their keys and certificates in a manner and for a purpose consistent with the requirements of the applicable CP and the Subscribers Agreement.

1.3.8 RELYING PARTIES

A Relying Party is the entity that relies on the validity of the binding of the subscriber’s name to a public key. The Relying Party is responsible for checking the validity of the certificate by examining the appropriate certificate status information, using validation services provided by the CAs as further described in respective CPS. A Relying Party’s right to rely on a certificate issued under applicable CPS, requirements for reliance, and limitations thereon, are governed by the terms of the issuing CA CP and the Relying Party Agreement.

The Relying Party bears the legal consequences of any failure to comply with the obligations set out in the Relying Party Agreement. The Relying Party must not use or rely on the certificates beyond the limitations set forth in the Relying Party Agreement and it must not rely on the certificate unless the verification process has deemed the certificate as valid and trustworthy.

Relying Parties shall use the Saudi National PKI, and rely on a certificate that has been issued under the issuing CA CP if:

- The certificate has been used for the purpose for which it has been issued, as described in the respective CP and applicable Subscriber Agreement;
- The Relying Party has verified the validity of the digital certificate, using procedures described in the Relying Party Agreement; and
- The Relying Party has accepted and agreed to the Relying Party Agreement at the time of relying on the certificate; it shall be deemed to have done so by relying on the certificate.

1.3.9 *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*

Certificates issued under Saudi National PKI are used to support the secure exchange of electronic information, secure e-Government and electronic commerce that may be employed for the following general uses:

- Confidentiality: where the certificate is used to encrypt messages between two subscribers;
- Signature: where the certificate is used to assure the message integrity, bind the signer to the document or transaction and provide Non-repudiation; or
- Authentication: where certificates are used to identify/authenticate the subscriber to services and application.

Each DTSP shall determine the types of transactions supported by the certificates it issues to its participants, which may include the following:

- Government to Government;
- Government to Citizen;
- Business to Government;
- Business to Business;
- Business to Citizen;
- Citizen to Citizen; or
- A subset of the above transaction types.

The uses for which a certificate is suitable, restricted or prohibited are set out in the appropriate DTSP, Subscriber or Relying Party Agreements to which the specific certificate relates.

Appropriate use of certificates includes any transaction involving government entities of the Kingdom of Saudi Arabia or transactions specifically approved by government entities. NIC does not prohibit the use of certificates by non-government entities or individuals for non-government transactions. The participants in the following transactions do so without access or recourse to the NIC:

- Business to Business;
- Business to Citizen;
- Citizen to Citizen; or
- A subset of the above transaction types.

1.4.2 *PROHIBITED CERTIFICATE USES*

Certificates issued under this CPS are not 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 NIC shall not be liable for any claims arising from such use.

1.5 POLICY ADMINISTRATION

1.5.1 *ORGANIZATION ADMINISTERING THE DOCUMENT*

This CPS is administered by NIC and is based on policies established under the Saudi National Root-CA CP.

1.5.2 *CONTACT PERSON*

Enquiries relating to this CPS shall be directed at:

Email: pki@nic.gov.sa

Telephone: +966 11 8081013

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

1.5.3 *PERSON DETERMINING CPS SUITABILITY FOR THE POLICY*

The approval of this CPS as being in conformance with the Saudi National Root-CA CP is performed by NIC in accordance with policies and procedures specified by NIC.

NIC is the entity responsible for determining the conformance of this CPS to the Saudi National Root-CA CP.

1.5.4 *CPS APPROVAL PROCEDURES*

The CPS shall be effective upon approval by NIC.

1.6 DEFINITIONS AND ACRONYMS

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

NIC issued certificates and certificate revocation lists (CRLs) will be published in repositories. The repositories shall be directories that provide access through the Lightweight Directory Access Protocol (LDAP) and through HTTP. Repositories may reside on dedicated directories, or may be part of a separate directory that serves broader purposes than just supporting the PKI.

The NIC operates repositories to support operations on a 24x7 basis and replicates issued certificates, CRLs and Authority Revocation Lists (ARLs) to additional repositories in order to enhance the overall performance and provide high availability for its validation services.

2.1.1 REPOSITORY OBLIGATIONS

The repository capabilities that Saudi National Root-CA and approved CAs deploy shall include:

- LDAP Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP, version 3) or Hypertext Transfer Protocol (HTTP);
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CPS; and
- Access control mechanisms when needed to protect repository availability and information.

The approved CAs shall post Subscriber certificates and CRLs to a LDAP directory and HTTP-based Web server. The NIC has instituted access controls, including strong authentication of authorized Relying Parties, to promote consistent access to CA-issued certificates and CRLs and to prevent modification or deletion of information.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

The Saudi National Root-CA publishes Root CA Certificate, approved CAs certificates, other peer CAs cross certificates and CRLs in the repository at https://ca.nic.gov.sa.

CAs maintain repositories that allow Relying Parties to make on-line enquiries regarding revocation and other certificate status information. CAs shall provide Relying Parties with information on how to find the appropriate repository to check certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the appropriate OCSP responder.

The CAs repositories shall contain several PKI-related elements:

- Subscriber’s certificates: approved CAs will decide on directory access restrictions to prevent misuse and unauthorized harvesting of information;
- CA certificates: CA certificates shall be made publicly available; and
- CRLs: CRLs shall be made publicly available to allow relying parties to verify the status of certificates.

2.2.2 PUBLICATION OF CA INFORMATION

NIC provides support for the on-line publication of information that is deemed public information.

The CP and CPS shall be made available to all Saudi National PKI Participants at NIC website https://ca.nic.gov.sa . This web site is the only source for up-to-date documentation and Saudi National Root-CA reserves the right to publish newer versions of the documentation without prior notice.

Additionally, Saudi National Root-CA publishes an approved, current and digitally signed version of the Saudi National Root-CA PDS.

The NIC Public LDAP directory and the NIC website https://ca.nic.gov.sa are the only authoritative sources for:

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

The NIC may also publish information concerning DTSP's as necessary to support their use and operation.

2.2.3 REPOSITORY STANDARDS AND INTEROPERABILITY

Repository information is stored using technology that supports the following industry standards and schema:

- LDAP v3 operations
- LDAP search filters
- LDAP v3 intelligent referral
- Relevant LDAP v3 RFCs, including RFC 1274, 1558, 1777, 1778, 1959, 2195, 2222, 2247, 2251, 2252, 2253, 2254, 2255, 2256, 2279, 2307, 2377, 2829, 2830, and 3377
- DSML (Directory Service Markup Language) v2
- X.509 digital certificates
- HTTP

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificates are published promptly following their generation and issue. CRL information shall be published as set in section 4.9.7.

The OCSP responder will immediately report a certificate that has been revoked as set in section 4.9.9.

This CPS and any subsequent changes should be made available to the Saudi National PKI authorized participants within two weeks of approval by NIC.

2.4 ACCESS CONTROLS ON REPOSITORIES

Certificates and CRLs in the repositories are available to Relying Parties on a 24X7 basis, subject to routine maintenance. The NIC protects 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 the NIC shall prevent unauthorized persons from adding, deleting or modifying repository entries. Access restrictions are implemented on directory search to prevent misuse and unauthorized harvesting of information.

Entities utilizing DTSP certificate validation services are required to agree to a Relying Party Agreement as a condition to accessing certificate status information.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

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

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

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

The subject name contained in a CA certificate must be meaningful in the sense that the 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

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

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

3.1.5 UNIQUENESS OF NAMES

The Saudi National Root-CA shall ensure that the set of names is unambiguous. NIC shall reject a Licence application of the CA in case where the name cannot sufficiently distinguish the new CA applicant from an existing CAs Distinguished Name. The name shall conform to X.500 standards for name uniqueness.

3.1.6 RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

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

NIC will resolve name collisions involving NIC issued certificates in accordance with the NIC Operations Policies and Procedures.

NIC shall have the right to revoke a Certificate upon receipt of a properly authenticated order from PA, an RA, an arbitrator or court of competent jurisdiction requiring the revocation of a Certificate or Certificates containing a Subject name in dispute.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

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 PKCS #10 or another cryptographically equivalent demonstration. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pre-generated keys are placed on smart cards.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

Entities wishing to join the the Saudi National PKI hierarchy or cross certify with the Saudi National Root-CA shall be authenticated in accordance with NIC specifications and requirements. In all cases, NIC personnel will verify information in the application, authenticity of the requesting representative and the representative's authorization to act in the name of the requesting CA.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

Root CA does not issue end-entity certificates.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Information that is not verified will not be included in certificates issued by the Saudi National Root-CA under Saudi National PKI.

3.2.5 CRITERIA FOR INTEROPERATION

The Saudi National Root-CA and other approved CAs will be designed, implemented, and operated using the following standards to facilitate interoperation:

- The CA will issue X.509 certificates and CRLs in accordance with the profiles listed in the respective CP;
- The CA will operate a LDAP directory in full compliance with the latest LDAP schema and interface specification; and
- The CA will operate an OCSP Responder that fully complies with Internet RFC 6960.

Any CA wishing to interoperate, join or cross certify with the Saudi National Root-CA, shall adhere to the requirements specified in Section 3.2.5 of the Saudi National Root-CA CP.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

For re-key of a CA key pair, an authorized representative of the CA shall request re-key prior to the expiration of the CA key pair. Detailed re-key procedure is specified in 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 PA shall provide sufficient information before NIC initiates generation of the CA certificate.

3.4 Identification and Authentication for Revocation Request

Prior to the revocation of a Certificate, a CA shall verify that the revocation has been requested by an entity authorized to request revocation.

Acceptable procedures for authenticating the revocation requests include:

- Having the Subscriber submit a Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record;
- Receiving a message from a Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked;
- Communication with the requesting entity to provide reasonable assurances that the person or organization requesting revocation is who they claim to be. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

The requests to revoke a CA Certificate shall be authenticated by NIC personnel to ensure that the revocation has in fact been requested by the CA.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 APPLICATION

This section specifies the requirements for initial application for certificate issuance by the Saudi National Root-CA.

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

~~For CA licensing process an application must be submitted and approved by DGA. NIC shall proceed with the process upon DGA approval. In addition, for commercial CAs, a license must be obtained from the DGA after an application is approved by the DGA.~~

An authorised representative from CA organization shall submit the application and follow the CA licensing process.

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

4.1.2 ENROLMENT PROCESS AND RESPONSIBILITIES

An entity wishing to become a CA shall agree to the terms of the applicable Agreement as part of the application process. An RA shall agree to the terms of the RA Agreement as part of its certificate application process. CA and RA applicants shall provide their credentials to demonstrate their identity and provide contact information during the contracting process.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

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

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

NIC shall decide on the acceptance or rejection of a CA certificate application or a cross-certification request 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 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 DGA (for commercial CAs), and gets final approval from NIC.

4.3.2 *Notification to Subscriber by the CA of Issuance of Certificate*

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

4.4 Certificate Acceptance

Certificate acceptance is governed by the Agreements set out between the Saudi National Root-CA and approved CAs. 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.

4.4.1 *Conduct Constituting Certificate Acceptance*

Certificate acceptance is governed by and should comply with the practices described in and any requirements imposed by the Saudi National Root-CA CP and the relevant agreements under which the certificate is being issued. The use of a certificate or the reliance on a certificate signifies acceptance by that person of the terms and conditions of the appropriate agreement.

4.4.2 *Publication of the Certificate by the CA*

Certificate generated is published in the repository at https://ca.nic.gov.sa by the Saudi National Root-CA.

4.4.3 *Notification of Certificate Issuance by the CA to other Entities*

NIC, DGA and CA PA shall be notified 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, Root CA CP, this CPS and applicable laws. The CAs shall protect their Private Keys from access by any other party and shall notify NIC upon the compromise of the private key or any reasonable suspicion of compromise.

Use of the private key corresponding to the public key in the certificate shall only be permitted once the Subscriber has agreed to and signed the Subscriber agreement and accepted the certificate. The certificate shall be used lawfully in accordance with the applicable Agreement, the terms of the Saudi National Root-CA CP and this CPS. Certificate use must be consistent with the Key Usage field extensions included in the certificate.

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of the private key following revocation of the associate certificate.

4.5.2 *Relying Party Public Key and Certificate Usage*

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

- The appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CPS. The Relying Party is solely responsible for assessing the appropriateness of the use of a Certificate;
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate; and
- The status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by a Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

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

4.6 CERTIFICATE RENEWAL

Certificate renewal is the issuance of a new certificate without changing the public key or any other information in the certificate. Certification renewal is not supported for NIC issued certificates.

4.7 CERTIFICATE RE-KEY

Certificate Re-Key refers to the issuance of a new certificate that has a new, different public key (corresponding to a new, different private key), the existing Subscriber information, a different serial number and may be assigned a different validity period to the original certificate.

4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to update the certificate to maintain continuity of Certificate usage.

The CA PA will determine maximum allowed time a subscriber key may be used and will publish this decision in an appropriate way. Dependent on that timeframe, re-key will be initiated for a subscriber instead of a certificate renewal.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

In accordance with the conditions specified in previous section, 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 as defined in Saudi National Root-CA Operations Policy.

Update procedures ensure that the person or organization seeking to update an end-user Subscriber Certificate is in fact the Subscriber, a sponsor of a device or a representative of an entity. One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrolment information a Challenge Phrase (or the equivalent thereof). Upon update of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's re-enrolment information, and the enrolment information (including contact information) has not changed, a new Certificate is automatically issued.

After updating in this fashion, an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in Section 3.2.3 of this CPS for the authentication of an original Certificate Application.

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 in accordance with Section 4.4.1 of this CPS.

4.7.6 Publication of the Re-keyed Certificate by the CA

The re-keyed certificate is published in the appropriate repository.

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. RA's may receive notification of the issuance of certificates they approve.

4.8 Certificate Modification

Certificate modification is not supported for NIC-issued certificates.

4.9 Certificate Revocation and Suspension

The Saudi National Root-CA publishes a revocation notice on its Web Site if any issuing CA certificate is revoked.

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 RCA, those of any applicable CP, PDS and CPS or any other applicable Agreements;

- NIC or DGA suspects or determines that revocation of a Certificate is in the best interest of the integrity of the NIC;
- 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/or 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.

An investigation into the need for revocation will take place by which the following is carried out:

- Validate the need for revocation and obtaining authorization for the revocation;
- On completion of investigation into need for revocation, either certificate is revoked or reinstated with certificate status as valid;
- On revocation of a certificate:
  - The reason for the revocation is recorded;
  - A CRL (Certificate Revocation List) is immediately generated and published on the Saudi National Root-CA Directory and/or specified as revoked by an OCSP Responder;
  - The Saudi National Root-CA publishes in a prominent manner a suspension notice on its Web Site about CA to which the certificate refers;
  - The CA, to which the certificate refers, notifies its End Users of the revocation;
  - A notice containing the Certificate details and the date and time of revocation is issued to the CA authorized representative.

4.9.2 WHO CAN REQUEST REVOCATION

The following entities can request revocation of a Certificate:

- NIC can request the revocation of any certificates issued by any CA participating in the Saudi National PKI in the interests of nation;
- DGA can request the revocation of any certificates issued by any CA participating in the Saudi National PKI in the interests of nation;

- The authorized signatory of the CA; or
- A legal, judicial or regulatory agency in Saudi Arabia.

The authority to revoke the Saudi National Root certificate rests with NIC.

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

4.9.3 PROCEDURE FOR REVOCATION REQUEST

When a revocation is requested by an authorized signatory of a CA, the revocation request may be submitted through:

- A digitally signed revocation request verifiable with the public key contained in the certificate to which the request refers to and performance of an off-line request; or
- A certificate revocation request physically delivered to Root CA by an appropriately authorized person.

NIC may also initiate CA Certificate revocation request if it deems it necessary.

In processing a revocation request, the Saudi National Root-CA will:

- Revoke the certificate on the Saudi National Root-CA, record the reason for the revocation, and maintain relevant documentation;
- Generate immediately a CRL (Certificate Revocation List) from the Saudi National Root-CA;
- Withdraw the certificate from the Saudi National Root-CA web site;
- Issue a notice containing the Certificate details and the date and time of revocation to the certificate subscriber;
- Notify the CA that its certificate has been revoked under the provisions of the e Transactions Law; and
- Publish the revocation on the Repository.

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

Saudi National Root-CA shall process authorized revocation requests within 24 hours.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

Relying Parties are required to comply with the Relying Party Agreement requirements for signature validation, which prescribe how certificate status information is to be obtained and used. One method by which Relying Parties may check Certificate status is by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties may meet this requirement either by checking Certificate status using the applicable repository or by using OCSP (if available). CAs shall provide Relying Parties with information on how to find the appropriate CRL, repository, or OCSP responder (where available) to check for revocation status.

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

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

The OCSP Responder will be configured with certificates with a sufficient validity period to mitigate risks associated with OCSP Responder key compromise.

4.9.10 Online Revocation Checking Requirements

The Saudi National Root-CA may make its Certificate status information available through an OCSP responder. Where a CA provides an OCSP service, the timeliness of certificate status information supplied by the OCSP Responder shall be as specified in Section 4.9.5. The OCSP Responder will be configured to process requests that comply with the format specified in OCSP profile section.

4.9.11 Other Forms of Revocation Advertisements Available

The Saudi National Root-CA will not provide other forms of revocation advertisements.

4.9.12 Special Requirements Related To Key Compromise

If NIC 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, NIC will immediately declare a disaster and invoke NIC PKI business continuity plan. NIC 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 DTSPs, subscribers and potential relying parties that there has been a key compromise, and (4) generate new CA key pair as per NIC Operations Policies and Procedures.

4.9.13 Circumstances for Suspension

If Saudi National Root-CA suspects that a certificate should be revoked for one of the circumstances described in Section 4.9.1, the Saudi National Root-CA may suspend the suspected certificate.

Pending completion of any inquiry ordered by NIC, no CA whose certificate has been suspended will issue any certificates during this suspension. The suspension of certificates issued by the Saudi National Root may occur immediately if the suspension has been requested by the authorized signatory of the licensed CA or after an investigation has taken place.

4.9.14 Who can Request Suspension

The following entities can request suspension of a Certificate:

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

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

When a suspension is requested by an authorized signatory of a CA, the procedure for processing suspension requests is as follows:

- The request is submitted to the Saudi National Root-CA via digitally or manually signed;
- Authenticate all requests for the temporary revocation of certificates;
- Record and retain all information pertaining to such requests, including a statement as to the action taken by the Saudi National Root-CA;
- The entity’s certificate is suspended;
- Publish notice of any temporary revocation of a certificate in its CRL or OCSP server;
- Root CA should announce in its web site the suspension of the CSP certificate; and
- The Saudi National Root-CA should notify the entity once their certificates have been suspended.

4.9.16 LIMITS ON SUSPENSION PERIOD

The maximum period for which a Certificate can be suspended will be defined by NIC but shall not exceed ninety (90) days.

4.9.17 CIRCUMSTANCES FOR TERMINATING THE SUSPENDED CERTIFICATES

When the entity which requested the suspension of the certificate is satisfied that the circumstances for suspension are no longer valid, the suspension shall be terminated. Once reactivated, the certificate validity period will be subject to the initial validity period.

If the entity which requested the suspension of the certificate is satisfied that the circumstances for suspension are valid, the certificate will be revoked.

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 relevant certificate, the reason for unsuspension and a method to 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 before a certificate is unsuspended.

4.10 CERTIFICATE STATUS SERVICES

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

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW AND RECOVERY

4.12.1 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

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

Saudi National Root-CA does not offer key escrow services.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

No stipulation.

5. Facility, Management and Operational Controls

5.1 Physical Controls

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

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

- NIC-PKIC systems are installed in a secure facility that is isolated from outside networks, with all access controlled;
- The NIC-PKIC 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 NIC-PKIC uses include:

- Perimeter alarms;
- Closed circuit television;
- Two-factor authentication using Biometrics, PIN number and physical keys;
- Faraday cage are in place to prevent electromagnetic radiation emissions for all Root CA operations;
- Human guards; and
- All the Networking and systems components including the certification components are installed in secure Room inside a safe.

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

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

5.1.1 Site Location and Construction

The CA systems are located in a dedicated high-security facility. The security of the location and operating premises has been implemented so that access of unauthorized persons has been prevented by use of seven layers of physical security. The site location, when combined with the physical security protection mechanisms such as guards, surveillance videos provides robust protection against unauthorized access to the CA equipment.

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 checks of the facility housing the CAs equipment shall be on a regular basis. The NIC-PKIC 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 NIC 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 by the NIC to fill these roles will be extraordinarily responsible. The functions performed in these roles form the basis of trust for the entire NIC. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

At a minimum, the following roles are established:

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

CA Master:

The CA Master role is responsible for:

- Installation, configuration, and maintenance of the CA hardware and software;
- Starting and stopping CA services;
- Generating and backing up CA keys;
- Backing up and restoring the database; and
- Establishing and maintaining CA system accounts (Security Officer).

Master users do not issue certificates to Subscribers.

CA Administrator:

The CA Administrator role is responsible for:

- Installation, configuration, and maintenance of the CA hardware and software;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters; and
- Generating and backing up CA keys.

Administrators do not issue certificates to Subscribers.

CA Officer:

The CA Officer role is responsible for:

- Verifying the accuracy of information included in certificates;
- Executing the issuance of certificates; and
- Executing the revocation of certificates.

CA Auditor:

The CA Auditor role is responsible for:

- Reviewing, maintaining, and archiving audit logs; and
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with this CPS.

CA Operator:

The CA Operator role is responsible for:

- Daily operation and maintenance of the system equipment;
- System backup and recovery operations; and
- Storage media renewal.

5.2.2 *Number of Persons Required per Task*

The NIC-PKIC 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 NIC PKI Trusted Roles document. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over the system operation.

The NIC will ensure that no single individual may gain access to CA private keys. At a minimum two individuals, using split-knowledge and ownership techniques such as twin password's and tokens, must perform any CA system start-up, CA system shutdown, key backup or key recovery operation.

5.2.3 *Identification and Authentication for Each Role*

Persons filling trusted roles shall undergo an appropriate security screening procedure before they can start their duties.

5.2.4 *Roles Requiring Separation of Duties*

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means.

Individual CA personnel are specifically designated to the four roles defined in Section 5.2.1 of this CPS and NIC PKI Trusted Roles document. Individuals who assume a CA Officer role may not assume a CA Administrator or CA Auditor role. An individual assigned a CA Auditor role shall not perform any other trusted role. No individual shall be assigned more than one identity.

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 NIC PKI Trusted Roles document and NIC PKI 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

NIC conducts background investigations for all NIC 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 NIC will provide proper training to all personnel performing duties with respect to the operation of the Saudi National Root-CA and CA Repositories and OCSP Responder. Training shall cover the following aspects;

- PKI and Information Security concepts;
- All PKI software versions in use on the CA, Repositories and OCSP Responder systems;
- All NIC PKI duties that the personnel are expected to perform;
- Disaster recovery and business continuity procedures; and
- The meaning and effect of the Saudi National Root-CA CP and this CPS.

Documentation of all personnel who received training and the level of training completed shall be maintained by the NIC.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

Individuals performing PKI roles are made aware of changes in the CA, Repository and OCSP Responder operation. Any significant change to the operations will necessitate a training awareness plan, and the execution of such plan is documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

The Saudi National Root-CA will take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA, Repositories and OCSP Responder that are not authorized in the CP, this CPS, or other procedures.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

When NIC uses a contractor to perform services, there will be adequate procedures explicitly stated objectives and supervision in place to ensure that any subcontractors perform in accordance with the Saudi National Root-CA CP, this CPS, the NIC PKI Security Policy as well as the requirements stipulated in the contractor's contract of employment. Contractor personnel employed to perform functions pertaining to the CA shall be subject to the same sanctions as other personnel as set forth in previous section.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

NIC provides sufficient documentation to its personnel in order for them to perform their job responsibilities competently and satisfactorily.

5.4 AUDIT LOGGING PROCEDURES

NIC will implement and maintain Trustworthy Systems to preserve an audit trail for material events and for key life cycle management, including key generation, backup, storage, recovery, destruction and management of cryptographic devices, the CA and OCSP Responder.

NIC systems shall generate audit log files for all events relating to the security of the CA, RA and OCSP Responder. All security audit logs are retained and made available for review during compliance audits. The security audit logs for each auditable event defined in this section are maintained in accordance with Section 5.4.3 which governs the retention period for security audit data.

5.4.1 TYPES OF EVENTS RECORDED

NIC enables all security auditing capabilities of the Root and DTSP CA's, the OCSP Responder, operating system and PKI applications during installation.

NIC shall ensure recording in audit log files all events relating to the security of the CA system hosted in NIC-PKIC, 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 DTSP Agreements.

5.4.2 FREQUENCY OF PROCESSING LOG

Audit logs are required to be processed in accordance with the NIC PKI 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 protects the electronic audit log system and audit information captured electronically or manually

- Read access to the journal information is granted to personnel requiring this access as part of their duties;

- Only authorized roles can obtain access; and
- The journal is stored in the database and access to the database is protected against unauthorized access by the CA application and through special security measures on the operating system level.

5.4.5 *AUDIT LOG BACKUP PROCEDURES*

The journal is an integral part of the CA database and is therefore part of the daily backup. The entire database is encrypted on the disk as well as on the backup media.

5.4.6 *AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)*

The audit log or journal is an integral part of the CA software.

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

5.4.7 *NOTIFICATION TO EVENT-CAUSING SUBJECT*

Event-causing subject are not notified.

5.4.8 *VULNERABILITY ASSESSMENTS*

The NIC performs routine assessments of security controls. This self-assessment includes periodic review of: error logs on systems, storage of assets and records, security audit data for alerts or irregularities, alarm logs, access logs, incident reports, and audit log analysis. 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, technology.

Based on the Risk Assessment exercise, NIC 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.

Apart from this NIC-PKIC is constantly (24x7) monitored, and all attempts to gain unauthorized access to any of the services are logged and analyzed.

The NIC performs third party vulnerability assessment for hosted CA infrastructure at least once a year.

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 Saudi National Root-CA.

- Audit logs generated by the PKI CA software;
- DTSP agreements;
- Records pertaining to identification and authentication information;
- 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;
- Documents identifying all personnel who received CA related training and the level of training completed;
- The Saudi National Root-CA shall archive any necessary keys and passwords for a period of time sufficient to support the functionalities; and
- The CA shall make these audit logs available to its Qualified Auditor upon request.

The CA shall make these audit logs available to its Qualified Auditor upon request.

5.5.2 *RETENTION PERIOD FOR ARCHIVE*

The NIC-PKIS's minimum retention period for archive data is established at ten years.

Applications needed to process the archive data shall also be maintained for the archival retention period.

Prior to the end of the archive retention period, the Saudi National Root-CA and CAs shall provide archived data and the applications necessary to read the archives to a NIC approved archival facility, which shall retain the applications necessary to read this archived data.

5.5.3 *PROTECTION OF ARCHIVE*

The archive is protected using a combination of physical security and procedural security means stored in a location other than the NIC-PKIC site. Only authorized personnel are permitted to review the archive data. Archive data and media are physically protected during transit and at the archive storage site using physical security means. The archived data stored at the secondary site provides adequate protection from environmental threats such as temperature, humidity and magnetism.

5.5.4 *ARCHIVE BACKUP PROCEDURES*

Only one copy of the archive is maintained. In other words, archive itself is not backed up. As specified in the NIC 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.

System logs are automatically time stamped and systems use a dedicated time server to maintain synchronized time.

The system time of all servers is synchronized with the time source of the NIC Time-Stamping Authority or another official time source. NIC time source is synchronised with the GPS clock. Further, there is a procedure in place that checks and corrects drift in the real time clock.

5.5.6 *Archive Collection System (Internal or External)*

The type of Archive Collection System, whether internal or external, is specified in the NIC Archival Policy.

5.5.7 *Procedures to Obtain and Verify Archive Information*

Information on how the archive information is created, verified, packaged, transmitted and stored is detailed in the NIC Archival Policy. These policies and procedures are updated and augmented to reflect the legal and best practice requirements for managing and protecting electronic records.

5.6 Key Changeover

To minimize risk from compromise of a CA's private signing key, the key will be changed often. Once changed, only the new key will be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs that contain certificates signed with that key, only then the old key may be retained. If the old key is retained, it shall be protected just as the new key.

The CA keys are automatically renewed at the frequency defined by section 6.3.2 of these Certificate Policies.

5.7 Compromise and Disaster Recovery

5.7.1 *Incident and Compromise Handling Procedures*

In the event that a potential hacking attempt or other form of compromise to a CA occurs, it shall perform an investigation to determine the degree of potential damage. NIC-PKIC shall notify NIC and PAs of CAs if any of the following occur;

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

CA PA shall be notified if any of the following cases occur;

- A CA certificate revocation is planned;
- Any incident preventing a CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

The above measures will allow participants to protect their interests as Relying Parties.

CAs shall re-establish operational capabilities as quickly as possible in accordance with the procedures set forth in the respective CA and NIC Operations Policies and Procedures.

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

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to the NIC management and the NIC's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, NIC's key compromise or related Business Continuity procedures will be enacted.

5.7.3 PRIVATE KEY COMPROMISE PROCEDURES

In the event of compromise, the recovery shall be as per CA private key compromise recovery procedures detailed in the Saudi National Root-CA Operations Policy.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

NIC 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 NIC critical PKI infrastructure equipment at the primary site (NIC-PKIC) have built-in hardware fault-tolerance, and configured to be highly available with auto-failover switching. NIC 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.

NIC 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 NIC 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.

NIC 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.

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

NIC 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. NIC Business Continuity Policy contains further details.

5.8 CA OR RA TERMINATION

5.8.1 CA TERMINATION

The termination of a CA is subject to the terms of the Agreement. Prior to termination, CA's shall provide archived data to NIC approved archival facility.

In the event that a CA ceases operation, it must notify its Subscribers in writing at least one month before termination of operations and arrange for the continued retention of the CA's keys and information. It must also notify in writing at least one month before termination of operations, all CA's with whom it is cross-certified.

The CA archives should be retained in the manner and for the time indicated in Section 5.5.2. NIC 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. NIC 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

CA key pair generation is performed by multiple trusted NIC personnel using trustworthy systems and processes that provide for the security and required cryptographic strength for the generated keys. For the Saudi National Root-CA and other CAs, the Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with the requirements of the NIC as mentioned in NIC Root-CA Key Generation Ceremony Policy. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by NIC management.

6.1.2 Private Key Delivery to Subscriber

No subscriber certificates are issued from the Saudi National Root-CA.

6.1.3 Public Key Delivery to Certificate Issuer

No subscriber certificates are issued from the Saudi National Root-CA.

6.1.4 CA Public Key Delivery to Relying Parties

Acceptable methods are specified in Section 6.1.4 of the Saudi National Root-CA CP.

Relying parties can download the issuing CA certificate from the NIC website by using the PKCS#7 format. When a subscriber receives the certificate, the issuing CA public key is included. Also included is the complete chain of certificates of the hierarchical Saudi National Root-CA containing all public keys that are part of the trust chain.

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. All FIPS-approved signature algorithms shall be considered acceptable.

All certificates issued shall use at least 2048 bit RSA, with Secure Hash Algorithm version (SHA-256) in accordance with FIPS 186-2 or equivalent. TLS or another protocol providing similar security to accomplish any of the requirements of this CPS shall use triple-DES or AES (minimum 128 bit key strength) for the symmetric key, and at least 2048 bit RSA or equivalent for asymmetric keys.

The current NIC standard for minimum key sizes is;

1. Root CA Key Pair:	2048 bits
2. Other CA Key Pair:	2048 bits
3. Subscriber Key Pairs:	2048 bits
4. OCSP Key Pair:	2048 bits

6.1.6 *Public Key Parameters Generation and Quality Checking*

The HSM pseudo-random number generator is validated by NIST. Primality testing of prime numbers shall be done according to ANSI X9.80 standards and/or multiple rounds of Rabin-Millar. However, no subscriber certificates are issued from the Saudi National Root-CA except for the supportive administrative roles.

6.1.7 *Key Usage Purposes*

The signing key of Saudi National Root-CA and other CAs are the only keys permitted for signing certificates and CRLs and have the keyCertSign and CRLSign key usage bit set.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 *Cryptographic Module Standards and Controls*

Cryptographic modules employed in the NIC shall comply with FIPS-PUB 140-2 “Security Requirements for Cryptographic Modules”. The Hardware Security Modules (HSM’s) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the CA keys.

6.2.2 *Private Key Multi-Person Control*

Multi-person control of CA private key is achieved using an “m-of-n” split key knowledge scheme. Saudi National Root-CA keys can only be accessed on the physical and logical level by adhering to '2 out of 4' control, meaning that 2 of the 4 persons are present.

6.2.3 *Private Key Escrow*

CA private keys are never escrowed.

6.2.4 *Private Key Backup*

The NIC-PKIC uses the mechanisms provided by the HSM’s to back up the Saudi National Root-CA and other CA signing keys. The associated access tokens will be divided and stored in both the backup and DR sites to provide for both local and offsite backup of the CA keys.

The CA signing keys are backed up under the same multi-person control as the original signature keys. The recovery requires that 2 out of 4 persons be present in order to gain physical and logical access.

Saudi National Root-CA private keys that are physically transported from one facility to another follows NIC Cryptographic Devices Lifecycle Management Policy and Procedure.

Saudi National Root-CA hardware containing CA private keys, and associated activation materials, are transported in a physically secure environment by authorized personnel as per the NIC PKI Trusted Roles, using multiple person controls, and using sealed tamper evident packaging.

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

6.2.5 PRIVATE KEY ARCHIVAL

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

Saudi National Root-CA maintains 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

The cryptographic modules implemented by the NIC are validated to FIPS 140-2 Level 3, ensuring that the CA keys can only be output in encrypted form.

The Saudi National Root-CA keys can be cloned from the master hardware cryptographic module to other hardware cryptographic modules so that they can be recovered if a major catastrophe destroys the productive set of keys.

The Saudi National Root-CA keys migrated from one secure cryptographic device to another, other than for the purposes of routine backup and restoration are completed in a physically secure environment by those in NIC PKI Trusted Roles under multi-person control (m of n).

The hardware and software tools used during the Saudi National Root-CA key migration process are tested by the CA prior to the migration event. The Saudi National Root-CA keys migration event follows change management process as per the documented script and complete process is logged.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The CA private keys are stored on FIPS 140-2 Level 3 validated modules in encrypted form.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

A CA’s private key shall be activated by a threshold number of stakeholders, 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. A deactivated key shall be kept encrypted or otherwise secured within the cryptographic module, to prevent unauthorized access.

6.2.9 METHODS OF DEACTIVATING PRIVATE KEY

A CA’s private keys shall be deactivated by a threshold number of shareholders, as defined in Saudi National Root-CA Operations Policy, by removing their secure media.

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 are destroyed as per NIC Cryptographic Devices Lifecycle Management Policy and Procedure.

6.2.11 CRYPTOGRAPHIC MODULE RATING

The CA private keys are stored on FIPS 140-2 Level 3 validated modules. Cryptographic hardware issued to Subscribers is FIPS 140-2 Level 2 compliant.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

The CA and Subscriber certificates are backed up and archived as part of the Saudi National Root-CA and CA routine backup procedures.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

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

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

At the end of a certificates lifecycle, if it has not been renewed it will expire and the Subscriber will have to reinitiate a registration process. The processes for disabling the Subscribers account are defined in the NIC Operations Policies and Procedures.

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

The CA cryptographic module activation data will be generated locally at the time of key generation by personnel in the trusted role and responsible for controlling the activation data.

6.4.2 ACTIVATION DATA PROTECTION

Written CA cryptographic module activation data is placed into tamper evident packages which are then stored within secure containers in a highly secured environment inside the NIC-PKIC.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

The CA servers are protected by external firewalls that filter out all unwanted traffic. Additionally, the CA systems are hardened and equipped with a high-security operating system. SA access to the system is granted only over secure and restricted protocols using strong public-key authentication.

NIC-PKIC has implemented layered security approach to ensure the security and integrity of the computers used to run the Saudi National Root-CA and other CA software. The following controls ensure the security of NIC-operated computer systems:

- Hardened operating system;
- Software packages are only installed from a trusted software repository;
- Minimal network connectivity;
- Authentication and authorization for all functions;
- Strong authentication and role-based access control for all vital functions;
- Disk and file encryption for all relevant data; and
- Proactive patch management.

6.5.2 COMPUTER SECURITY RATING

The 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 maintains controls to provide reasonable assurance that CA systems development, maintenance activities, patching, and changes to CA systems are documented, tested, authorized, and properly implemented to maintain CA system integrity.

The NIC-PKIC employs the following System Development controls;

- The NIC-PKIC uses shrink-wrapped software from product vendors. Where the NIC-PKIC uses its own software products, these have been developed using documented software development processes;
- Hardware and software procured to operate the CA is purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device);
- CA hardware and software configurations are dedicated to performing one task: the CA. No other applications, hardware devices, network connections, or component software that is not part of the CA operation will be installed;
- The NIC-PKIC undertakes all reasonable precautions to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA are procured. The CA hardware and software is scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates are purchased in the same manner as original equipment, and are installed by trusted and trained personnel according to policies and procedures established in NIC's Operations Policies and Procedures.

6.6.2 SECURITY MANAGEMENT CONTROLS

The Saudi National Root-CA maintains controls to provide reasonable assurance that changes to CA systems operating systems, databases, applications, network devices, and hardware

are documented, tested, authorized, and properly implemented to maintain CA system integrity.

System security management shall be controlled by the privileges assigned to system accounts and by the trusted roles described in Section 5.2.1, according to appropriate standards (e.g. BS ISO/IEC 27001:2013 or similar).

The configuration of the CA system as well as any modifications and upgrades must be documented and controlled in accordance with the NIC Change Management Policy. A formal configuration management methodology must be used for installation, ongoing maintenance and evolution of the CA system. No upgrades shall be permitted without prior offline testing and assessment, and regular backups must be taken.

6.6.3 LIFE CYCLE SECURITY CONTROLS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The Saudi National Root-CA is operated as an Offline CA and does not connected to any network.

The Repository and OCSP Responder infrastructure are connected to the Internet in such a way so as to provide continuous service to Relying Parties. Redundancy is provided through the Repository and network infrastructure to prevent loss of service even during maintenance and backup procedures.

The NIC-PKIC uses a network design of multiple security layers making use of several security technologies including firewalls, intrusion prevention systems, anti-virus, anti-spyware software to protect network access to on-line CA's, Repository and OCSP Responder equipment. These technologies limit the services allowed to and from the on-line CA's, Repository and OCSP Responder equipment to those authorized to have such access.

The NIC-PKIC's network security controls are designed to protect the NIC infrastructure against network attacks. All unused network ports and services are turned off. 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 will deny all but the necessary services to the PKI equipment.

6.8 TIME STAMPING

Certificates, CRLs, and other revocation database entries contain time and date information. System logs are automatically time stamped and systems use a dedicated time server to maintain synchronized time.

Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's Certificate;
- Revocation of a Subscriber's Certificate;
- Posting of CRL updates;
- OCSP or other CSA response.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

This section contains the rules and guidelines followed by this Saudi National Root-CA in populating X.509 certificates and CRL extensions. The certificate profiles are covered in Appendix-A of the Saudi National Root-CA CP.

7.1.1 VERSION NUMBERS

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

7.1.2 CERTIFICATE EXTENSIONS

The CA certificates shall comply with profiles covered in Appendix-A of the Saudi National Root-CA CP.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

Saudi National Root-CA and subordinate CAs 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 and other CA 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

Name must be meaningful and must be associated with the DTSP CA. Names are constrained to be unique Distinguished names (DN).

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

CA and Subscriber Certificates issued under this CPS 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

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

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

CAs 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

The NIC will only process OCSP requests and responses 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

NIC is responsible for overseeing the audit of the Saudi National Root-CA and other CAs. NIC shall supervise audits of the operations of the Saudi National Root-CA and other CA's to ensure that they are in compliance with the applicable CP and CPS. The audits shall include the review of all relevant documents maintained by the CA regarding their operations within the NIC, applicable agreements, and other related NIC Operations Policies and Procedures.

8.1 Frequency or Circumstances of Assessments

The Saudi National Root-CA and other approved CAs shall be subjected to periodic compliance audits which are no less frequent than once a year. NIC also performing internal audit at least a quarterly basis against a randomly selected sample for monitor adherence and service quality. Moreover, NIC may require ad-hoc compliance audits of Saudi National Root-CA and any CA's operation 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.

NIC will appoint Qualified Auditor from a panel provided by DGA, who shall be Licensed WebTrust Practitioner to perform such compliance audits as a primary responsibility.

8.3 Assessor's Relationship to Assessed Entity

The chosen auditor will be an independent third party and aside from the audit function, 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 NIC with a compliance report highlighting any discrepancies.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If irregularities are found by the auditor, NIC shall be informed in writing immediately. The Saudi National Root-CA must submit a report to the auditors or directly to NIC, as to any remedial action the Saudi National Root-CA will take in response to the identified deficiencies. This report shall include a time for completion to be approved by NIC.

Where Saudi National Root-CA fails to take appropriate action in response to the identified deficiencies, NIC shall be informed and shall take the appropriate action, according to the severity of the deficiencies which shall include:

- Noting the deficiencies but allowing the Saudi National Root-CA to continue operations until the next planned, or newly scheduled, inspection;
- Suspending the CA's certificate; or
- Revoking the CA's certificate.

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 NIC and communicated to DGA of the final outcome.

The Saudi National Root-CA shall make the Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, an explanatory letter is to be signed by the Qualified Auditor.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

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

9.1.2 CERTIFICATE ACCESS FEES

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

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

Non-governmental CAs shall maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. This insurance requirement does not apply to governmental entities.

The NIC and Governmental CAs are, at a minimum, covered by existing government insurance provisions. Details of coverage are specified in the applicable agreements.

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 DTSP.

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 NIC may be made publicly available at the discretion of NIC and/or a Policy Authority. Specific confidentiality requirements for business information are defined in the NIC Privacy Policy and the associated Subscriber, Relying Party and DTSP agreements.

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

Any corporate or personal information held by the NIC-PKIC, CAs, RAs, or LRAs 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 NIC Privacy policy.

(i) Registration Information

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

- Certificate applications, whether approved or not;
- Certificate information collected as part of the registration process;
- Completed Subscriber Agreements;
- Any information requested by the NIC when it receives an application from a third party to operate as a Cross-Certified CA.

(ii) Certificate Information

The reasons for a certificate being suspended or revoked is considered confidential information, with the sole exception of the revocation of the Saudi National Root-CA, a Cross-Certified CA, an RA or a LRA due to;

- The compromise of their private key, in which case a disclosure may be made that the private key has been compromised;
- The termination of the Saudi National Root-CA, a Cross-Certified CA, an RA or a LRA, in which case prior disclosure of the termination may be given.

(iii) PKI Documentation

The NIC PKI Document Control Policy specifies which documents are considered to be 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 NIC, Privacy Policy, NIC Operations Policies and Procedures and applicable Agreements. Such as:

1. Certificate Information

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

2. PKI Documentation

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

- Saudi National Root-CA CP;
- Saudi National Root-CA CPS;
- Saudi National Root-CA PDS;
- NIC PKI Dispute Resolution Policy; and
- NIC Privacy Policy.

3. Disclosure of Certificate Revocation Information

Certificate revocation information is provided via the CRL in the repositories and via the OCSP Responders.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

The NIC shall protect the confidential information it possesses in accordance with its NIC Privacy Policy and applicable laws and Agreements.

9.4 PRIVACY OF PERSONAL INFORMATION

Any personal identifying information collected by a CA shall be protected in accordance with the NIC Privacy Policy. The NIC will use reasonable measures to protect personal identifying information from disclosure to any third party.

9.4.1 PRIVACY PLAN

The NIC shall protect the confidential information it possesses in accordance with the NIC Privacy Policy.

9.4.2 INFORMATION TREATED AS PRIVATE

Any information about Subscribers that is not publicly available through the content of the issued certificate, repository and online CRL's is treated as private.

9.4.3 INFORMATION NOT DEEMED PRIVATE

Information appearing in Subscriber Certificates such as the name, organization affiliation and pubic key will not be deemed private.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

Access to NIC held private information shall be restricted to those with an official need-to-know basis in order to perform their official duties.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

Unless otherwise stated in this CPS, the Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

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

9.4.7 *Other Information Disclosure Circumstances*

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

9.5 Intellectual Property Rights

The allocation of Intellectual Property Rights among NIC participants are governed by the applicable agreements.

9.6 Representations and Warranties

9.6.1 *Saudi National Root-CA Representations and Warranties*

- The NIC represents and warrants that it shall conform to the stipulations of the Saudi National Root-CA CP and this CPS, including: Providing the operational infrastructure and certification services;
- Making reasonable efforts to ensure it conducts an efficient and trustworthy operation. “Reasonable efforts” include but are not limited to operating in compliance with;
- Documented NIC Operations Policies and Procedures;
- Within applicable Saudi Law and regulations;
- Maintaining this CPS and enforcing the practices described within it and in all relevant collateral documentation;
- Publishing approved CA certificates in the repositories;
- Investigating any suspected compromise which may threaten the integrity of the NIC;
- Revoking approved CA certificates in accordance with Section 4.9 and posting such revoked certificates in a ARL;
- Promptly notifying a CA in the event it initiates revocation of their CA certificate;
- Conducting compliance audits of the Saudi National Root-CA operations;
- Use of Saudi National Root-CA private signing key only to sign certificates and CRLs and for no other purpose;
- Institute procedures to ensure CA personnel associated with PKI roles (e.g. PKI Master User; PKI Officers, and PKI Administrators) are accountable for actions they perform and ensure evidence is available to link any action to the person performing such action;
- 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 issued certificates, 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.

9.6.2 CA's Representations and Warranties

CAs in performing their functions will operate their certification services in accordance with;

- The Agreement;
- The CA CP;
- The CA CPS;
- The CA PDS;
- The Saudi National Root-CA CP;
- This CPS;
- The Saudi National Root-CA PDS;
- Documented NIC Operations Policies and Procedures; and
- Applicable Saudi Laws and regulations.

The CAs shall

- 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 Saudi National Root-CA issued certificates and CRLs;
- Use the Hardware Security Modules (HSM's) for keys generation that 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

RA's discharge their obligations in accordance with the practices outlined in overview of this CPS, the NIC CP and the RA Agreement.

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 DTSPs;
- Notify the DTSP 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
- Upon termination of Subscriber Agreement, revocation or expiration of the Subscriber Certificate, immediately cease use 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;
- Ensuring 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
- Determining that such Certificate provides adequate assurances for its intended use.

9.7 DISCLAIMERS OF WARRANTIES

NIC, 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 a DTSP CA or other Subordinate entity, any digital signature backed by such certificates, and any products provided by the NIC. The NIC 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, DTSPs are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by DTSPs or Saudi National Root-CA;
- Subscribers to compensate a Relying Party which incurs a loss as a result of the Subscribers breach of Subscriber’s 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 Saudi National 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 DTSPs shall indemnify, defend and hold harmless:

- NIC, its CA PA, officers, employees, agents, consultants, and subsidiaries from any and all claims, damages, costs (including, without limitation, attorneys’ fees), judgments, awards or liability;
- The DTSP’s own employees, arising from any of the DTSP’s operations and activities as a DTSP , of any entity or services subordinated or outsourced by the DTSP, and
- Any parties relying on the DTSP’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

This CPS shall be effective upon approval by NIC.

9.10.2 TERMINATION

This CPS, as amended from time to time, shall remain in force until it is replaced by a new version.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this CPS, all NIC 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

All communication between NIC, NIC-PKIC and cross certified CAs shall be in writing or via digitally signed communication. If in writing, the communication shall be signed on the appropriate organization letterhead. If electronic, a Digital Signature shall be made using a private key whose corresponding public key is in compliance with the Saudi National Root-CA CP.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

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

9.12.2 NOTIFICATION MECHANISM AND PERIOD

NIC reserve the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URL's, and changes to contact information. NIC's decision to designate amendments as material or non-material shall be at NIC's sole discretion.

Any changes to this CPS shall be made and available within two weeks from approval by NIC.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

The policy OID shall only change pursuant to a decision from NIC.

9.13 DISPUTE RESOLUTION PROVISIONS

Any dispute arising out of or related to the digital certificates issued by the NIC shall initially be submitted to voluntary mediation. If mediation is not successful, then the dispute will be resolved by binding arbitration, in accordance with NIC PKI Dispute Resolution Policy.

9.13.1 DISPUTE RESOLUTION POLICY

NIC PKI Dispute Resolution Policy is applicable to all participants of the NIC.

All CAs will ensure that any agreements they enter into with Relying Parties, Subscribers or other Certificate Authorities will include details of the NIC PKI Dispute Resolution Policy.

9.14 GOVERNING LAW

This CPS will be governed and construed in accordance with the laws of the Kingdom of Saudi Arabia.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to national, state, local and foreign laws, rules and regulation, 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 the Saudi National Root-CA CP or any of its rights or duties under the Saudi National Root-CA CP, without the prior written consent of NIC.

9.16.3 SEVERABILITY

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

9.16.4 ENFORCEMENT (ATTORNEY FEES 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 Kingdom of Saudi Arabia.

9.16.5 FORCE MAJEURE

The NIC shall not be in default or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms of this CPS or the Saudi National Root-CA CP or any other related agreement due to any causes beyond its reasonable control, which causes include, without limitation, acts of God, riots and insurrections, terrorist activities, war, accidents, fire, strikes and other labour difficulties, embargoes, judicial action specifically preventing the operation of the NIC, lack of or inability to obtain energy, or utilities, or acts of civil or military authorities.

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.

Nothing contained in this CPS shall be deemed to constitute either the NIC, or any of its subcontractors, agents, officers, suppliers, employees, partners, principals, or CA PA to be a partner, Affiliate, trustee, of any Relying Party or any third party, or to create any fiduciary relationship between the NIC and any Relying party, or any third party, for any purpose whatsoever.

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

9.17.2 ADMINISTRATIVE PROCESSES

No Stipulation.