NIC GOVERNMENT-CA 2

CERTIFICATION PRACTICE STATEMENT

Document Classification:

Public

Version Number: 1.2

Issue Date: May 22, 2023

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 Government Certification Authority (Government-CA 2). In particular, this CPS establishes the processes and procedures the Government Certification Authority (Government-CA 2) follows to:

- Issue NIC compliant certificates to Subscribers,
- Manage certificate life cycle;
- Operate the Directory; and
- Operate the OCSP Responder.

The Government-CA 2 is owned by the Saudi Data and AI Authority (SDAIA). Government-CA 2 is a Certification Authority under the Saudi National Root-CA. This is achieved by the Saudi National Root-CA issuing a digitally signed CA Certificate that authenticates the Public Key of the Government-CA 2. The Government-CA 2 is responsible for issuing and managing Digital Certificates to Government employees, Citizens, organisation entities, non-human subscribers (like Servers and Network Devices) within the Government domain, through Digital Trust Service Providers (DTSPs) within the framework.

The Government-CA 2 is hosted in the National Information Center – PKI Center (NIC-PKIC) which is responsible for managing Government-CA 2 operations as per the agreed service levels.

This CPS complies with the Saudi National PKI Policy and in line with Internet Request for Comment (RFC) 3647 [RFC 3647].

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

1.1 OVERVIEW

This Certification Practice Statement (CPS) establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by the Government-CA 2 as governed by the Government-CA 2 Certificate Policy (Government-CA 2 CP).

More specifically, this CPS describes the practices that the Government-CA 2 employs for:

- Securely managing the core infrastructure that supports the PKI hosted at NIC-PKIC, and
- Issuing, managing, revoking and renewing certificates,

in accordance with the requirements of the Government-CA 2 CP.

The certificate types supported by Government-CA 2 under Saudi National PKI framework are covered in Appendix A of the Government-CA 2 Certificate Policy document. This defines the requirements and criteria for issuance and management of PKI certificates asserting distinct Levels of Assurance as advice to subscriber and any Relying Party.

Any use of or reference to this CPS outside the context of the Government-CA 2 and Saudi National PKI is completely at the using party’s risk. The terms and provisions of the

Government-CA 2 CPS shall be interpreted under and governed by the Government-CA 2 CP and NIC PKI Operations Policies and Procedures.

It is the responsibility of all parties applying for or using a Digital Certificate issued under Government-CA 2 CP, to read this CPS and the PKI Disclosure Statement (PDS) to understand the practices established for the lifecycle management of the Certificates issued by the Government-CA 2.

1.1.1 CERTIFICATE POLICY

X.509 certificates issued by the Government-CA 2 to subscribers will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party (RP) to decide whether a Certificate is trusted for a particular purpose. Subscriber Certificates issued by the Government-CA 2 will identify the applicable policy in the certificate Policies extension by including applicable OID(s).

1.1.2 RELATIONSHIP BETWEEN THE CP AND THE CPS

This CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by Government-CA 2 as governed by the Government-CA 2 CP and related documents which describe NIC requirements and use of Certificates.

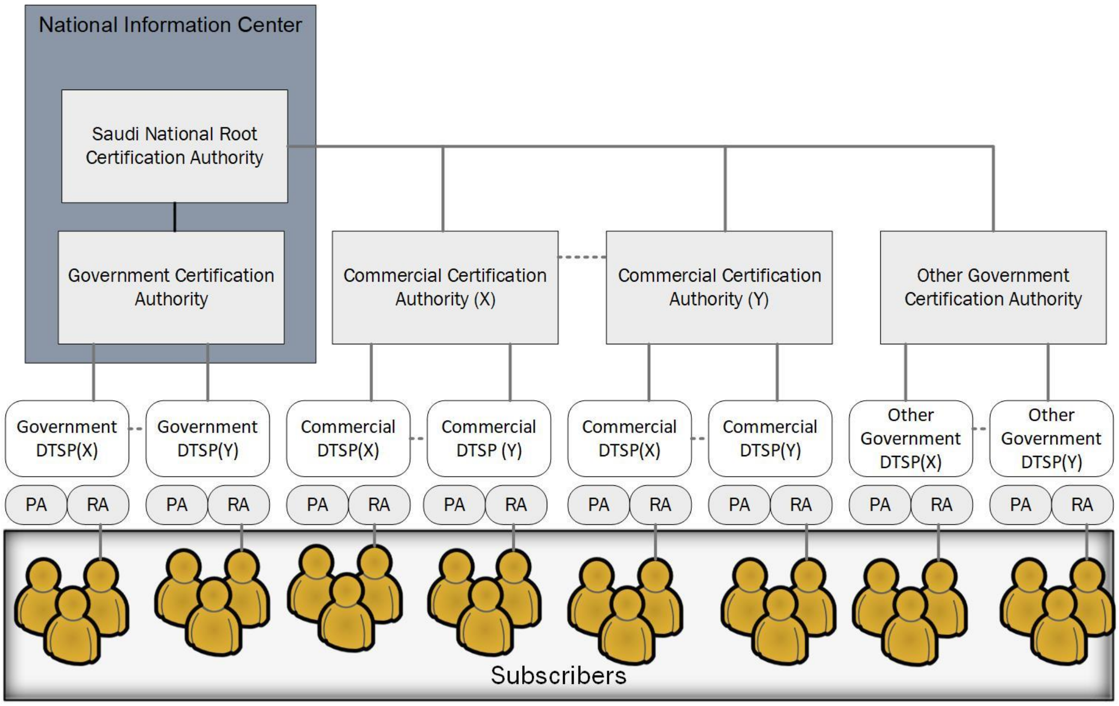
1.1.3 INTERACTION WITH OTHER PKIS

NIC will decide on issues related to cross-certification with other Certification Authorities.

1.1.4 SCOPE

This CPS applies to all certificates issued by the Government-CA 2.

The Government-CA 2 is a subordinate CA in the Saudi National PKI hierarchy, maintained and operated by NIC in an online environment for the issuance and management of Subscriber certificates and revocation lists. More specifically the Government-CA 2 issues end-user certificates and certificates for its DTSPs. The following figure shows the Government-CA 2 in the Saudi National PKI hierarchy.


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

This document is the Government-CA 2 Certification Practice Statement (CPS), and is identified by the object identifier (OID):

OID: 2.16.682.1.101.5000.1.3.1.2.2

Please refer to the latest NIC OID Allocation document available on https://ca.nic.gov.sa.

1.3 PKI Participants

The following are roles relevant to the administration and operation of the Government-CA 2 under the Government-CA 2-CP.

1.3.1 Certification Authorities

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

The Government-CA 2 operating under the Saudi National Root-CA shall perform the following functions:

- Issue certificates in accordance with Government-CA 2 CP, this CPS and the DTSP Agreement to:
  - Registration Authorities;
  - Individuals within government agencies as directed by the respective DTSP;
  - Government entities as directed by the relevant PA; and
  - Responsible persons within organizations, in connection with the Identification and Authentication of Devices (Computing and Communications equipment).
- Manage certificate life cycles;
- Provide Relying Parties with access to:
  - Certificate information published in a directory; and
  - The public keys associated with certificates that are listed in the directory.
- Government-CA 2 will issue the following:
  - Encryption Certificates;
  - Signature Certificates; and
  - Authentication Certificates.
- Publish issued certificates in a selected 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 DTSPs; and
- Assist in audits conducted by or on behalf of NIC.

1.3.2 Registration Authorities

Government-CA 2, subject to the approval of NIC, shall designate specific DTSPs which in turn appoint RAs to perform the Subscriber Identification and Authentication and Certificate request and revocation functions defined in this CPS and related documents.

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

- Process Certificate application requests in accordance with the Government-CA 2 CP, CPS and applicable RA Agreement, and other policies and procedures with regard to the Certificates issued;
- Maintain and process all supporting documentation related to the Certificate application process;
- Process Certificate Revocation requests in accordance with Government-CA 2 CP and CPS, applicable RA Agreement, and other relevant operational policies and procedures with respect to the Certificates issued. Without limitation to the generality of the foregoing, the RA shall request the revocation of any Certificate that it has approved for issuance according to the conditions described later in section 4.9.1;

- Comply with the provisions of its RA Agreement and the provisions of the Government-CA 2 CP and CPS including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements; and
- Follow NIC PKI Privacy policy in accordance with Government-CA 2 CP and CPS and applicable RA Agreement.

1.3.3 SUBSCRIBERS

Subscribers are individuals (end users), and entities (organizations) 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 Government-CA 2 CP. Under the Government-CA 2 CP and this CPS and depending upon the DTSP, Subscribers are defined as either:

- End users (Government employees, Citizens, and associates); or
- Entities (Government departments);

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 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 Government-CA 2 CP, this CPS and the Subscribers Agreement.

1.3.4 SUBJECTS

A Subject is the entity named or identified in a certificate issued to an individual (end user) or entity (organization) and who/which holds or controls a private key corresponding to the pubic key listed in the Certificate.

1.3.5 RELYING PARTIES

A Relying Party is the entity that relies on the validity of the binding of the subscriber’s identity to a public key. The Relying Party is responsible for checking the validity of the certificate by examining the appropriate certificate status information, using validation services provided by the Government-CA 2 as further described in this CPS. A Relying Party’s right to rely on a certificate issued under this CPS, requirements for reliance, and limitations thereon, are governed by the terms of the Government-CA 2 CP and the Relying Party Agreement.

Relying Parties shall use the Saudi National PKI, and rely on a certificate that has been issued under the Government-CA 2 CP and this CPS if:

- The certificate has been used for the purpose for which it has been issued, as described in the Government-CA 2 CP and applicable Subscriber Agreement;
- The Relying Party has verified the validity of the digital certificate, using procedures described in the Relying Party Agreement;
- The Relying Party has accepted and agreed to the Relying Party Agreement at the time of relying on the certificate; it shall be deemed to have done so by relying on the certificate; and
- The relying party accepts in totality, the certificate policy applicable to the certificate, which can be identified by reference of the certificate policy OID mentioned in the certificate.

1.3.6 OTHER PARTICIPANTS

1.3.6.1 GOVERNMENT-CA 2 POLICY AUTHORITY (GOVERNMENT-CA 2 PA)

Government-CA 2 Policy Authority (Government-CA 2 PA) is responsible for the governance of the Government-CA 2. Its members are appointed by NIC and may include members from Government DTSPs. Its tasks include:

- Ensuring the operation of the Government-CA 2 comply with the requirements of the Government-CA 2 CP, PDS, CPS and NIC PKI Operations Policies and Procedures;
- Review and approve the Subscriber Agreement, Relying Party Agreement and other related Agreements based on the Government-CA 2's specific business requirements;
- Seeking resolution of disputes between participants operating in its domain;
- Establishing and implementing its own CP, PDS and CPS in conjunction with the Saudi National PKI Policy Document; and
- Act as liaison with NIC.

1.3.6.2 DIGITAL TRUST SERVICE PROVIDER (DTSP)

An entity which issues and manages digital certificates, electronic signature tools and methods and any other associated services, which operates with or without its own physical certification authority (CA).

The DTSP is owned by an organization which is approved by Government-CA 2 PA and NIC to be remotely connected to the Government-CA 2 to facilitate certificate life cycle management to its own class of subscribers.

The DTSP comprise of Policy Administrator (PA) and Registration Authority (RA) including Local Registration Authority (LRA) if needed.

1.3.6.3 POLICY ADMINISTRATOR (PA)

Policy Administrator (PA) is responsible for the governance of the DTSP. These Policy Administrators are located at various Government DTSPs. Its tasks include:

- Ensuring DTSP operations complying with Government-CA 2 CP requirements;

- Ensuring RA operations complying with Government-CA 2 CP and RA security requirements;
- Conduct compliance reviews of its RAs;
- Assist in audits conducted by or on behalf of NIC;
- Establishing and implementing policies and procedures as required by Government-CA 2 and NIC; and
- Act as liaison with Government-CA 2 and NIC.

1.3.6.4 TRUST AGENT

Trusted Agents (TAs) can perform the identity proofing duties of an RA when authorized to do so by a PA. TAs are obligated to operate in accordance with the TA Agreement, Government-CA 2 CP, CPS and NIC PKI Operations Policies and Procedures. The primary responsibility of a TA is to examine and confirm according to the applicable DTSP procedures, that a DTSP Applicant's identity is authentic.

1.3.6.5 DEVICE SPONSOR

The Device Sponsor shall serve as the representative of a Device to a DTSP in order to register the device as a Subscriber with the Government-CA 2. The requirements for device Sponsors in the Government-CA 2 are set forth under 3.2.3.2.

1.3.6.6 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 Government-CA 2 may make their Certificate status information available through an OCSP responder in addition to any other mechanisms they wish to employ. The Government-CA 2 shall publish status information for the certificates it issues in a Certificate Revocation List (CRL).

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The Government-CA 2 may issue some or all of the following types of certificates:

- Confidentiality certificates, where the certificate is used for encryption to ensure the confidentiality and secrecy of data;
- Signatures certificates, where the certificate is used to assure the message integrity, bind the signer to the document or transaction and provide Non-repudiation (the elimination of deniability); and
- Authentication certificates, where certificates are used to identify/authenticate the subscriber to services and applications.

The Government-CA 2 issues certificates under this CPS only to those Government end entities who have signed their acceptance of a Subscriber Agreement in the appropriate form and whose application for certificates has been approved by DTSP.

The following certificate assurance levels are supported for end-entity certificates issued by the Government-CA 2. The Government-CA 2 will assess the risk and apply appropriate rating.

Assurance Level	Description and Assurance Level
Low	This level provides little confidence in the accuracy or legitimacy of the claimed identity as it requires no or low assurance of the binding between the identity of the entity named in the certificate and the Subscriber. It is intended for Subscribers handling information of little or no value within minimally secured environments. Identity assertions at this level are appropriate for transactions with minimal consequences to Relying Parties from the registration of a fraudulent identity. Digital certificates at this level require no or low assurance of the binding between the identity of the entity named in the certificate and the Subscriber. The keys and certificates can only be generated in a software security module and be stored in a software form factor. Given the limited assurance provided, a Key Usage of non-repudiation is not permitted, nor are Extended Key Usages of smartcard logon or code signing.
Medium	This level provides medium confidence in the accuracy or legitimacy of the claimed identity. It is intended for Subscribers handling information of medium value within substantially secured environments. Identity assertions at this level are appropriate for transactions with serious (substantial) consequences to Relying Parties from the registration of a fraudulent identity. The keys and certificates at this level can be generated in either a software or hardware security module and can be stored in either a software or hardware form factor. User consent is required each time the private key is activated.
High	This level provides a high confidence in the accuracy or legitimacy of the claimed identity. It is intended for Subscribers handling information of high value within highly secured environments. Identity assertions at this level are appropriate for transactions with catastrophic consequences to Relying Parties from the registration of a fraudulent identity. Digital certificates at this level require very high assurance of the binding between the identity of the entity named in the certificate and the certificate holder. The keys and certificates can only be generated in a hardware security module and can only be stored in a hardware form factor. Authenticated-user’s consent or PIN unlocks are required each time the private key is activated.

1.4.1.1 *CERTIFICATE ISSUED TO EMPLOYEES*

Certificates issued from the Government-CA 2 to the Government employees are normally used by individuals to sign and encrypt e-mail, data and to authenticate to applications (client authentication).

Following are some of the common usage of the certificate:

- Inter-Government Correspondence;
- Information Publication;
- Forms Submission;
- Application work-flow; and
- e-Tendering.

The individual certificate may also be used for other general or specific Government purposes which are not covered explicitly above, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by (1) law of Saudi Arabia, (2) the Government-CA 2 CP and the CPS under which the certificate has been issued and (3) Subscriber's agreement.

1.4.1.2 *CERTIFICATE ISSUED TO ORGANIZATIONAL ENTITY*

Certificates issued to Organizational entities assure the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so. These certificates can be used for the purposes covered under employee certificate in the previous paragraph.

1.4.1.3 *CERTIFICATE ISSUED TO DEVICE*

If the Certificate subject is a device, then the device shall have a sponsor authorized by the device sponsor to apply for a certificate as mentioned in section 3.2.3.2.

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 Government-CA 2 shall not be liable for any claims arising from such use.

1.5 POLICY ADMINISTRATION

1.5.1 *ADMINISTRATION ORGANIZATION*

This CPS is administered by the Government-CA 2 PA and is based on policies established under the Government-CA 2 CP (see section 1.3.1).

1.5.2 CONTACT PERSON

Queries regarding the Government-CA 2 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 Government-CA 2 PA is responsible for approving this CPS and establishing that the Government-CA 2 conforms to the requirements of Government-CA 2 CP in accordance with policies and procedures specified by NIC.

1.5.4 CPS APPROVAL

The CPS shall be effective upon approval by the Government-CA 2 Policy Authority. Procedure for approval and amendments are covered under section 9.12.1 of this CPS.

1.6 DEFINITIONS AND ACRONYMS

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Government-CA 2 issued certificates and certificate revocation lists (CRLs) will be published in repositories. NIC shall operate Repositories to support the Government-CA 2’s operations. 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.

NIC operates repositories to support operations on a 24x7 basis and replicates Government-CA 2 issued certificates, CRLs and Authority Revocation List’s (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 NIC will 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 Government-CA 2 CP; and
- Access control mechanisms when needed to protect repository availability and information.

The Government-CA 2 shall post Subscriber certificates and CRLs to an LDAP directory and an HTTP-based web server. NIC-PKIC has instituted access controls, including strong authentication of authorized Relying Parties, to promote consistent access to Government-CA 2 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 Government-CA 2 maintains repositories that allow Relying Parties to make on-line enquiries regarding revocation and other certificate status information. Government-CA 2 shall be providing 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.

Government-CA 2 repositories shall contain several PKI-related elements:

- Subscriber’s certificates: Government-CA 2 decides on directory access restrictions to prevent misuse and unauthorized harvesting of information;
- CA certificates: CA certificates are made publicly available; and
- CRLs: CRLs are made publicly available to allow relying parties to verify the status of certificates.

Government-CA 2 PA will decide on directory access restrictions to prevent misuse and unauthorized harvesting of information.

2.2.2 Publication of CA Information

The CPS shall be made available to all Government-CA 2 PKI Participants at the NIC website https://ca.nic.gov.sa. This web site is the only source for up-to-date documentation and Government-CA 2 reserves the right to publish newer versions of the documentation without prior notice.

Additionally, Government-CA 2 will publish an approved, current and digitally signed version of its CP and PDS.

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

- All publicly accessible certificates issued by the Government-CA 2; and
- The certificate revocation list (CRL) for Government-CA 2.

2.2.3 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 issuance. CRL publication is in accordance with section 4.9.7 of the Government-CA 2 CP. Other certificate status information is published in accordance with the provisions of this CPS.

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

Updates to this CPS are published in accordance with section 9.12.2 of this CPS.

This CPS and any subsequent changes should be made available to the participants as set forth in section 2.2.2 within two weeks of approval by the Government-CA 2 PA and NIC.

2.4 Access Controls on Repositories

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

The Government-CA 2 will protect repository information not intended for public dissemination or modification through the use of strong authentication, access controls, and an overall Information Security Management System that prevents unauthorized access to information.

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

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

Refer to the equivalent section in the CP.

Details of the certificate are found in Appendix-A of the CP.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

Refer to the equivalent section in the CP.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

Refer to the equivalent section in the CP.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

Refer to the equivalent section in the CP.

3.1.5 UNIQUENESS OF NAMES

Refer to the equivalent section in the CP.

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 Government-CA 2, DTSPs, however, does not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application.

The Government-CA 2 is responsible for ensuring name uniqueness through its DTSPs.

The Government-CA 2 shall have the right to revoke a Certificate upon receipt of a properly authenticated order from NIC, a DTSP, 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. Where a key pair is generated by a CA on behalf of a Subscriber, for example where pre-generated keys are placed on smart card or token before giving it the DTSP has to ensure that the private key is in possession of the right subject.

For Subscribers using centralized signing platform, Signing keys are generated using FIPS 140-2 Level 3 or higher certified hardware security module and stored in an encrypted database on the central storage. Key wrapping is accepted for the centralized signing platform Subscribers. Keys are protected to ensure only the relevant subject has access.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

Entities wishing to join 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 the information in the application, the authenticity of the requesting representative and the representative's authorization to act in the name of the requesting CA.

3.2.3 IDENTITY-PROOFING OF INDIVIDUAL IDENTITY

3.2.3.1 IDENTITY-PROOFING OF END USER SUBSCRIBERS

Government-CA 2 is responsible for the identification and authentication of Subscribers. This process is performed by the DTSPs. The DTSPs will ensure that the applicant's identity information is verified in accordance with Government-CA 2 requirements and standards.

The DTSPs shall act in accordance with this CPS and all Government-CA 2 collateral documentation. In doing so, it will comply with the corresponding practices, procedures and policies described therein.

For collection and verification of information provided by the certificate subscriber applicant DTSPs define process based on the certificate type requirements. The typical verification process could be:

1. Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents;
2. The following will be considered valid identity documents:
   - National ID / passport for citizens;
   - Residence permit / passport for residents.
3. Letter from an authorized party (as prescribed by the DTSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process; and
4. During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics.

Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types.

This section provides the generally applicable verification process for Government-CA 2 issued certificates. Respective verification process applicable to specific certificate types is provided in Appendix-A of the Government-CA 2 CP document, which is mandated.

3.2.3.2 AUTHENTICATION OF INDIVIDUAL IDENTITY

Government-CA 2 is responsible for the identification and authentication of Subscribers. This process is performed by the DTSPs. The DTSPs will ensure that the applicant's identity information is verified in accordance with Government-CA 2 requirements and standards.

The DTSPs shall act in accordance with this CPS and all Government-CA 2 collateral documentation. In doing so, it will comply with the corresponding practices, procedures and policies described therein.

For collection and verification of information provided by the certificate subscriber applicant DTSPs define process based on the certificate type requirements. The typical verification process could be:

5. Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents;
6. The following will be considered valid identity documents:
    - National ID / passport for citizens;
    - Residence permit / passport for residents.
7. Letter from an authorized party (as prescribed by the DTSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process; and
8. During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics.

Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types.

This section provides the generally applicable verification process for Government-CA 2 issued certificates. Respective verification process applicable to specific certificate types is provided in Appendix-A of the Government-CA 2 CP document, which is mandated.

When computing and communication devices (routers, firewalls, servers, etc) are named as certificate subjects the device will have a human sponsor. The Government-CA 2, through the DTSPs, will authenticate the identity of the sponsor applying for the device certificate.

The sponsor is responsible for providing the DTSP with the following registration information;

- Equipment identification (e.g. serial number) or service name (e.g. DNS name);
- Equipment authorizations and attributes (if such information is to be included in the certificate); and
- Contact information to enable the DTSP or the RA to communicate with the sponsor when required.

The DTSP will authenticate the identity of the device sponsor by:

- Performing face-to-face registration of the sponsor, with their identity confirmed in accordance with the requirements of their respective Subscriber Agreement

Where a device sponsor/Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types. The Government-CA 2 may have additional requirements including proof that the device sponsor applying for the device certificate is authorized to apply for a device certificate for that particular device apart from the standard process mentioned above and covered in the respective agreement.

This section provides the generally applicable verification process for Government-CA 2 issued certificates. Respective verification process applicable to specific certificate types is provided in Appendix -A of the Government-CA 2 CP document, which is mandated.

3.2.3.3 AUTHENTICATION OF ORGANIZATIONAL ENTITIES

Whenever a certificate contains an organization name, the identity of the organization and other enrollment information provided by the Certificate applicant is confirmed in accordance with the Government-CA 2's operational policies and procedures.

At a minimum, the Government-CA 2 shall:

- Determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable Saudi government agency or competent authority that confirms the existence of the organization.
- Confirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate applicant certain information about the organization, that the organization has authorized the Certificate application and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so. When a certificate includes the name of an individual as an authorized representative of the Organization, the employment of that individual and his authority to act on behalf of the Organization shall also be confirmed.

Where an Entity certificate has been issued by a Government-CA 2 using the Identity and Authentication process described in this section, the certificate can be used to obtain further NIC-issued certificates without having to undertake another face-to-face registration.

For RA certificate under DTSP the request will contain the following information as a minimum:

- RA Details (Full Name, ID details, email address, phone);
- Requester Organization Information and address;
- Subject of RA (DN) (optional); and
- DTSP Approval;

The request will be supported with an Identity Proof.

NIC Representative will strongly validate the identity of the requestor by ensuring the authenticity of the RA through validating his identity.

This section provides the generally applicable verification process for Government-CA 2 issued certificates. Respective verification process applicable to specific Certificate Types is provided in Appendix-A of the Government-CA 2 CP document, which is mandated.

3.2.3.4 *IDENTITY-PROOFING OF END USER SUBSCRIBERS*

Government-CA 2 is responsible for the identification and authentication of Subscribers. This process is performed by the DTSPs. The DTSPs will ensure that the applicant's identity information is verified in accordance with Government-CA 2 requirements and standards.

The DTSPs shall act in accordance with this CPS and all Government-CA 2 collateral documentation. In doing so, it will comply with the corresponding practices, procedures and policies described therein.

For collection and verification of information provided by the certificate subscriber applicant DTSPs define process based on the certificate type requirements. The typical verification process could be:

9. Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents;
10. The following will be considered valid identity documents:
    - National ID / passport for citizens;
    - Residence permit / passport for residents.
11. Letter from an authorized party (as prescribed by the DTSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process; and
12. During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics.

Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types.

This section provides the generally applicable verification process for Government-CA 2 issued certificates. Respective verification process applicable to specific certificate types is provided in Appendix-A of the Government-CA 2 CP document, which is mandated.

3.2.4 *NON-VERIFIED SUBSCRIBER INFORMATION*

Non-verified information shall not be included in high assurance certificates issued under Government-CA 2, unless specifically mentioned in the Certificate Types under Appendix-A of the Government-CA 2 CP document.

3.2.5 *VALIDATION OF AUTHORITY*

See Section 3.2.2

3.2.6 *CRITERIA OF INTEROPERATION*

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Subscribers are required to obtain new key pairs at least once every three years. (The usage periods for CA and Subscriber private keys are described in section 6.3.2.) During the Re-keying process, the Government-CA 2 will create a new certificate with the same characteristics as the old certificate but with a new and different key pair and serial number. This new certificate may be given a new validity period or use the validity period that appeared in the old certificate.

When it has been less than three (3) years since the time the Subscriber was identified by the RA, the Government-CA 2 will authenticate an electronic request for a new certificate using the currently valid certificate issued to the Subscriber by the Government-CA 2.

Where it has been longer than three (3) years from the time that the Subscriber's identity has been authenticated, then the Subscriber certificate re-key will follow the same procedures as the initial certificate issuance process.

For routine re-key of RA Certificate refer to NIC Level-One CA Operations Policies and Associated Procedures section 8.

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. Details of the procedure covered in Saudi National Root-CA Operations Policy section 11.

3.3.2 Identification and Authentication for Re-key After Revocation

For re-key after revocation, the CA must authenticate the re-key in the same manner as for initial registration as described in Appendix-A of Government-CA 2 CP.

If Government-CA 2 certificate is revoked, an authorized representative of the CA shall provide sufficient information as specified in Saudi National Root CA Operations Policy before NIC initiates re-keying of the Government-CA 2 certificate.

3.4 Identification and Authentication for Revocation Requests

Prior to the revocation of a Certificate, a Government-CA 2 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; or
- Communication with the requesting entity to provide reasonable assurances that the person or organization requesting revocation is who they claim to be. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

If a secure request for revocation is received, the certificate status should be put in Suspend mode, until further verification is carried out.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The DTSP will perform the following steps when an applicant applies for a certificate:

- Establish the applicant's authorization to obtain a certificate;
- Establish and record the identity of the applicant; and
- Transmit to the Government-CA 2 a confirmation that the Applicant has met the authentication requirements and the information which is to appear in the Certificate.

The Government-CA 2 will perform the following steps when it receives the confirmation and certificate information from the DTSP:

- Verify that the transmission is from an authorized DTSP;
- Generate the Certificate relating to that Applicant; and
- Transmits the Certificate to the Applicant and/or to the requesting DTSP.

Communication between the Government-CA 2 and the DTSP are authenticated and protected from modification through the use of digitally signed messages and by requiring the CA and RA to validate the integrity and authenticity of the messages. These communications are transmitted via a secure protocol. Where shared secrets are transmitted electronically, these transmissions are conducted over encrypted channels using cryptographic mechanisms that are commensurate with the strength of the public/private key pair being used. Any out-of-band communications will protect the confidentiality and integrity of the data.

4.1.1 SUBMISSION OF CERTIFICATE APPLICATION

Subscriber certificate applicants, including those applying for a device or entity certificate, will follow the application process specified in section 3.2.3 and the Subscriber Agreement.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

4.1.2.1 SUBSCRIBERS

Subscriber certificate applicants shall agree to the terms of the Subscriber Agreement and undergo an enrollment process consisting of:

- Completing a Certificate Application and providing true and correct information;
- Generating, or arranging to have generated, a key pair;
- Delivering his/her public key to a Government-CA 2; and
- Demonstrating possession of the private key corresponding to the public key delivered to the Government-CA 2, as specified in section 3.2.1 of this CPS.

4.1.2.2 DTSP CERTIFICATES

An entity wishing to become DTSP under the Government-CA 2 shall agree to the terms of the DTSP Agreement as part of the application process. The DTSP applicants shall provide their credentials to demonstrate their identity and contact information during the application process.

All applicants shall agree to the terms and conditions of the applicable Agreement, such as: Subscriber Agreement, Relying Party or RA/LRA/TA Agreement. Identification and Authentication process is described in the CPS under section 3.2.3.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTITY-PROOFING FUNCTIONS

DTSPs shall perform identification and authentication of all required Subscriber information as described in section 3.2.3 of this CPS.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

The DTSP will approve an application for a subscriber certificate if the following criteria are met;

- Successful identification and authentication of all required Subscriber information as described in the Subscribers Agreement and outlined in section 3.2 of this CPS.

The DTSP will reject a certificate application if:

- Identification and authentication of all required Subscriber information as described in the Subscribers Agreement cannot be completed;
- The Subscriber fails to furnish supporting documentation upon request;
- The Subscriber fails to respond to notices within a specified time; or
- The DTSP believes that issuing a certificate to the Subscriber may bring the Government-CA 2 into disrepute.

Policies specific to each certificate type have been detailed in the Certificate Types section in Appendix-A of the Government-CA 2 CP document. It is mandatory to comply with all policies specific to the respective certificate type.

For RA certificate under DTSP, the DTSP shall ensure that its RA which is applying for certification meets the entitlement requirements for RA certification. Detailed procedure is described in NIC Level-One CA Operations Policy section 7.

The application process for DTSPs under Government-CA 2 would be as per the Government DTSP Joining Process and NIC shall decide on the acceptance or rejection of the DTSP application request based on fulfillment of requirements.

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

When the DTSP receives a request for certificate from a Subscriber, the DTSP will:

- Verify the identity of the Subscriber;
- Verify the authority of the requestor and the integrity of the information in the certificate request; and

- Submit the certificate request to the Government-CA 2.

Upon receiving a validated certificate request from DTSP, the Government-CA 2 will create and sign the Subscriber certificate and deliver it to the Subscriber using a secure method.

All authorization and other attribute information received from an applicant are verified before inclusion in the certificate, unless such verification is not required for specific attributes, identifiers, and/or Certificate Types in Appendix-A of the Government-CA 2 CP document.

The Government-CA 2, through its DTSP, is responsible for verifying the data to be included in the Certificate. At a minimum the DTSP will follow the steps described in section 3.2 of the Government-CA 2 CP and this CPS.

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

When DTSPs receive a request for a Certificate, Certificate is not issued before the applicant accepts the terms of a Subscriber Agreement and successfully completes the application form.

Following successfully completion of the registration process, the Government-CA 2 will create and sign the certificate if all certificate requirements have been met and make the certificate available to the subscriber.

4.3.2 NOTIFICATION TO SUBSCRIBER OF CERTIFICATE ISSUANCE

Subscriber certificates shall be issued directly using a controlled process where the Subscriber takes immediate receipt of the certificate. This provides direct notification of certificate issuance.

4.4 CERTIFICATE ACCEPTANCE

Prior to a Subscriber being able to use their Certificate, the registration process deployed by the Government-CA 2 provides the Subscriber with appropriate disclosure and acknowledgement of the Subscriber’s responsibilities defined in the Subscribers Agreement and notifies the Subscriber of the creation and contents of the Certificate.

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Certificate acceptance is governed by the agreements set out between the DTSP and Applicants, any requirements imposed by Government-CA 2 CP and CPS and the relevant agreements under which the certificate is being issued.

The use of a Certificate or the reliance upon a Certificate signifies acceptance by that person of the terms and conditions of the CP and applicable agreements by which they irrevocably agree to be bound.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

Certificates will be published, once accepted, in the appropriate repository as described in section 2.1 of this CPS.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

NIC shall be notified upon the issuance of Government-CA 2 Certificate by the Saudi National Root-CA.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Refer to the equivalent section in the CP.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Refer to the equivalent section in the CP.

4.6 CERTIFICATE RENEWAL

Certificate renewal is the issuance of a new certificate without changing the public key or any other information in the certificate. Certificate renewal is not supported for Government-CA 2 -issued certificates.

CIRCUMSTANCE FOR CERTIFICATE RENEWAL

See section 4.6.

Who may request renewal

See section 4.6.

Processing certificate renewal requests

See section 4.6.

Notification of new certificate issuance to subscriber

See section 4.6.

Conduct constituting acceptance of a renewal certificate

See section 4.6.

Publication of the renewal certificate by the CA

See section 4.6.

4.7 CERTIFICATE RE-KEY

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

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

4.7.1 CIRCUMSTANCES 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.

Manual Certificate re-key may take place after a certificate is revoked and the subscriber information is still accountable. Manual Certificate re-key may also be performed within one-month of certificate expiry, or after certificate expiry.

Automatic updates of managed digital IDs and any or all the certificates constituting the digital ID may be performed on or after reaching 70% of the certificate lifetime.

4.7.2 WHO CAN REQUEST A CERTIFICATE RE-KEY

Certificate re-key may be requested by:

- The Government-CA 2 for its CA certificate;
- A subscriber for his individual certificate;
- A sponsor for a device certificate; or
- An authorized representative for an Organizational Certificate.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

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. Acceptable procedures are through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key.

Other than the above mentioned procedures, an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in section 3.3.1 of this CPS for the authentication of an original Certificate Application.

4.7.4 NOTIFICATION OF 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 Appendix-A and Registration Authority 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, Government-CA 2 does not notify other entities of a re-keyed certificate apart from requesting CSP.

4.8 CERTIFICATE MODIFICATION

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

The Government-CA 2 CP does not support other forms of Certificate modification.

CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

See Section 4.8.

Who may request certificate modification

See Section 4.8.

Processing certificate modification requests

See Section 4.8.

Notification of new certificate issuance to subscriber

See Section 4.8.

Conduct constituting acceptance of modified certificate

See Section 4.8.

Publication of the modified certificate by the CA

See Section 4.8.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

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

The CA and/or DTSP will notify subscribers of certificate revocation or suspension using any of the below methods:

- Access to the CRL in the CA repository
- Email notification to subscriber (Such notification is deemed complete, once the email is sent by NIC to the subscriber's registered email address.)
- Telephonic notification to subscriber

The CA will notify other participants of certificate revocation or suspension through access to the CRL in the CA repository.

4.9.1 CIRCUMSTANCE FOR REVOCATION

Refer to the equivalent section in the CP.

4.9.2 WHO CAN REQUEST REVOCATION

Refer to the equivalent section in the CP.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

The procedure for a revocation request is defined in section 3.4.

Upon revocation, the certificate shall be revoked and placed on a CRL. An up-to-date CRL will be issued in accordance with the stipulations detailed in section 4.9.7 of the Government-CA 2 CPS. Where OCSP services are provided by a CA, the OCSP Responder will be updated within 30 minutes with the status of the revoked certificate.

A CA or DTSP requesting revocation of its CA or RA Certificate is required to communicate the request to the appropriate Policy Authority. The PA or NIC will then authorize the revocation of the Certificate. NIC or a PA may also initiate CA or RA Certificate revocation if it deems necessary. An ARL will be published on the revocation of a CA certificate. For Revocation of RA Certificates refer to NIC Level-One CA Operations Policy section 9.

4.9.4 REVOCATION REQUEST GRACE PERIOD

Revocation request grace period is not permitted once a revocation request has been verified.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

The Government-CA 2 shall process authorized revocation requests within 24 hours.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

Refer to the equivalent section in the CP.

4.9.7 CRL ISSUANCE FREQUENCY

Refer to the equivalent section in the CP.

4.9.8 MAXIMUM LATENCY OF CRLS

Refer to the equivalent section in the CP.

4.9.9 ONLINE REVOCATION CHECKING AVAILABILITY

Government-CA 2 may provide access to an OCSP Responder covering the certificates they issue.

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

Refer to the equivalent section in the CP.

4.9.11 Other Forms of Revocation Advertisements Available

Refer to the equivalent section in the CP.

4.9.12 Special Requirements Re Key Compromise

If NIC discovers, or has a reason to believe, that there has been a compromise of the private key of the Government-CA 2, 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 Level-One CA operations policies and procedures.

4.9.13 Circumstances for Suspension

If the Government-CA 2 suspects that a certificate should be revoked for one of the circumstances described in section 4.9.1, the Government-CA 2 may suspend the suspected certificate.

4.9.14 Who Can Request Suspension

Refer to the equivalent section in the CP.

4.9.15 Procedure for Suspension Request

When the request comes from a subscriber, a sponsor of a device or a representative of an entity, it must be submitted to an RA via a digitally signed e-mail message. The RA will forward the request to the CA in a similar fashion. When the request comes from an RA, it must be submitted directly to the CA via a digitally signed e-mail message.

The procedure for processing suspension requests is as follows:

- The request is submitted to the CA as described above;
- The digital signature on the request is verified;
- The entity’s certificates are suspended;
- The CA may notify the entity once their certificates have been suspended;
- Certificates are suspended upon receipt of the request by the CA without notification.

Once a suspension request has been received and authenticated, the certificate will be suspended and the suspended certificate shall be published in the relevant CRL or ARL.

Subscribers must present themselves in person to an RA to request re-activation of their suspended certificates. For suspension of RA Certificates refer to NIC Level-One CA Operations Policy section 10.

4.9.16 LIMITS ON SUSPENSION PERIOD

Refer to the equivalent section in the CP.

4.9.17 CIRCUMSTANCES FOR TERMINATING SUSPENDED CERTIFICATES

Refer to the equivalent section in the CP.

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 Government-CA 2 shall authenticate the request as well as the authorization of the requester before a certificate is unsuspended.

4.10 CERTIFICATE STATUS SERVICES

OPERATIONAL CHARACTERISTICS

The status of public certificates is available from CRL's in the repositories and via an OCSP responder (where available).

SERVICE AVAILABILITY

Refer to the equivalent section in the CP.

OPTIONAL FEATURES

No stipulation.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW AND RECOVERY POLICY AND PRACTICES

When data-encryption is supported, the Government-CA 2 must maintain a backup of the private decryption keys to support accessing data encrypted with an unavailable Key.

The Subscriber's Decryption Private Key can be recovered for the Subscriber or for a third party under following conditions:

- The Subscriber can request recovery at any time;
- An authorized individual belonging to the Subscriber organization (if the Subscriber has left the company or some other reason); and
- Compliance or Legal office can request recovery with consent of the NIC.

4.12.1 KEY ESCROW POLICY AND PRACTICES

Government-CA 2 does not offer key escrow services to Subscribers.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

No stipulation.

5. FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

NIC operates the Saudi National Root-CA and other approved CAs, Repositories and OCSP Responder at NIC-PKIC, with appropriate physical and procedural access controls for all hardware and software sub-systems used in the issuance and revocation of certificates. NIC limits access to functions critical to registration and certificate to personnel in Trusted Roles (see section 5.2.1 of this CPS).

The Government-CA 2 is collocated in NIC-PKIC and follows the physical security requirements specified as below:

- 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 access logs.

RA equipment shall be protected from unauthorized access by the DTSPs. The security mechanisms shall be commensurate with the level of threat in the CA environment.

A security checks of the facility housing the CAs equipment shall occur on a regular basis. NIC-PKIC facility shall never leave unattended

5.1.1 SITE LOCATION AND CONSTRUCTION

The location and construction of the facility housing the Government-CA 2, NIC-PKIC equipment is consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 PHYSICAL ACCESS

NIC-PKIC systems are protected by six 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.

NIC has implemented policies and procedures to ensure that the physical environments in which the Government-CA 2 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;
- 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 NIC-PKIC uses include:

- Perimeter alarms;
- Closed circuit television;
- Two-factor authentication using Card reader and keyed door or Combination number.
- Human guards; and
- All the Networking and systems components including the certification components are installed in secure Data cabinets with pin locks from both sides.

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

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

5.1.3 POWER AND AIR CONDITIONING

NIC-PKIC has a UPS and back-up electrical generators and sufficient back-up capability to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

The design of NIC-PKIC ensures that no single point of failure is supported by providing the following measures:

- Two independent power supplies feeding NIC-PKIC;
- Uninterruptible Power Supply units and stand-by generators for the entire building; and
- Switchover of the services to a backup facility in the case of an emergency or disaster as per NIC PKI Business Continuity Plan.

A fully redundant air-conditioning system is installed in the PKI areas.

5.1.4 WATER EXPOSURE

NIC-PKIC has taken reasonable precautions to minimize the impact of water exposure. These include installing the PKI equipment on elevated floors with moisture detectors in a facility that is located above ground level.

5.1.5 FIRE PREVENTION AND PROTECTION

NIC-PKIC follows best practices and industry standard for fire prevention and protection. Some of the measures deployed include:

- Fire-resistant walls and pillars;
- Fire, smoke and gas detectors installed throughout the facility which are interconnected with the facilities alarm system;

- An adequate number of fire extinguishers have been provided with a suitable fire extinguishing agent. Mobile fire extinguishers are also provided in sufficient numbers within the facility; and
- The controls implemented comply with applicable safety regulations of the Kingdom of Saudi Arabia.

5.1.6 *MEDIA STORAGE*

Media storage under the control of NIC-PKIC is subject to multiple-layer security storage requirements. NIC-PKIC procedures include full back-up of the Government-CA 2 repositories and OCSP Responder data, offsite storage in two physically separate locations with security similar to that of the facility in which the CA activities are performed. Media is stored so as to protect them from accidental damage (e.g., water, fire, or electromagnetic). Media that contain audit, archive, or backup information are duplicated and stored in locations separate from the CA's.

5.1.7 *WASTE DISPOSAL*

NIC-PKIC security procedures provide that sensitive media and documentation that are no longer needed for operations are destroyed using secure disposal processes. For example, sensitive paper documentation is shredded, burned, or otherwise rendered unrecoverable. Electronic media is physically destroyed prior to disposal.

5.1.8 *OFF-SITE BACKUP*

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

The backup site has physical and procedural controls commensurate to that of NIC-PKIC.

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 NIC to fill these roles will be extraordinarily responsible. The functions performed in these roles form the basis of trust for uses of the Government-CA 2. 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:

1. **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.

2. 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.

3. 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.

4. 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.

5. 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

NIC 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 previous sections and 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 Government-CA 2 will ensure that no single individual may gain access to CA private keys. At a minimum two individuals, must perform any CA system start-up, CA system shutdown, key backup or key recovery operation.

5.2.3 IDENTITY-PROOFING FOR EACH ROLE

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

5.2.4 SEPARATION OF ROLES

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 five roles defined in section 5.2.1 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 trusted 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 must 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

NIC-PKIC will provide proper training to all personnel performing duties with respect to the operation of the Government-CA 2, Repositories and OCSP Responder. Training shall cover the following aspects:

- PKI and Information Security concepts;
- All PKI software versions in use on the Government-CA 2, Repositories and OCSP Responder systems;
- All NIC-PKIC PKI duties that the personnel are expected to perform on Government-CA 2;
- Disaster recovery and business continuity procedures; and
- The meaning and effect of the Government-CA 2 CP and this CPS.

The RA Administrator(s) engaged in Certificate issuance shall be given detailed training to perform their tasks. Government-CA 2 shall design examination based on the training which is to be qualified by each RA Administrator.

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

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

Individuals performing PKI roles are made aware of changes in the Government-CA 2, 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 Government-CA 2 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

NIC 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 Government-CA 2 CP, this CPS and/or other procedures.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

When NIC uses a contractor to perform services, there will be adequate procedures with explicitly stated objectives and supervision will be in place to ensure that any tasks performed in accordance with the Government-CA 2 CP, this CPS, NIC PKI Policies as well as the requirements stipulated in the contractor's contract of employment. Contractor personnel shall be subject to the same sanctions as other personnel as set forth in Section 5.3.6., the relevant training and skills requirements from Section 5.3.3 and the event logging requirements of Section 5.4.1.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

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

5.4 AUDIT LOGGING PROCEDURES

NIC-PKIC 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 of the Government-CA 2 and other associated components.

NIC-PKIC systems shall generate audit log files for all events relating to the security of the Government-CA 2 and other associated components. 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 5.5.2 which governs the archive retention period for security audit data.

5.4.1 TYPES OF EVENTS RECORDED

NIC-PKIC enables all security auditing capabilities of the Government-CA 2 and other associated components, operating system and PKI applications during installation. At a minimum, each audit record includes the following:

- The type of event;
- The date and time the event occurred;
- A success or failure indicator of the event (e.g. CA signing event, revocation event, certificate validation event);
- The identity of the entity and/or operator that caused the event; and
- Description of the event.

The minimum audit records to be kept are detailed in NIC PKI Audit and Compliance Policy. All security audit capabilities of the Government-CA 2 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;
- CA personnel changes;
- documentation relating to certificate requests and the verification;
- documentation relating to certificate revocation;
- Discrepancy and No compromise reports;
- Information concerning the destruction of sensitive information;
- Current and past versions of all Certificate Policies;
- Current and past versions of Certification Practice Statements;
- Vulnerability Assessment Reports;
- Threat and Risk Assessment Reports;
- Compliance Inspection Reports; and
- Current and past versions of Agreements.

5.4.2 FREQUENCY OF PROCESSING DATA

Audit logs are required to be processed in accordance with NIC PKI Audit and Compliance Policy.

5.4.3 RETENTION PERIOD FOR SECURITY AUDIT DATA

The Government-CA 2 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 SECURITY AUDIT DATA

Read access to the journal information is granted to personnel requiring this access as part of their duties. Only authorized roles can obtain access:

The journal is stored in the text files and access to this is protected against unauthorized access by the CA application and through special security measures on the operating system level.

5.4.5 SECURITY AUDIT DATA 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.

Audit log backup procedures are in accordance with NIC PKI Audit and Compliance Policy.

5.4.6 SECURITY AUDIT COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The audit log or journal is an integral part of the CA software. NIC audit collection system is detailed in 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

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.

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

NIC performs third party penetration testing for NIC-PKIC infrastructure at least, once a year and doing regular vulnerability assessment internally. Also Risk Assessment is performed at least once a year as per NIC PKI Risk Assessment Methodology. NIC PKI Risk Assessment exercise 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, the Government-CA 2 shall develop, implement, and maintain a security plan to control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF EVENTS ARCHIVED

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

- Audit logs generated by the PKI CA software;
- DTSP and other agreements;
- Records pertaining to identification and authentication information;
- Physical access logs;
- System configuration changes and maintenance;
- CA personnel changes;
- Discrepancy and No compromise reports;
- Information concerning the destruction of sensitive information;
- Current and past versions of all Certificate Policies;
- Current and past versions of Certification Practice Statements;

- Vulnerability Assessment Reports;
- Threat and Risk Assessment Reports;
- Compliance Inspection Reports;
- Documents identifying all personnel who received CA related training and the level of training completed; and
- The Government-CA 2 shall archive any necessary keys and passwords for a period of time sufficient to support the functionalities.

5.5.2 RETENTION PERIOD FOR ARCHIVE

The minimum retention period for archive data is established at ten years.

The Government-CA 2 shall ensure that DTSPs shall retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least ten years after any Certificate based on that documentation ceases to be valid.

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 Government-CA 2 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. 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.

5.5.4 ARCHIVE BACKUP PROCEDURES

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

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

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

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

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

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

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 *INCIDENT AND COMPROMISE HANDLING PROCEDURES*

The Government-CA 2 has incident response and disaster recovery plans, and associated procedures meeting the requirements specified in Section 5.7.4.

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. Government-CA 2-PA shall notify NIC 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; and
- Any incident preventing a CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

Government-CA 2-PA shall be notified by NIC 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; and
- The above measures will allow participants to protect their interests as Relying Parties.

CA shall re-establish operational capabilities as quickly as possible in accordance with the procedures set forth in Saudi National Root-CA Operations Policy and NIC PKI Business Continuity Plan.

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 NIC management and NIC's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, Saudi National Root-CA Operations Policy section 12-13 or related Business Continuity procedures will be enacted.

5.7.3 CA PRIVATE KEY COMPROMISE RECOVERY PROCEDURES

CA private key compromise recovery procedures are detailed in Saudi National Root-CA Operations Policy section 14.

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 infrastructure equipment at the primary site (NIC-PKIC) has built-in hardware fault-tolerance, and is configured to be highly available with auto-failover switching. NIC currently maintains copies of backup media and infrastructure system software, which include but is 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 PKI 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 PKI 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 PKI Business Continuity Policy contains further details.

5.8 CA OR RA TERMINATION

5.8.1 CA TERMINATION

No stipulation.

5.8.2 RA TERMINATION

If DTSP terminates operation for convenience, contract expiration, re-organization, or other non-security related reason, the Agreement between NIC and the DTSP shall set forth what actions are to be taken to ensure continued support for certificates previously issued by the Government-CA 2.

Upon termination of the RA Agreement, the RA certificate shall be revoked.

NIC will be the custodian of CA/RA archival records in case of termination.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

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

Government-CA 2 key pair is generated in pre-planned Key Generation Ceremonies in accordance with the requirements of NIC as mentioned in the NIC Level-One CA Key Generation Ceremony Policy. The activities performed in key generation ceremony are video recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by Government-CA 2 management.

RA key pairs will be generated in cryptographic modules at least compliant to FIPS 140-2 Level 2 or higher.

Subscriber key pairs are generated based on the Assurance Level. If subscriber key pairs are generated using cryptographic modules, then the cryptographic modules shall be at least compliant to FIPS 140-2 Level 2 or higher.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

Where a Subscribers private key is generated in the presence and control of the Subscriber, private key delivery to the Subscriber is not applicable.

Where private keys are not created in the presence of the Subscriber, they will be delivered electronically using industry standard based PKCS messages over secure protocols which provide equivalent or higher encryption strength than the key being transported or may be delivered on a hardware cryptographic module. In all cases, the following requirements are met:

- Anyone who generates a private signing key for a Subscriber does not retain any copy of the key after delivery of the private key to the Subscriber;
- The private key is protected from activation, compromise, or modification during the delivery process;
- The Subscriber acknowledges receipt of the private key;
- Delivery is accomplished in a way that ensures that the correct token and activation data are provided to the correct Subscriber.
  - For cryptographic modules, accountability by the RA for the location and state of the module is maintained until the Subscriber accepts possession of it.
  - For electronic delivery of private keys, the key material is encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data is delivered using a separate secure channel.

For Subscribers using centralized signing platform, Signing keys are generated using FIPS 140-2 Level 3 or higher certified hardware security module and stored in an encrypted database on the central storage. Key wrapping is accepted for the centralized signing platform subscribers. The signing keys are under the control of Subscriber and used through key activation data provided by Subscriber during every transaction.

6.1.3 Public Key Delivery to Certificate Issuer

The Applicant's Public Key must be transferred to Government-CA 2 using a method designed to ensure that:

- The Public Key is not changed during transit; and
- The sender possesses the Private Key that corresponds to the transferred Public Key.

Delivery of public keys shall be achieved with a certificate request using a recognized secure protocol such as PKCS#10.

6.1.4 CA Public Key Delivery to Subscribers and Relying Parties

Acceptable methods are specified in section 6.1.4 of the Government-CA 2 CP.

6.1.5 Key Sizes

Refer to the equivalent section in the CP.

6.1.6 Public Key Parameters Generation and Quality Checking

The HSM pseudo-random number generator is validated by NIST. Public key parameters prescribed are generated in accordance with industry best practices.

6.1.7 Key Usage Purposes

Refer to the equivalent section in the CP.

6.2 Private Key Protection and Crypto-Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

See section 6.1.1 of this CPS for the description of the cryptographic modules.

6.2.2 CA Private Key Multi-Person Control

Multi-person control of CA private key is achieved using an "m-of-n" split key knowledge scheme. Government-CA 2 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. Government-CA 2 does not escrow end-user Subscriber private keys with any third party.

6.2.4 *PRIVATE KEY BACKUP*

6.2.4.1 *BACKUP OF CA SIGNING PRIVATE KEY*

NIC-PKIC uses the mechanisms provided by the HSM's to backup the Government-CA 2 CA signing key. A second copy may be kept at the CA backup location identified as business continuity location. A third copy may be kept at the CA backup location identified as disaster recovery location. Procedures for Government-CA 2 signing Private Key backup are detailed in NIC Level-One CA Backup and Restore Policy. The CA signing key is backed up under the same multi-person control as the original signature keys.

Government-CA 2 private keys that are physically transported from one facility to another follows NIC Cryptographic Devices Lifecycle Management Policy and Procedure.

Government-CA 2 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.

Government-CA 2 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.

6.2.4.2 *BACKUP OF SUBSCRIBER PRIVATE KEYS*

The Government-CA 2 which issues certificates supporting data-encryption must offer the following services to Subscribers and authorized parties:

- The securely storage of issued private decryption keys; and
- A mechanism to securely retrieve the necessary key pairs and certificates when required

Except for the centralized signing platform Subscribers, private signing keys and authentication private keys will not be backed up.

6.2.5 *PRIVATE KEY ARCHIVAL*

The Government-CA 2 which issues certificates supporting data-encryption must provide the capability to archive issued private keys once the certificate has expired or once the backup period has ended. A complete history of all private keys and certificates issued must be maintained. The archive recovery service will enable a certificate holder or authorized authority access to the certificate and key upon the completion of NIC and Government-CA 2 key recovery processes.

The Government-CA 2 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 NIC are validated to FIPS 140-2 Level 3 ensuring that the CA keys cannot be exported to less secure media.

The Government-CA 2 keys can be cloned for secure backup from the master hardware cryptographic module to other hardware cryptographic module(s) using secure mechanisms so that they can be recovered if a major catastrophe destroys the productive set of keys.

RA, LRA and Subscriber private keys shall not be transferred from the module they are generated in.

Government-CA 2 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 Government-CA 2 key migration process are tested by the CA prior to the migration event. The Government-CA 2 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.

Subscriber/RAs private keys shall be stored in cryptographic modules at least compliant to FIPS 140-2 level 2 or higher.

6.2.8 METHOD OF ACTIVATING PRIVATE KEYS

A CA’s private key shall be activated by a threshold number of Shareholders, as defined in NIC Level-One CA Operations Policy section 5, supplying their activation data. Such activation data shall be held on secure media and shall require the successful completion of a multi-person authentication process. A deactivated key shall be kept encrypted or otherwise secured within the cryptographic module, to prevent unauthorized access.

Subscribers must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication includes but is not limited to passwords and PINs.

6.2.9 METHODS OF DEACTIVATING PRIVATE KEYS

A CA’s private keys shall be deactivated by a threshold number of shareholders, as defined in NIC Level-One CA Operations Policy section 6, by removing their secure media.

Subscriber private keys may be deactivated after each operation upon logging out of the application or upon removal of a hardware token from the reader depending upon the authentication mechanism employed. In all cases, Subscribers have an obligation to adequately protect their private key(s).

6.2.10 METHODS OF DESTROYING PRIVATE KEYS

The copies of Government-CA 2 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.

NIC Government-CA 2 makes no expiry for end entity decryption key, thus doesn’t destroy it. In addition, the means of destroying subscriber’s private key are not defined as currently there’s no business need for it.

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 or higher compliant.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 *PUBLIC KEY ARCHIVE*

The CA and Subscriber certificates are backed up and archived as part of the Government-CA 2 and NIC-PKIC routine backup procedures.

6.3.2 *CERTIFICATE OPERATIONAL PERIODS AND KEY USAGE PERIODS*

Refer to the equivalent section in the CP.

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.

A shared secret may be generated by an RA upon successful completion of subscriber registration process.

Subscriber will use the shared secret / Activation data to successfully identify himself and prove possession of associated private key at the time of certificate generation. Such activation data may also be used to protect the transport of a subscriber's keys and certificates to the subscriber.

6.4.2 *ACTIVATION DATA PROTECTION*

If written down CA cryptographic module activation data is placed into secure packages which are then stored within secure containers in a highly secured environment inside NIC-PKIC.

Activation data shall be supplied to Subscribers using secure delivery methods.

6.4.3 *OTHER ASPECTS OF ACTIVATION DATA*

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 *SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS*

The Government-CA 2 servers hosted in NIC-PKIC 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 Government-CA 2 software. The following controls ensure the security of NIC-PKIC 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 SECURITY CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

Government-CA 2 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.

NIC employs the following System Development controls:

- NIC may use standard software from product vendors for version control. Where NIC 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;
- NIC 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 PKI Operations Policies and Procedures.

6.6.2 SECURITY MANAGEMENT CONTROLS

Government-CA 2 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 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 RATINGS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The Repository and OCSP Responder infrastructure will be 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.

NIC-PKIC uses 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 Government-CA 2's, Repository and OCSP Responder equipment. These technologies may limit the services allowed to and from the on-line CA's, Repository and OCSP Responder equipment to those authorized to have such access.

NIC-PKIC's network security controls are designed to protect 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 shall 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 CA response.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

This section contains the rules and guidelines followed by this CA in populating X.509 certificates and CRL extensions. The Certificate profile for the Government-CA 2 is described in the Saudi National Root-CA CP.

7.1.1 VERSION NUMBERS

Refer to the equivalent section in the CP.

7.1.2 CERTIFICATE EXTENSIONS

Refer to the equivalent section in the CP.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

Refer to the equivalent section in the CP.

7.1.4 NAME FORMS

Refer to the equivalent section in the CP.

7.1.5 NAME CONSTRAINTS

Refer to the equivalent section in the CP.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

Refer to the equivalent section in the CP.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

Refer to the equivalent section in the CP.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

Refer to the equivalent section in the CP.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION

Refer to the equivalent section in the CP.

7.2 CRL PROFILE

Refer to the equivalent section in the CP.

7.2.1 VERSION NUMBERS

Refer to the equivalent section in the CP.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

The following values are supported for the reasonCode extension when present as a CRL entry for an end entity Certificate.

- keyCompromise (1).
- affiliationChanged (3).
- superseded (4).
- certificateHold (6).

7.3 OCSP PROFILE

Refer to the equivalent section in the CP.

7.3.1 VERSION NUMBER

Refer to the equivalent section in the CP.

7.3.2 OCSP EXTENSIONS

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The Government-CA 2 PA shall be responsible for overseeing compliance of the Government-CA 2, DTSPs, Government-CA 2 CP and CPS. NIC-PKIC and Government-CA 2 PA shall ensure that the requirements of the Government-CA 2 CP and CPS and the provisions of applicable Agreements with NIC are implemented and enforced.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The Government-CA 2 shall be subjected to periodic compliance audits which are no less frequent than once a year and after each significant change to the deployed procedures and techniques. 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 any DTSP's operation to validate that it is operating in accordance with the applicable CP, PDS, CPS, Audit and Compliance Policy and NIC PKI Operations Policies and Procedures. Similarly, the Government-CA 2 PA has the right to require periodic inspections of its DTSPs to validate that the DTSPs are operating in accordance with the Government-CA 2 CP and/or DTSP agreement. The Government-CA 2 shall internally audit each delegated third party's (DTSP, RA) compliance against defined requirements on an annual basis.

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 who shall be Licensed WebTrust Practitioner to perform such compliance audits as a primary responsibility.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

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

8.4 TOPICS COVERED BY ASSESSMENT

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

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

The auditor shall provide the Government-CA 2 PA and/or NIC with a compliance report highlighting any discrepancies.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If irregularities are found by the auditor, the audited party shall be informed in writing of the findings. The audited party must submit a report to the auditor or directly to NIC or Government-CA 2 PA, as determined by NIC, as to any remedial action the audited party will take in response to the identified deficiencies. This report shall include a time for completion to be approved by the auditor, or by NIC as appropriate.

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

- Noting the deficiencies but allowing the 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 the Government-CA 2 PA and/or NIC as applicable.

The Government-CA 2 shall make the Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, an explanatory letter is to be signed by the Qualified Auditor.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE/RENEWAL FEE

Refer to the equivalent section in the CP.

9.1.2 CERTIFICATE ACCESS FEES

Refer to the equivalent section in the CP.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEE

Refer to the equivalent section in the CP.

9.1.4 FEES FOR OTHER SERVICES

Refer to the equivalent section in the CP.

9.1.5 REFUND POLICY

Refer to the equivalent section in the CP.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 INSURANCE COVERAGE

Non-governmental DTSP’s shall be maintaining 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 Government-CA 2 acts within the bounds of laws in Saudi Arabia, under the administration of the National Information Center.

9.2.2 OTHER ASSETS

Refer to the equivalent section in the CP.

9.2.3 INSURANCE/WARRANTY COVERAGE FOR END-ENTITIES

Refer to the equivalent section in the CP.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Information pertaining to the Government-CA 2 may be made publicly available at the discretion of NIC and/or a Government-CA 2 Policy Authority. Specific confidentiality requirements for business information are defined in NIC PKI Privacy Policy and the associated Subscriber, Relying Party and DTSP agreements.

9.3.1 *SCOPE OF CONFIDENTIAL INFORMATION*

9.3.1.1 *REGISTRATION INFORMATION*

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

- Certificate applications, whether approved or not;
- Certificate information collected as part of the registration process;
- Completed Subscriber Agreements;
- Any information requested by NIC when it receives an application from a third party to operate as a DTSP CA or a Cross-Certified CA;
- Any corporate or personal information held by NIC, 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 Government-CA 2 CP, and in accordance with NIC PKI Privacy policy.

9.3.1.2 *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 DTSP 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; or
- The termination of the Saudi National Root-CA, a DTSP CA, a Cross-Certified CA, an RA or a LRA, in which case prior disclosure of the termination may be given.

9.3.1.3 *PKI DOCUMENTATION*

NIC PKI Document Control Policy specifies which documents are considered to be confidential.

9.3.2 *INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION*

9.3.2.1 *CERTIFICATE INFORMATION*

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

9.3.2.2 *PKI DOCUMENTATION*

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

- The Government-CA 2 CP;
- The Government-CA 2 CPS;

- PKI Disclosure Statements;
- NIC PKI Dispute Resolution Policy;
- NIC PKI Privacy Policy; and
- Any other policy documents which are classified public.

9.3.2.3 DISCLOSURE OF CERTIFICATE REVOCATION INFORMATION

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

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

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

9.4 PRIVACY OF PERSONAL INFORMATION

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

9.4.1 PRIVACY PLAN

The Government-CA 2 and the DTSPs shall protect the confidential information it possesses in accordance with NIC PKI 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. NCDC Privacy Policy identifies the personally identifiable information that can be collected to enable issuance of a certificate.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

Access to Government-CA 2 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, NIC PKI 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/ADMINISTRATIVE PROCESS

Refer to the equivalent section in the CP.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Refer to the equivalent section in the CP.

9.5 INTELLECTUAL PROPERTY RIGHTS

Refer to the equivalent section in the CP.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 GOVERNMENT-CA 2'S REPRESENTATIONS AND WARRANTIES

Refer to the equivalent section in the CP.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

Refer to the equivalent section in the CP.

9.6.3 RELYING PARTIES REPRESENTATIONS AND WARRANTIES

Refer to the equivalent section in the CP.

9.6.4 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

Refer to the equivalent section in the CP.

9.7 DISCLAIMERS OF WARRANTIES

Refer to the equivalent section in the CP.

9.8 LIMITATIONS OF LIABILITY

Refer to the equivalent section in the CP.

9.9 INDEMNITIES

Refer to the equivalent section in the CP.

9.10 TERM AND TERMINATION

9.10.1 TERM

This DTPS 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 Government-CA 2 participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Refer to the equivalent section in the CP.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

The Government-CA 2 PA shall review this CPS at least once per year. Errors, updates, or suggested changes to this CPS shall be communicated to the Government-CA 2 PA and/or NIC. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change. Any technical changes in the Government-CA 2 shall be managed as per the NIC PKI Change Management Policy.

Subject to the approval of NIC, the Government-CA 2 PA reserves the right to change this CPS from time to time. The Government-CA 2 PA 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

The Government-CA 2 PA reserves the right to amend this CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URL’s, and changes to contact information. All the Saudi PKI participants and other parties designated by the Government-CA 2 PA shall provide their comments to the Government-CA 2 PA in accordance with NIC rules.

The Government-CA 2 PA’s decision to designate amendments as material or non-material shall be at the PA’s sole discretion.

Any changes to this CPS shall be made available within two weeks of 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 PROCEDURES

Any dispute arising out of or related to the digital certificates issued by the Government-CA 2 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.

9.13.1.1 DISPUTE RESOLUTION COMMITTEE

NIC PKI Dispute Resolution Committee which will arbitrate on all claims or disputes arising out of or related to the PKI operation of NIC.

9.13.1.2 DISPUTE RESOLUTION POLICY

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

All DTSPs will ensure that any agreements they enter into with Relying Parties, Subscribers or other Certificate Authorities will include details of 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

Refer to the equivalent section in the CP.

9.16.3 SEVERABILITY

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

9.16.4 ENFORCEMENT (ATTORNEY FEES/WAIVER OF RIGHTS)

This document shall be treated according to laws of Kingdom of Saudi Arabia. Legal disputes arising from the operation of the Government-CA 2 will be treated according to laws of Kingdom of Saudi Arabia.

9.16.5 FORCE MAJEURE

The Government-CA 2 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

Government-CA 2 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 Government-CA 2, 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

Nothing contained in this CPS shall be deemed to constitute either the Government-CA 2, 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 Government-CA 2 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 Government-CA 2.

9.17.2 ADMINISTRATIVE PROCESSES

As specified in NIC PKI Operations Policies and applicable Agreements.