وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Certification Practice Statement
NR-CA

Document Name:	Certification Practices Statement NR-CA
Document Reference:	CS-PI-CSP-PMA-POL-0003
Issue:	1.0
Issue Date:	12/06/2019
Status:	Final
Prepared By:	Chihebeddine MBAREK
Reviewed By:	Fahad Saeed J S ABDULLA Chihebeddine MBAREK Thameur BELGHITH
External Review By:	Samir PAWASKAR
Approved By:	Fahad Saeed J S ABDULLA

Amendment history

Date	Issue	Status	Author
10/12/2018	0.1	Draft version	PKI Section
25/04/2019	0.2	First review	PKI Section
28/04/2019	0.3	Second version for review	PKI Section
11/06/2019	0.4	External Review	Samir Pawaskar
12/06/2019	0.9	Document for approval	PKI Team
	1.0	Final Document	Fahad Saeed J S Abdulla

Contents

1 Introduction....9

1.1 Overview....9

1.2 Document Name and Identification....12

1.3 PKI Participants....12

1.3.1 Certification Service Provider and National Root Certification Authority....12

1.3.2 Registration Authorities....13

1.3.3 Subscribers....13

1.3.4 Relying Parties....14

1.4 Certificate Usage....14

1.4.1 Appropriate certificate usage....14

1.4.2 Prohibited certificate usage....14

1.5 Policy Administration....14

1.6 Definitions and Acronyms....16

1.6.1 Terminology and definitions....16

1.6.2 Abbreviations....16

1.6.3 References....16

2 Publication and Repository Responsibilities....16

3 Identification and Authentication....17

3.1 Naming....17

3.2 Initial Identity Validation....18

3.3 Identification and Authentication for Re-key Requests....18

3.4 Identification and Authentication for Revocation Requests....18

4 Certificate Life-Cycle Operational Requirements 18

4.1 Certificate Application 19

4.2 Certificate Application Processing 19

4.3 Certificate Issuance 20

4.4 Certificate Acceptance 20

4.5 Key Pair and Certificate Usage 21

4.5.1 Subscriber duties 21

4.5.2 Relying party duties 21

4.6 Certificate Renewal 21

4.7 Certificate Re-key 22

4.8 Certificate Modification 22

4.9 Certificate Revocation and Suspension 22

4.10 Certificate Status Services 23

4.11 End of Subscription 23

4.12 Key Escrow and Recovery 23

5 Management, Operational and Physical Controls 24

5.1 Physical Security Controls 24

5.2 Procedural Controls 24

5.3 Personnel Security Controls 25

5.3.1 Qualifications, Experience, Clearances 25

5.3.2 Background Checks and Clearance Procedures 25

5.3.3 Training Requirements and Procedures 25

5.3.4 Retraining Period and Retraining Procedures 26

5.3.5 Sanctions against Personnel 26

5.3.6 Controls of independent contractors 26

5.3.7 Documentation for initial training and retraining 26

5.4 Audit Logging Procedures 26

5.5 Records Archival 27

5.5.1 Types of records 28

5.5.2 Retention period 28

5.5.3 Protection of archive 28

5.5.4 Archive backup procedures 28

5.5.5 Time-stamping of records 28

5.5.6 Archive Collection 28

5.5.7 Procedures to obtain and verify archive information 28

5.6 Key Changeover 29

5.7 Compromise and Disaster Recovery 29

5.7.1 Incident and compromise handling procedures 29

5.7.2 Computing resources, software, and/or data are corrupted 29

5.7.3 Entity private key compromise procedures 29

5.7.4 Business continuity capabilities after a disaster 30

5.8 CA or RA Termination 30

6 Technical Security Controls 31

6.1 Key Pair Generation and Installation 31

6.1.1 CA Private Key Pair Generation 31

6.1.2 Private key provisioning 32

6.1.3 Public key provisioning 32

6.1.4 CA's public key provisioning to potential relying parties....32

6.1.5 Key sizes....32

6.1.6 Public key parameter generation 32

6.1.7 Key usage....32

6.2 Private Key Protection and Cryptographic Module Engineering Controls 33

6.2.1 NR-CA Key Generation Devices....33

6.2.2 NR-CA Private key shared control....33

6.2.3 NR-CA Private Key escrow 33

6.2.4 NR-CA Private key backup....33

6.2.5 NR-CA Private key archival....34

6.2.6 Private key transfer into or from a cryptographic module....34

6.2.7 Private key storage on cryptographic module....34

6.2.8 Method of activating private key....34

6.2.9 Method of deactivating private key....34

6.2.10 NR-CA Private Key Destruction 34

6.2.11 Cryptographic Module Rating 35

6.3 Other Aspects of Key Pair Management 35

6.3.1 Public key archival 35

6.3.2 Certificate operational periods and key pair usage periods 35

6.4 Activation Data....35

6.4.1 Activation data protection....35

6.4.2 Other aspects of activation data 36

6.5 Computer Security Controls 36

6.6 Life Cycle Security Controls 36

6.7 Network security controls 36

7 Certificates and CRL Profiles 36

7.1 Certificate Profile 36

7.1.1 Version number(s) 36

7.1.1 Certificate extensions 48

7.1.2 Algorithm object identifiers 48

7.1.3 Name forms 48

7.1.4 Name constraints 48

7.1.5 Certificate policy object identifier 48

7.1.6 Usage of Policy Constraints extension 48

7.1.7 Policy qualifiers syntax and semantics 48

7.1.8 Processing semantics for the critical Certificate Policies 48

7.2 CRL Profile 48

7.2.1 Version number(s) 53

7.2.2 CRL entry extensions 53

8 Compliance Audit and Other Assessments 53

9 Other Business and Legal Matters 55

9.1 Fees 55

9.2 Financial Responsibility 55

9.2.1 Insurance coverage 55

9.2.2 Other assets 55

9.2.3 Insurance or warranty coverage for end-entities 55

9.3 Confidentiality of Business Information 55

9.4 Privacy of Personal Information 55

9.5 Intellectual Property Rights 57

9.6 Representations and Warranties 57

9.7 Disclaimers of Warranties 57

9.8 Indemnities 58

9.9 Term and termination 58

9.10 Individual notices and communications with participants 58

9.12 Amendments 58

9.13 Dispute Resolution Procedures 58

9.14 Governing Law 59

9.15 Compliance with applicable law 59

9.16 Miscellaneous provisions 59

9.17 Other Provisions 59

1 Introduction

The present Certification Practice Statement (hereinafter, CPS) of the CSPs-PMA National Root Certification Authority of the State of Qatar (hereinafter, NR-CA) applies to all public services of the CSPs-PMA NR-CA.

This CPS complies with the formal requirements of Internet Engineering Task Force (IETF) [RFC 3647] with regard to format and content. While certain section titles are included according to the structure of [RFC 3647]; the topic may not necessarily apply in the implementation of the PKI services of the NR-CA. Such sections are denoted as “Section not applicable”.

The CPS addresses in detail the technical, procedural and organizational policies and practices of the NR-CA with regard to all services available and during the complete lifetime of certificates, issued by the NR-CA.

Further information with regard to this CPS and the NR-CA can be obtained from the CSPs-PMA, Public Key Management and Digital Identity Section, through contact information provided in section 1.5.

The present document complies with the Decree Law No. (16) of 2010 on the Promulgation of the Electronic Commerce and Transactions Law (hereafter referred to as the E-Commerce Law) and the Bylaw No. (01) of 2012 Promulgating the Bylaw regulating the work of certification service providers pursuant to the Electronic Commerce and Transactions Law (hereafter referred to as the Bylaw). It aims to fall back as much as possible on existing and internationally recognized standards. Wherever it is possible; sections from these standards will be referenced rather than copied.

1.1 Overview

The technology used for the certification services related to the issuance and management of the NR-CA certificates and the certificates issued by the NR-CA is the Public Key Infrastructure (PKI) technology. PKI is an acronym for a system of **P**ublic **K**ey cryptography combined with an **I**nfrastructure that is designed to provide a level of security for communicated and stored electronic information sufficient to justify trust in such information by business, consumers, governments and the courts.

A Certification Practice Statement (CPS) is a statement of the practices that a Certification Authority employs in issuing certificates. A CPS is a comprehensive treatment of how the CA makes its services available. This CPS is intended to be used within the domain of the NR-CA in its function of issuer of root-signing certificates to licensed certification service providers and of cross-certificates to approved foreign certification services. This CPS aims at delimiting the domain of providing certification services to the subscribers and relying parties within the CA domain. This CPS also outlines the relationship between the NR-CA and other CAs within the CSPs-PMA licensed PKI hierarchies.

The E-Commerce Law requires certification service providers willing to operate in the State of Qatar to obtain a license in order (prior) to engage in activities related to maintaining a PKI, issuing certificates,

or providing services related to electronic signatures (e.g. time-stamping services, signature generation services, signature validation services).

The E-Commerce Law mandates the Public Key Management and Digital Identity Section as owner and enforcing authority for the Decree and in particular for licensing the certification service providers within Qatar. In order to pursue the application of this Decree, bylaw have been issued mandating Public Key Management and Digital Identity Section to establish and fulfil the role of the Policy Management Authority (PMA) for certification service providers. Hence the above described certification services from any CSP willing to operate in the State of Qatar must be licensed by this CSPs Policy Management Authority (CSPs-PMA) before starting issuing certificates or providing services related to electronic signatures.

Licensed certification services shall be root-signed by the NR-CA. In practice this means that technical Certification Authorities (CAs) issuing certificates to end-entities as well as any other type of licensed certification service related to electronic signature (e.g. a Time-Stamping Authority (TSA) providing time-stamping services and issuing time-stamp tokens) being granted a license by the CSPs-PMA will be issued with a certificate signed by the NR-CA. Similarly, the certification services from approved foreign CSPs will be cross-certified by the NR-CA. Any certificate delivered by the NR-CA based on such license SHALL be revoked when the license has been cancelled by the CSPs-PMA.

Public Key Management and Digital Identity Section in quality of CSPs-PMA will act as a certification service provider with regards to this specific NR-CA root-signing and cross-certifying activities and have business ownership and final responsibility in providing those certification services, e.g. in issuing and managing the root-signed certificates to licensed certification services (e.g. CA, TSA) in accordance to the present NR-CA Certification Practice Statement (NR-CA CPS). In this context, Public Key Management and Digital Identity Section has managed the hosting facilities and services as well as the operational aspects of the NR-CA.

The government of Qatar manages a Public Key Infrastructure (PKI) that uses standard PKI technologies, policies & operating procedures and application interfaces. Certification services provided from this PKI enable citizens, residents and corporate organizations to conduct secure electronic transactions. This PKI (NR-CA) and the related certification services are provided and operated by The Public Key Management and Digital Identity Section in quality of CSPs-PMA in the state of Qatar. The CSPs-PMA is the authority that has final responsibility in providing those PKI certification services, e.g. in issuing and managing the issuing CAs.

This is illustrated in Figure 1 below that depicts the Trust Model for PKI's in the State of Qatar.

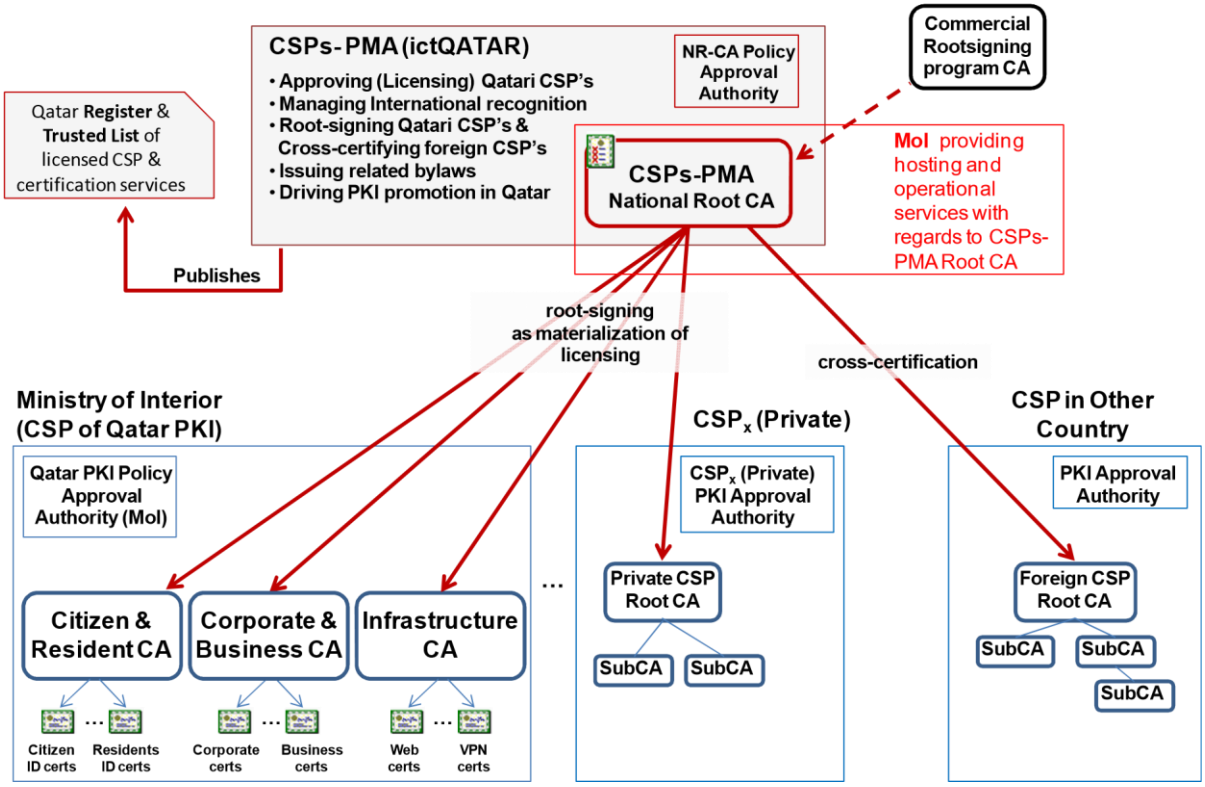

Figure 1: Trust Model for PKI's in the State of Qatar

Within the framework of the Qatar government's licensing scheme for certification service providers, the Qatar Root Certification Authority (NR-CA) is the top authority in Qatar with regard to digital certification services offered in Qatar.

The present CPS applies to the NR-CA and identifies the roles, responsibilities and practices of all its constitutive component services. This CPS also applies to all subscribers and relying parties as well as CAs that belong to the PKI hierarchies in Qatar from licensed certification service providers as they may be referenced herein.

The provisions of the present CPS with regard to practices, level of services, responsibilities and liability, bind all parties involved including the NR-CA, subscribers (which are licensed or approved CAs or TSAs) and relying parties.

The present CPS governs the issuance of the CA certificates during the application period during which the NR-CA may issue and manage issued certificates. It describes the policy requirements to issue,

manage and use certificates within the scope of the NR-CA domain, i.e. the root-signing of licensed certifications services operated in the State of Qatar and the cross-certification of approved foreign certification services. The NR-CA issues certificates to licensed CAs that carry out electronic certification services within their own domains and in support of multiple types of certificates.

1.2 Document Name and Identification

This document is named "QPKI CSPs-PMA NR-CA CPS" and is referenced in related documents as [CS-PI-CSP-PMA-POL-0003].

The NR-CA will also use the OID XXXXXXX to identify this CPS.

1.3 PKI Participants

Several parties make up the participants of this NR-CA PKI. The parties mentioned hereunder including the NR-CA, subscribers and relying parties are collectively called PKI participants.

1.3.1 Certification Service Provider and National Root Certification Authority

A Certification Service Provider (CSP) issuing certificates is an organization that has final responsibility on the issuance and the life-cycle management of the certificates it issues. It makes use of one or several technical Certification Authorities (CAs) to issue digital certificates that are used in the public domain or within a business or transactions context. In the context of the Qatar National Root CA root-signing or cross-certifying licensed Qatari CSPs and their certifications services or approved foreign CSPs and their certification services, Public Key Management and Digital Identity Section in quality of CSPs-PMA, is acting as CSP i.e. the legal entity identified in the NR-CA issued certificates as the Issuer, and has overall and final responsibility for the provision of the entire set of (sub-)component certification services required for the provision of its services (e.g. registration services, certificate generation services, dissemination services, revocation management services, certificate validity status services, subject device provision services).

The actual hosting and certification operations including issuance, certificates status, and repository services are managed and carried by Public Key Management and Digital Identity Section in quality of CSPs-PMA. CSPs-PMA is mentioned hereinafter as "the NR-CA operator".

The CSPs-PMA acting as CSP with regards to the NR-CA is responsible to draft the policy and procedures prevailing in issuing root-signing certificates and cross-certificates within its own domain. In this regard, the CSPs-PMA is also a Policy Approval Authority with regard to the issuance of those certificates issued by the NR-CA.

The CSPs-PMA ensures the availability of all services pertaining to the certificates, including the issuing, revocation, status verification as they may become available or required in specific applications.

To provide to relying parties notice or knowledge functions associated with the revoked certificates requires appropriate publication in a certificate revocation list. The NR-CA operates such a list

according in the context of the CSPs Licensing Scheme in the State of Qatar and within the limits set out by of the laws of the State of Qatar.

The NR-CA is established in the State of Qatar. It can be contacted at the address published in section 1.5 of this CPS. To deliver NR-CA services including the issuance, revocation, renewal, status verification of root-signing certificates to licensed Qatari CSPs and cross-certificates to approved foreign CSPs, the NR-CA operates a secure facility and provides for a disaster recovery facility in Qatar. See section 5 for further details.

In specific the NR-CA's domain of responsibility comprises of the overall lifecycle management of the above mentioned root-signing certificates and cross-certificates including:

- Issuance
- Revocation
- Certificate Validity Status (verification) Service
- Directory Service

1.3.2 Registration Authorities

The CSPs-PMA in the context of the NR-CA operates a single RA with the task to request the issuance and revocation of a certificate under this CPS. In the NR-CA domain, the CSPs-PMA Approval & Licensing team acts as the RA. It is represented by its leader, acting as Registration Authority Officer (RAO). When a subscriber (i.e. a licensed CSP or an approved foreign CSP) requests for the creation of a CA certificate under the NR-CA, it is the Public Key Management and Digital Identity Section in quality of CSPs-PMA that will validate the request and decide whether to issue the CA certificate. For more details section 3.

1.3.3 Subscribers

The subscribers of the NR-CA services are either:

- Licensed Qatari CSPs for their certification services being licensed in accordance with the Qatari CSPs Licensing Scheme as per the E-Commerce Law and the associated Bylaw.
- Approved foreign CSPs for their certification services being approved in accordance with the Qatari CSPs Licensing Scheme as per the E-Commerce Law and the associated Bylaw.

These subscribers and their NR-CA root-signed or cross-certified certification services (e.g. CAs, TSAs):

- Are identified in the Subject field of their certificate issued by the NR-CA.
- Controls the private key corresponding to the public key that is listed in the subscriber certificate.

1.3.4 Relying Parties

Relying parties are entities including natural or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate.

To verify the validity of a digital certificate issued by the NR-CA they receive, relying parties must always verify such a certificate against the NR-CA Certificate Validity Status Service (e.g. CRL, webpage) prior to relying on information featured in such a received certificate.

1.4 Certificate Usage

Certain limitations apply to the usage of certificates issued by the NR-CA that includes the ones stated hereunder.

1.4.1 Appropriate certificate usage

The certificates issued by NR-CA can be used to:

- Sign certificates within a PKI hierarchy. Such certificates can be used to assert the identity of a CA, OCSP server or Time-Stamping Authority (TSA). The purpose of the certificates issued by the NR-CA is to authenticate a CA, OCSP server or Timestamp server.
- Sign certificate revocation lists (CRLs), containing the list of subscribers' revoked certificates.

1.4.2 Prohibited certificate usage

Certain limitations apply to the usage of certificates issued by the NR-CA as stated in this CPS. Rootsigned certifications services are not authorized to issue services that are falling out of the scope of the license they have been granted.

The use of the NR-CA certificate to sign end-user or server certificates (other than licensed or approved CAs, OCSP server or Time-Stamping Authorities) is prohibited.

1.5 Policy Administration

The Public Key Management and Digital Identity Section in quality of CSPs-PMA, is bearing responsibility for the drafting, publishing, OID registration, maintenance, and interpretation of this CPS.

The Policy administration of this CPS is distinct and remains independent from other Policy authorities managing or approving of policies of other CAs, licensed or approved, operating within the domain of the Qatari licensing scheme as defined in the E-Commerce Law

Any policy approved by the NR-CA has to ultimately comply with the provisions of this CPS.

The CSPs-PMA in the context of the NR-CA certification services shall set-up a specific managerial body, a so-called NR-CA Policy Approval Authority (PAA) having the responsibility to manage and operate these specific NR-CA activities.

This NR-CA Policy Approval Authority shall be composed of a specific management cell of CSPs-PMA. The procedure used to add or remove members of this PAA shall be determined and ruled by internal documents. This PAA shall be the highest level management body with final authority and responsibility for:

a. Specifying and approving the NR-CA infrastructure.
b. Specifying and approving the NR-CA practices and policies, in particular the Certification Practice Statements (CPS) and the related Certificate Policies when applicable.
c. Defining the review process for such practices and policies including responsibilities for maintaining the NR-CA CPS and related policies.
d. Defining the review process that ensures that the NR-CA properly implements the above practices.
e. Defining the review process that ensures that the related policies are supported by the NRCA CPS.
f. Publication of the NR-CA CPS and of its revisions.
g. Specifying installation, key ceremonies, operation and life-cycle management (including deprecation) procedures of the NR-CA.
h. Specifying root-signing certification procedures and handling root-signing certification requests.
i. Specifying cross-certification procedures and handling cross-certification requests.
j. Evaluating the proper working of the NR-CA environment.
k. Allocating members to the key ceremonies as witness as well as trusted operatives and key custodians.
l. Evaluating of changes to the NR-CA environment (management, operational, hardware, software and security).

m. Evaluating case-by-case issues where key NR-CA staff/personnel did not respect the security and/or operational procedures, including ethics.
n. Deciding on critical issues in case of incidents, disasters and other severe problems with regards to the NR-CA.

The NR-CA Policy Approval Authority can be contacted at the following address:

QCERT - CSPs-PMA - PAA

Cyber security Sector
P.O.Box 24514, Doha, Qatar
Doha, Qatar, [csppmaqatar@qcert.org]

The CSPs-PMA accepts comments regarding this CPS only when they are addressed to the PAA.

1.6 Definitions and Acronyms

1.6.1 Terminology and definitions

Definitions applicable to the present document are to be found in the "CSPs Licensing Conformity Assessment Criteria - Overview Document" [CS-PI-CSP-PMA-CRT-0001].

All other definitions from the E-Commerce and the associated Bylaw are included by reference when applicable.

1.6.2 Abbreviations

Abbreviations applicable to the present document are to be found in the "CSPs Licensing Conformity Assessment Criteria - Overview Document" [CS-PI-CSP-PMA-CRT-0001].

1.6.3 References

References applicable to the present document are to be found in the "CSPs Licensing Conformity Assessment Criteria - Overview Document" [CS-PI-CSP-PMA-CRT-0001].

The NR-CA conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates [CAB EV Guidelines] published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

The present CPS endorses the following standards: [RFC 3647], [RFC 5280], [RFC 3739], [ETSI 319 411-3], [ETSI EN 319 411-1 V1.2.2] and [ISO/IEC 27001].

2 Publication and Repository Responsibilities

The CSPs-PMA with regards to the NR-CA activities publishes information about all digital certificates it issues in (an) online publicly accessible Certificate Dissemination Webpage at [QPKI URL]. The NR-CA reserves its rights to publish certificate status information on third party repositories.

The CSPs-PMA with regards to the NR-CA activities retains an online repository of documents where it makes certain disclosures about NR-CA practices, procedures and the content of certain of its policies including the present CPS. It reserves its right to make available and publish information on its policies by any means it sees fit.

PKI participants are notified that the CSPs-PMA may publish information they submit directly or indirectly to the CSPs-PMA on publicly accessible directories for purposes associated with the provision of NR-CA issued electronic certificate validity status information.

The NR-CA publishes digital certificate status information in frequent intervals as indicated in this CPS. The provision of NR-CA issued electronic certificate validity status information is a 24/7 available service.

The NR-CA publishes CRL's at regular intervals at [QPKI URL]. The NR-CA publishes CRLs including any changes since the publication of the previous CRL, at regular intervals.

The CSPs-PMA with regards to the NR-CA activities maintains the Certificate Dissemination Webpage, the CRL distribution point and the information on this URL until minimum 7 years after the expiration date of all certificates, containing the CRL distribution point. Approved versions of documents to be published on the Repository are uploaded within 24 hours.

Due to their sensitivity, the CSPs-PMA with regards to the NR-CA activities refrains from making publicly available certain subcomponents and elements of such documents including certain security controls, procedures related with the functioning of inter alia registration authorities, internal security polices etc. Such documents and documented practices are, however, conditionally available to designated authorized parties in the context of audit(s) that the CSPs-PMA owes duty to with regards to the NR-CA activities.

The certificate dissemination webpage, the document repository (containing e.g. CPS) and the CRLs are publicly available on the CSPs-PMA website on the Internet.

3 Identification and Authentication

The RA maintains documented practices and procedures to authenticate the identity and/or other attributes of a certificate subscriber. Prior to requesting the issuance of a certificate the RA verifies the identity of the organization that requests a root-signing certificate or cross-certificate under the NR-CA. See section 3.2 for further details.

The RA authenticates the requests of parties wishing the revocation of certificates under the provisions of the present CPS.

3.1 Naming

To identify the applicant certification service (e.g. CA, TSA) to be either root-signed or cross-certified (here after referred to as the **applicant**), the NR-CA follows certain naming and identification rules that include types of names assigned to the subject, such as X.500 distinguished names RFC-822 names and X.400 names. These rules will be applied by the RA (i.e. the CSPs-PMA).

Names do [not] have to be meaningful or unique. Subscribers cannot be anonymous or pseudonymous. Names can only contain trademarks in case the subscriber has the legal right to use the trademark in question.

3.2 Initial Identity Validation

The Initial Identity Validation is prepared during the assessment of the applicant in the framework of the Qatari licensing scheme defined in the context of the E-Commerce Law and the associated Bylaw. It will be verified by the RA according to the requirements of Identity Validation defined according to internal policies and procedures documented in the "CSPs-PMA licensing scheme" documents.

3.3 Identification and Authentication for Re-key Requests

Same provisions as those defined in sections 3.1 and 3.2 apply.

3.4 Identification and Authentication for Revocation Requests

For the identification and authentication procedures of revocation requests, a formal request is required to be addressed to the RA and issued by the entity that performed the initial subscription, or by the CSPs-PMA that has the final authority to cancel the license (or respectively the approval) of a licensed Qatari certification service (respectively of an approved foreign certification service).

Suspensions on any of the NR-CA issued root-signing or cross-certificates is not allowed.

4 Certificate Life-Cycle Operational Requirements

Any of the certification services (e.g. CA, TSA) for which a certificate has been issued by the NR-CA (including cross-certification) has a continuous obligation to inform the RA (i.e. the CSPs-PMA) of all changes in the information featured in a certificate during the operational period of such certificate or of any other fact that materially affects the validity of a certificate. In particular this obligation is linked to the notification obligation of any change to its certification practices and operations as required in the CSPs- Licensing Scheme.

The RA will then take appropriate measures to make sure that the situation is rectified (e.g. ask the CA for the revocation of the existing certificates and the generation of new certificates with the correct data in case of incorrectly issued certificate).

The NR-CA issues or revokes certificates only at the request of the RA to the exclusion of any other entity, unless explicitly instructed so by the RA, with the exception of a proven key compromise. In case of a proven CA key compromise, the NR-CA will immediately revoke the certification service certificate concerned, even without request from the RA.

To fulfill its tasks the CSPs-PMA with regards to the NR-CA activities may use the services of third party agents. Towards the subscribers and relying parties the CSPs-PMA assumes full responsibility and accountability for acts or omissions of all third-party agents it uses to deliver NR-CA certification services.

4.1 Certificate Application

The NR-CA acts upon request of the RA that has the authority and is designated to request a root-signing or cross-certification.

The subscriber will issue to the RA its request for certificate issuance to the applicant (i.e. the subject of the certificate to be issued). It is the responsibility of the RA to identify the applicant, to verify whether he is who he claims to be, to verify whether he is either licensed (or approved) and mandated to request a root-signing certificate (or cross-certificate) for the organization for whom he acts and to validate the information to be certified.

The initial Subscriber (and applicant) enrolment requires a face-to-face procedure where at least, both Subscriber and RA Officer are present. During this procedure, the registration documents will be validated by the RA Officer; the identity and authorizations of the Subscriber will also be verified. Before the face-to-face procedure takes place, the Subscriber generates a PKCS#10 request for the certificate request (the applicant keys are generated prior the request). Conform to PKCS#10, the request is signed by the private key, enabling the Subscriber to prove the possession of this key. A print out of the key to be certified is signed by the subscriber and the RA and kept archived together with the Applicant Definition form.

In case of root-signing or cross-certification process where a certificate already exists for the public key (e.g. CAs, OCSP services or Time-Stamping Authorities) with existing keys, this existing certificate will be provided to the RA as well so that the RA can verify that the same public key (and thus also the same private key) is concerned in the PKCS#10 request and as present in this existing certificate of the CA to be root-signed or cross-certified. A print out of the certificate and the key to be certified is signed by the subscriber and the RA and kept archived together with the Applicant Definition form.

4.2 Certificate Application Processing

The RA acts upon a certificate application (request) to validate the identity of the requesting organization.

Subsequently, the RA either approves or rejects the certificate application. Such approval or rejection does not necessarily have to be justified to the applicant or any other party.

During the assessment of the applicant in the framework of the Qatari licensing scheme defined in the E-Commerce Law and the associated Bylaw, all details about the applicant and its certification service are defined, including the identification of the organization that will act as CSP, all required procedures and documentation (including CPS, CPs, etc.), description of the applicant purpose, the required applicant certificate profile and the values of each and any attribute that should be present in the applicant certificate (together further referred to as “Applicant Definition”). This Applicant Definition is an integral part of the certificate request. Without it the NR-CA is not able to process the CA certificate request.

If the request is accepted, the signed certificate request will be delivered by the RA to the NR-CA.

Upon final agreement of an Applicant Definition, the RA, and the NR-CA will agree upon a date and a backup date when mandated people can make themselves available at the NR-CA premises to perform a certification services.

4.3 Certificate Issuance

The NR-CA trusted operatives and NR-CA Key custodians gather at the NR-CA premises to activate the NR-CA key and to issue the certificate.

The RA officer (RAO) comes personally at the NR-CA location and is duly authenticated through this physical presentation. More than one member of the CSPs-PMA PAA make authorization of RAO assigned personnel in writing. This authorization is verified by the NR-CA trusted operatives and NR-CA Key custodians to authenticate the RAO.

The NR-CA specifically verifies the completeness, integrity and uniqueness of the data presented by the RA and notifies the RA of any problem thereof. The NR-CA will indicate whether the Applicant Definition is technically feasible. In case the NR-CA does not accept the Applicant Definition, the NR-CA, the RA and the requesting organization will together work out an acceptable Applicant definition.

A request from the RA is granted approval provided that:

- It is validly formatted.
- It comes from the duly authorized RA.
- Contains valid subscriber data

A formal approval to perform the Ceremony is signed by the NR-CA persons in charge of the certification ceremony and the RA officer. This can be done on the signed print out of the key to be certified.

The NR-CA ensures that the certificate issued by the NR-CA contains all data that was presented to it in the request of the RA.

Following issuance of a certificate, the NR-CA posts an issued certificate on the Certificate Repository and delivers the certificate to RA officer for further publication in the Qatar Trusted List and for handover to the subscriber.

4.4 Certificate Acceptance

The Subscriber is responsible for checking the details associated with their certificate. Usage of the certificate is considered as acceptance.

In case the Subscriber does not accept the certificate, the reason for non-acceptance will be discussed. If no measures can be agreed upon in order to obtain the acceptance the certificate will be revoked.

If it is possible to start the ceremony over in a way that the reason for non-acceptance will not reoccur, the ceremony will be repeated to generate a certificate that can be agreed.

No other entities or organizations are notified directly of the certificate issuance. They are indirectly notified through the update of the Register and/or Qatar Trusted List.

4.5 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below.

4.5.1 Subscriber duties

Unless otherwise stated in this CPS, subscriber‘s duties include the ones below:

- Refraining from tampering with a certificate.
- Only using certificates for legal and authorized purposes in accordance with the common general requirements applicable to all CSPs, and with its own CPS.
- Using a certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorized use of their private keys.
- Refrain from using the certificate outside its validity period or after it has been revoked.

4.5.2 Relying party duties

A party relying on a certificate issued by the NR-CA will:

- Use proper cryptographic tools to validate the certificate signature and validity period.
- Validate the certificate by using a CRL or a web based certificate validity status information service in accordance with the certificate path validation procedure.
- Trust the certificate only if it has not been revoked and within the validity period.
- Rely on the certificate, as may be reasonable under the circumstances.
- Trust the certificate only for the signing of certificates and CRLs.

4.6 Certificate Renewal

Certificate renewal will only be allowed for Subscriber whose key validity exceeds the expiry date of the certificate, and when the Subscriber has obtained a new license for the certification service concerned in accordance with the Qatari CSPs Licensing Scheme defined in the E-Commerce Law and the associated Bylaw.

Certificate renewal may occur in exceptional circumstances decided by the NR-CA PAA, amongst other:

- Upgrade of the cryptographic algorithms

- Disaster recovery (e.g. Subscriber's certificates revoked, NR-CA exceptional rekey)

Certificate Renewal of CA certificates issued by the NR-CA is treated as a new CA certificate application.

4.7 Certificate Re-key

Re-key of root-signed or cross-certified certification services being already issued certificates by the NR-CA shall be treated as a new certificate application.

4.8 Certificate Modification

The NR-CA does not allow certificate modification. The Subscriber must immediately inform the CSP Certification Service of any changes to the data on the Certificate, or when the certified data has become inaccurate or has changed in any way. The Subscriber must ask the CSP to revoke the Certificate. The Certificate revocation process is then started immediately. The revocation procedures are set out in Section 4.9 of the present CPS.

In case the Subscriber wants to change the certified information, or has requested the revocation of his/her Certificate due to circumstances mentioned in the previous paragraph, and wishes to be issued a new Certificate, the Subscriber shall process to a full Certificate application as for initial enrolment.

4.9 Certificate Revocation and Suspension

Upon duly authenticated request from the RA or the CSPs-PMA, the NR-CA Operator revokes or suspend an existing certification service's certificate.

The RA requests promptly the revocation of a certificate after:

- Having received notice by the subscriber that there has been a loss, theft, modification, unauthorized disclosure, or other compromise of the private key of the certificate's subject.
- There has been a modification of the information contained in the certificate of the certificate's subject.

The RA requests promptly the suspension of a certificate after:

- Notifying that the CSP:
    - no longer complies with rules and controls stated on the E-Commerce law, the associated Bylaw and the CSPs-PMA licensing scheme documents.
    - License has been expired and the CSP has not submitted renewal licensing application.

Upon having had proof of compromise of the private key of the certificate's subject, the NR-CA will immediately revoke the relevant certificate. The NR-CA will then notify the RA.

The E-Commerce Law imposes CSPs to obtain a license in order to be allowed to operate. This license will be delivered for a maximum period of 5 years after which a new license is required. Any certificate delivered by the NR-CA based on such license SHALL be revoked when the license has been cancelled by the CSPs-PMA. In this case, the CSPs-PMA requests promptly the revocation of the certificate to the NR-CA.

Revocation is final. Suspension is temporary.

The NR-CA publishes notices of revoked or suspended certificates in the CRL and in the Repository.

4.10 Certificate Status Services

The NR-CA makes available on a 24/7 basis a certificate validity status information services including CRLs and appropriate web pages (see chapter 2 Publication and Repository Responsibilities).

CRL

- CRLs are signed and time-stamped by the NR-CA.
- A CRL is issued each 6 months, at an agreed time. In addition, a new CRL will be generated and published following the revocation of any certificate.
- The CSPs-PMA makes all CRLs issued in the previous 12 months available on its Website.

4.11 End of Subscription

Subscriber subscription ends when a certificate is revoked, expired or the service is terminated.

4.12 Key Escrow and Recovery

Subscriber's key backup, escrow and key recovery are not applicable as these services are not provided by the CSPs-PMA in the context of the NR-CA activities.

5 Management, Operational and Physical Controls

This section describes non-technical security controls used by the NR-CA Operator to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

5.1 Physical Security Controls

The CSPs-PMA ensures that appropriate physical controls are implemented on the NR-CA (hosting) premises. The NR-CA's premises physical controls include the following:

- The site hosting the NR-CA implement proper security controls, including access control, intrusion detection and monitoring. Access to the sites is limited to authorized personnel listed on an access control list, which is subject to audit.
- The NR-CA's secure premises within these sites are located in an area appropriate for high security operations. These premises feature numbered zones and locked rooms, cages, safes, and cabinets.
- Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones such as locating NR-CA operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists.
- Power and air conditioning operate with a high degree of redundancy.
- Premises are protected from any water damages.
- Prevention and protection as well as measures against fire exposures are implemented.
- Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.
- To prevent unwanted disclosure of sensitive data, waste is disposed of in a secure manner.
- An off-site backup is implemented.

5.2 Procedural Controls

The CSPs-PMA, and any 3rd party involved in NR-CA activities (in particular the NR-CA Operator), follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of electronic signature-related technologies.

The CSPs-PMA with regards to the NR-CA activities obtains a signed statement from each member of the staff concerned on not having conflicting interests with the NR-CA activities, maintaining confidentiality and protecting personal data.

All members of the staff operating the key management operations, administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

The CSPs-PMA conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make due diligence attempt to determine their trustworthiness and competence.

Where dual or multiple control is required at least two trusted members of the NR-CA staff need to bring their respective and split knowledge in order to be able to proceed with the ongoing operation.

The CSPs-PMA with regards to the NR-CA activities ensures that all actions with respect to the NR-CA can be attributed to the system of the NR-CA and the member of the NR-CA staff that has performed the action.

The CSPs-PMA ensures separation among the following discreet work groups:

- NR-CA operating personnel that manages operations on certificates.
- Administrative personnel to operate the platform supporting the NR-CA.
- Security personnel to enforce security measures.
- Internal audit personnel.

5.3 Personnel Security Controls

The CSPs-PMA ensures implementation of security controls with regard to the duties and performance of the members of its staff with regards to the NR-CA activities. These security controls are documented in an internal confidential policy and include the areas below.

5.3.1 Qualifications, Experience, Clearances

The CSPs-PMA with regards to the NR-CA activities ensures that checks are performed to establish the background, qualifications, and experience needed to perform within the competence context of the specific job. Such background checks include:

- Criminal convictions for serious crimes.
- Misrepresentations by the candidate.
- Appropriateness of references.
- Any clearances as deemed appropriate.

5.3.2 Background Checks and Clearance Procedures

The CSPs-PMA with regards to the NR-CA activities makes the relevant checks on prospective employees by means of status reports issued by a competent authority or third-party statements.

5.3.3 Training Requirements and Procedures

The CSPs-PMA with regards to the NR-CA activities makes available relevant technical training for their personnel to perform their NR-CA functions.

5.3.4 Retraining Period and Retraining Procedures

Periodic training updates will be carried out to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.5 Sanctions against Personnel

The CSPs-PMA with regards to the NR-CA activities sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the NR-CA personnel, as it might be appropriate under the circumstances and as per the prevailing HR Policy and Country Law.

5.3.6 Controls of independent contractors

Independent NR-CA component services subcontractors and their personnel are subject to the same background checks as the CSPs-PMA personnel with regards to the NR-CA activities. The background checks include:

- Criminal convictions for serious crimes.
- Misrepresentations by the candidate.
- Appropriateness of references.
- Any clearances as deemed appropriate.
- Privacy protection.
- Confidentiality conditions.

5.3.7 Documentation for initial training and retraining

The CSPs-PMA with regards to the NR-CA activities makes available documentation to personnel, during initial training and retraining.

5.4 Audit Logging Procedures

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. The CSPs-PMA with regards to the NR-CA activities ensures that the following controls are implemented:

- The NR-CA event logging system records events that include but are not limited to:
    - NR-CA Key management.
    - Issuance of a certificate.
    - Revocation of a certificate.
    - Publishing of a CRL.
- All event-logging records related to the NR-CA activities are audited.
- Audit trail records contain:
    - The identification of the operation.
    - The data and time of the operation.

- The identification of the certificate, involved in the operation.
- The identity of the transaction requestor (i.e. the RAO in the event of certificate issuance or revocation, or more than one member of the CSPs-PMA PAA for the events other than certificate issuance).

In addition, the CSPs-PMA with regards to the NR-CA activities maintains internal logs and audit trails of relevant operational events in the infrastructure, including, but not limited to:

- Start and stop of servers.
  - Outages and major problems.
  - Physical access of personnel and other persons to sensitive parts of the NR-CA site.
  - Backup and restore.
  - Report of disaster recovery tests.
  - Audit inspections.
  - Upgrades and changes to systems, software and infrastructure.
  - Security intrusions and attempts at intrusion.
- Other documents that are required for audits include:
  - Infrastructure plans and descriptions.
  - Physical site plans and descriptions.
  - Configuration of hardware and software.
  - Personnel access control lists.

The CSPs-PMA with regards to the NR-CA activities ensures that designated personnel reviews log files at regular intervals and detects and reports anomalous events.

Log files and audit trails are archived for inspection by the authorized personnel of the CSPs-PMA, the NR-CA Operator, the RA and designated auditors. The log files are properly protected by an access control mechanism, so that no others can have access. Log files and audit trails are backed up.

Auditing events are not given log notice.

5.5 Records Archival

The CSPs-PMA with regards to the NR-CA activities keeps records of the following items:

- All certificates for a period of a minimum of 10 years after the expiration of that certificate.
- Audit trails on the issuance of certificates for a period of a minimum of 10 years after issuance of a certificate.
- Audit trail of the revocation of a certificate for a period of a minimum of 10 years after revocation of a certificate.
- CRLs for a minimum of 10 years after publishing.

The very last back up of the NR-CA archive will be retained for 10 years following the issuance of the last certificate by the NR-CA.

The CSPs-PMA with regards to the NR-CA activities keeps archives in a retrievable format.

The CSPs-PMA with regards to the NR-CA activities ensures the integrity of the physical storage media and implements proper backups to prevent data loss.

Archives are accessible to authorized personnel of the CSPs-PMA, the NR-CA Operator and the RA.

5.5.1 Types of records

The CSPs-PMA with regards to the NR-CA activities retains in a trustworthy manner records of digital certificates, audit data, NR-CA systems information and documentation.

5.5.2 Retention period

The CSPs-PMA with regards to the NR-CA activities retains in a trustworthy manner, records of digital certificates for a term as indicated under article 5.5 in this CPS.

5.5.3 Protection of archive

Only the records administrator (member of staff assigned with the records retention duty) may access a NR-CA archive. Measures are taken to ensure:

- Protection against modification of archive, such as storing the data on a write once medium.
- Protection against deletion of archive.
- Protection against deterioration and/or obsolescence of the media on which the archive is stored, such as a requirement for data to be migrated periodically to unused media.

5.5.4 Archive backup procedures

A full backup is taken at each Key Ceremony.

5.5.5 Time-stamping of records

The precise time of archiving all events, records and documents in electronic form listed in section 5.4 and 5.5 shall be recorded with reliable time source.

5.5.6 Archive Collection

The NR-CA archive collection system is internal.

5.5.7 Procedures to obtain and verify archive information

Only CSPs-PMA and NR-CA staff members with a clear hierarchical control and a definite job description may obtain and verify archive information.

The CSPs-PMA with regards to the NR-CA activities retains records in electronic or in paper-based format.

5.6 Key Changeover

Only applicable in the context of NR-CA key pair re-generation and re-installation (see section 6.1 of the present CPS) and in the context of NR-CA private key compromise (see section 5.7.3 of the present CPS). In that case, the new public key will be presented in a self-signed certificate.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and compromise handling procedures

In a separate internal document, the CSPs-PMA with regards to the NR-CA activities specifies applicable incident, compromise reporting and handling procedures. The CSPs-PMA specifies the recovery procedures used when computing resources, software, and/or data are corrupted or suspected of being corrupted.

5.7.2 Computing resources, software, and/or data are corrupted

The CSPs-PMA acting as CSP with regards to the NR-CA activities, supported in its tasks by the NR-CA Operator, and by all other PKI Participants (other than Subscribers and Relying Parties), establishes the necessary measures to ensure full recovery of NR-CA services in case of a disaster, corrupted servers, software or data.

The CSPs-PMA with regards to the NR-CA activities establishes:

- Disaster recovery resources in dual locations sufficiently distant from each other.
- Fast communications between the two sites to ensure data integrity.

Disaster recovery infrastructure and procedures shall be fully tested at least once a year with witnessing of more than one member of the CSPs-PMA PAA.

5.7.3 Entity private key compromise procedures

For Subscribers key compromise, see section 4.9 of the present CPS.

Compromise of the NR-CA private key(s) or of the associated activation data shall imply the immediate revocation of the certificate of the compromised key(s). The revocation of a NR-CA Key is a critical process and related procedures are described in internal private documents.

The CSPs-PMA with regards to the NR-CA activities, will additionally take the following measures:

- Notify the NR-CA community.
- Notify all other PKI Participants.

- List the certificate of the corrupted NR-CA in the CRL (in this case the CRL is called ARL. CRLs and ARLs can be merged within a single file, but revoked NR-CA certificate will be additionally listed on the NR-CA Certificate Dissemination Webpage).
- Revoke all the certificates signed by the corrupted NR-CA.
- After assessing the reasons for corruption of the NR-CA private key and revocation of the NR-CA certificate, and after having taken all the necessary measures to avoid the cause of revocation in the future, and after obtaining authorization from CSPs-PMA PAA, a new key pair and the associated certificate may be generated.

5.7.4 Business continuity capabilities after a disaster

The CSPs-PMA with regards to the NR-CA activities establishes the necessary measures to full and automatic recovery of the on-line services such as CRL availability, OCSP service in case of a disaster, corrupted servers, software or data.

The CSPs-PMA with regards to the NR-CA activities establishes the necessary measures to ensure full recovery of the off-line services service in case of a disaster, corrupted servers, software or data.

A Business Continuity Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

5.8 CA or RA Termination

In the case of NR-CA or RA termination, the CSPs-PMA with regards to the NR-CA activities shall ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

The CSPs-PMA with regards to the NR-CA activities shall inform within a reasonable delay the following of the termination:

- All Subscribers.
- All other PKI Participants.
- Relying parties to the extend feasible.

The CSPs-PMA with regards to the NR-CA activities shall terminate all authorization of subcontractors to act on behalf of the terminated service (NR-CA or RA) in the performance of any functions related to the process of issuing root-signing certificates or cross-certificates.

Before termination of the NR-CA activities, the CSPs-PMA will take measures to transfer the following information to a designated organization: all information, data, documents, repositories, archives and audit trails with regards to the NR-CA and shall maintain or transfer the validation status services URLs as mentioned in the certificates that would still be valid at the moment of termination, until expiry of the latest certificate.

6 Technical Security Controls

This section defines the security measures the CSPs-PMA with regards to the NR-CA activities takes to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key access tokens).

6.1 Key Pair Generation and Installation

The CSPs-PMA with regards to the NR-CA activities implements and documents key generation procedures in accordance with this CPS.

6.1.1 CA Private Key Pair Generation

6.1.1.1 NR-CA

The CSPs-PMA with regards to the NR-CA activities undertakes the generation of the NR-CA key pair(s) and protects its private key(s) in a Hardware Security Module, using a trustworthy system and takes the required precautions to prevent compromise or unauthorized use, according to a documented procedure. The CSPs-PMA ensures the implementation and documentation of key generation procedures, in line with this CPS. It acknowledges public, international and ETSI standards on trustworthy systems and is ruling the way:

- At least four trusted persons participate in the generation and installation of NR-CA private key(s): two trusted operatives and two key custodians.
- The CSPs-PMA National Root CA Key Generation Ceremony will be witnessed by the CA's Qualified Auditor (see 8 Compliance Audit and Other Assessments)
- The CSPs-PMA ensures the distribution of the tokens giving access to the private key(s) to the their trusted operatives and key custodians.
- The NR-CA Operator and key custodians act upon authorization by the CSPs-PMA who is the owner of the NR-CA private keys, to perform cryptographic operations using the NR-CA private key(s).
- The Qualified Auditor will then issue a report opining that the NR-CA, during its NR-CA Key Pair and Certificate generation process:
    - Documented its NR-CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement.
    - Included appropriate detail in its NR-CA Key Generation Script.
    - Maintained effective controls to provide reasonable assurance that the NR-CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its NR-CA Key Generation Script.
    - Performed, during the NR-CA key generation process, all the procedures required by its NR-CA Key Generation Script.
- A video of the entire key generation ceremony will be recorded and stored securely for auditing purposes.

6.1.1.2 Issuing CAs

The security measures that are in place for key generation of Issuing CA's are governed by their own CPS, following the minimal requirements of the Qatari Licensing Scheme defined in the E-Commerce Law and the associated Bylaw.

6.1.2 Private key provisioning

6.1.2.1 NR-CA

The private key is generated during the Key Ceremony procedure as ruled in a documented procedure.

6.1.2.2 Subscribers

The CSPs-PMA with regards to the NR-CA activities does not generate private keys for Subscribers.

6.1.3 Public key provisioning

6.1.3.1 NR-CA

The public key is generated and certified during the same Key Ceremony procedure.

6.1.3.2 Subscribers

Subscribers bring the public key of their applicant certification services to be certified (i.e. rootsigned CAs, cross-certified CAs, OCSP servers, Time-Samping Authorities) physically face-to-face registration by the RA (see section 4.1 Certificate Application).

6.1.4 CA's public key provisioning to potential relying parties

The CSPs-PMA with regards to the NR-CA activities will publish its public key(s) on its dedicated dissemination web page.

6.1.5 Key sizes

The minimum size of the modulus, n, for the NR-CA Keys using the RSA SHA-256 algorithm is 4096 bits.

6.1.6 Public key parameter generation

Public key RSA exponents are chosen secure. Public Key module generation is done with state of the art parameter generation technology. Parameter generation is implemented using state of the art technology and shall be regularly re-evaluated regarding new advances in cryptology.

6.1.7 Key usage

The NR-CA uses private signing keys only for signing CRLs and applicant certification services (i.e. CA's, OCSP server and Time-Stamping Authorities) certificates in accordance with the intended use of each of these keys. Other usages are restricted.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 NR-CA Key Generation Devices

The NR-CA uses a secure cryptographic device, Hardware Security Module (HSM), to store the private key meeting the appropriate FIPS 140-1 level 3 requirements. The device has received an EAL4+ CC certification from the "Canadian Common Criteria Evaluation and Certification Scheme" and the related document bear number 383-4-114-CR and is FIPS 140-2 Level 3 certified (NIST Certificate 1776).

The HSMs do not leave the secured environment of the NR-CA secure premises. In case the HSMs require maintenance or repair, the HSMs will be securely transported to the producer. The private keys will not be present in the HSM when brought outside the secured environment of the NR-CA for maintenance or repair. When in use, the HSMs are physically present in the secured environment of the NR-CA.

6.2.2 NR-CA Private key shared control

NR-CAs keys are activated only during circumstances described in the XXXXXXX document.

The NR-CA private keys remains controlled by multiple authorized persons, to safeguard and improve the trustworthiness of private keys; the NR-CA trusted operatives and key custodians. These trusted persons are assigned with the task to activate and deactivate the NR-CAs private keys.

A certain number of persons 'm' (at least 2), out of 'n' persons (3 persons), the total number of authorized holders, needs to be present concurrently together with two (2) NR-CA trusted operatives to activate or re-activate the NR-CA private key.

The CSPs-PMA PAA keeps written, auditable, records of tokens and related password distribution to trusted operatives and key custodians. In case trusted operatives or key custodians are to be replaced, it shall keep track of the renewed tokens and/or password distribution.

More than one member of the CSPs-PMA PAA makes authorization of NR-CA private key protection tokens and related password distribution and of assigned personnel in writing.

6.2.3 NR-CA Private Key escrow

Private keys of the NR-CA may not be escrowed. The CSPs-PMA with regards to the NR-CA activities implements internal disaster recovery measures.

6.2.4 NR-CA Private key backup

The private key(s) is (are) backed up, stored and recovered by multiple and appropriately authorized members of NR-CA staff serving in trustworthy positions. More than one member of the CSPs-PMA PAA make authorization of key back up and assigned personnel in writing.

A backup of the generated key material is taken and stored under the same security measures as the primary key material.

6.2.5 NR-CA Private key archival

Not applicable.

6.2.6 Private key transfer into or from a cryptographic module

Not applicable.

6.2.7 Private key storage on cryptographic module

See section 6.1.1 CA Private Key Pair Generation.

6.2.8 Method of activating private key

The NR-CA private keys remain under m out of n multi-personnel control. NR-CA trusted operatives and key custodians are assigned with the task to activate and deactivate the NR-CA private keys. NRCA keys are then active only for defined time periods.

Subscriber's private key activation is the responsibility of the Subscriber.

6.2.9 Method of deactivating private key

The NR-CA private keys remain under m out of n multi-personnel control. NR-CA trusted operatives and key custodians are assigned with the task deactivate the NR-CA private keys.

6.2.10 NR-CA Private Key Destruction

At the end of their lifetime the private keys are destroyed by at least three trusted NR-CA staff members at the presence of at least one representative of the CSPs-PMA PAA, in order to ensure that these private keys cannot ever be retrieved and used again.

The NR-CA keys are destroyed by removing permanently from any hardware modules the keys are stored on.

Key destruction process is documented in XXXXX document and any associated records are archived.

The decision for private key destruction outside the context of the end of its lifetime needs to be authorized in writing by multiple members of the CSPs-PMA PAA. This decision includes the assignment of the personnel.

6.2.11 Cryptographic Module Rating

To protect against attacks on the secure devices or HSMs including Side-Channel Attacks (e.g. timing, power consumption, EM emission, fault injection) and attacks against the random number generator secure devices and HSMs should be successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High. The device has received an EAL4+ CC certification from the "Canadian Common Criteria Evaluation and Certification Scheme" and the related document bear number 383-4-114-CR.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The CSPs-PMA acting as CSP with regards to the NR-CA activities archives its own NR-CA public keys. See section 5.5 of the present CPS for archival conditions.

6.3.2 Certificate operational periods and key pair usage periods

Considering that the Subscriber certificates will be valid for a period of maximum 10 years, the NR-CA Certificate shall have a validity at least greater than 5 years after the latest Subscriber certificate issuance, augmented with a period taking into account the NR-CA private key usage period and rekey activities.

The certificate validity and key usage periods within the CSPs-PMA hierarchy are defined as follows:

- NR-CA certificates are valid for 20 years and two months (re-key activities shall be planned within 2 months at the end of the private key usage period), with a key usage period of 15 years.
- Issuing certificates's validity is aligned on the license. They are valid for 10 years by default, which is the duration of the license. However if a new certificate is issued to the Subscriber during the period of validity of the license (e.g. if the Subscriber renew its key pair), the new certificate validity will be aligned on the remaining license's duration.

6.4 Activation Data

6.4.1 Activation data protection

The CSPs-PMA acting as CSP with regards to the NR-CA activities ensures that activation data associated to NR-CAs private keys and operations are securely generated, managed, stored and archived as described in the relevant sub-section of sections 6.1 and 6.2.

Subscriber's activation data protection is the responsibility of the Subscriber. This should be managed in accordance with the requirements specified in their own CPS, following the minimal requirements of the Qatari CSPs Licensing Scheme established in the context of the E-Commerce law and the associated Bylaw.

6.4.2 Other aspects of activation data

Not applicable.

6.5 Computer Security Controls

The CSPs-PMA ensures that computer security controls are implemented in compliance with the technical standard [ETSI EN 319 411-1 V1.2.2].

6.6 Life Cycle Security Controls

The CSPs-PMA ensures that periodic development control, security management and life cycle security controls are implemented in compliance with the technical standard [ETSI EN 319 411-1 V1.2.2].

6.7 Network security controls

The CSPs-PMA acting as CSP with regards to the NR-CA activities ensures the maintenance of a high-level network of systems security. Network intrusions are monitored and detected. In specific:

- The NR-CA related website provides for encrypted connections through the Secure Socket Layer (SSL) protocol and anti-virus protection.
- The NR-CA network is protected by an intrusion detection system.
- It is prohibited to access sensitive NR-CA resources including NR-CA databases from outside of the NR-CA‘s own network.
- There are no online connections with any party that allow atomized requests regarding certificate management (including certification requests and revocation requests).

7 Certificates and CRL Profiles

This section is used to specify the Certificate and CRL formats. This includes information on profiles, versions, and extensions used.

7.1 Certificate Profile

7.1.1 Version number(s)

X.509 v3 is supported and used for all certificates related to the NR-CA.

The NR-CA Certificate profile is further described in the following table. All fields of type DirectoryString are of type UTF8String.

NR-CA Certificate Profile								
Attribute	**Field**	**IN[1]**	**RFC 5280 Ref.**	**CE[2]**	**O/M[3]**	**CO[4]**	**Value**	**Comment**
Certificate					M			
TBSCertificate								
Signature				False	M			
	algorithm		4.1.1.2		M	S	OID = 1.2.840.113549.1.1.11 RSA with SHA-256.	
	signatureValue		4.1.1.3		M	D	Issuing CA Signature.	value inserted here dependent on algorithm selected
TBSCertificate			4.1.2					
Version				False				
			4.1.2.1		M	S	Value = "2"	Version 3

[1] IN = Included: Attribute / field included within the certificate profile.

[2] CE = Critical Extension.

[3] O/M: O = Optional, M = Mandatory.

[4] CO = Content: S = Static, D = Dynamic, F = Formatted by CA, V = Validated by CA.

NR-CA Certificate Profile								
Attribute	**Field**	**IN**	**RFC 5280 Ref.**	**CE**	**O/M**	**CO**	**Value**	**Comment**
SerialNumber				False				
	CertificateSerialNumber		4.1.2.2		M	FDV	Validated on duplicates.	
signature				False	M			
	algorithm		4.1.2.3 (= 4.1.1.2)		M	S	OID = 1.2.840.113549.1.1.11 RSA with SHA-256	value inserted here MUST match the OID in signatureAlgorithm field in the sequence Certificate (rfc 5280, section 4.1.1.2)
issuer			4.1.2.4	False	M	S		
	countryName				M	S	QA	Will be encoded according to "ISO 3166-1alpha-2 code elements". PrintableString, size 2 (rfc5280)
	organizationUnitName				O	S	CSPs-PMA	OU fields are an option UTF8 encoded
	organizationName				O	S	ictQATAR	UTF8 encoded
	commonName				O	S	Qatar National Root CA	UTF8 encoded

Validity			4.1.2.5	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore					D	Certificate generation process date/time.	
	NotAfter					D	Certificate generation process date/time + [242] Months	
subject			4.1.2.6	False	M			

NR-CA Certificate Profile								
Attribute	**Field**	**IN**	**RFC 5280 Ref.**	**CE**	**O/M**	**CO**	**Value**	**Comment**
	countryName				M	S	QA	Will be encoded according to "ISO 3166-1alpha-2 code elements". PrintableString, size 2 (rfc5280)
	organizationUnitName				O	S	CSPs-PMA	OU fields are an option UTF8 encoded
	organizationName				O	S	ictQATAR	UTF8 encoded
	commonName				O	S	Qatar National Root CA	UTF8 encoded
subjectPublicKeyInfo			4.1.2.7	False	M			
	algorithm						RSA	
	subjectPublicKey				M		Public Key: Key length: 4096 (RSA)	
Extensions			4.1.2.9		M			
Authority Properties								
authorityKeyIdentifier			4.2.1.1	False	O			Mandatory in all certificates except for self-signed NRCA certificates

	keyIdentifier				M		SHA-1 Hash of the NRCA public key	When this extension is used this field MUST be supported as a minimum
	authorityCertIssuer				O			
	(1) authorityCertSerialNauthorityCertSerialNumber				O			
authorityInfoAccess				False	O			This field is optional and can be included, as long as it is not marked critical

NR-CA Certificate Profile								
Attribute	**Field**	**IN[10]**	**RFC 5280 Ref.**	**CE[11]**	**O/M[12]**	**CO[13]**	**Value**	**Comment**
	AccessMethod						Id-ad-2	
	accessLocation						http:// [URL to be defined]/NR-CA.crt	
	AccessMethod							
	accessLocation							
cRLDistributionPoints			4.2.1.13	False	M			
	distributionPoint				M	S		

fullName				M		http:// [URL to be defined] /NR-CA.crl	UTF8String Path where the CRL resides (distribution point 1) RFC 5280 states that when the HTTP or FTP URI scheme is used, the URI MUST point to a single **DER encoded CRL** as specified in [RFC2585] **while** [3ext] states that this field MUST be ldap, http or https, Participants of the PKD MUST include PKD-URL. If http or https is used, the url MUST point to a ldif. Although ldif can be build upon DER encoded crl, one wonders whether one shouldn't read the contrary (i.e. ldif for ldap distributionpoints)
reasons				X			
(2) cRLIssuer				X			

NR-CA Certificate Profile								
Attribute	**Field**	**IN**	**RFC 5280 Ref.**	**CE**	**O/M**	**CO**	**Value**	**Comment**
IssuerAltName			4.2.1.7	False	X			This field should NOT be used
	(3)							
Subject Properties								
subjectAltName			4.2.1.6	False	X			This field should NOT be used
subjectKeyIdentifier			4.2.1.2	False	M			
	keyIdentifier				M	Fixed	The Key Identifier comprises a four-bit field with a 0100 value, followed by the least significant 60 bits of the SHA-1 hash of the value or subjectPublicKey bit string (tag, not including the length and number of unused bit-string bits).	
Policy Properties								
keyUsage			4.2.1.3	True	MC			
	digitalSignature					S	False	

	nonRepudiation					S	False	
	keyEncipherment					S	False	
	dataEncipherment					S	False	
	keyAgreement					S	False	
	keyCertSign				M	S	True	
	cRLSign				M	S	True	
	encipherOnly					S	False	
	decipherOnly					S	False	

NR-CA Certificate Profile								
Attribute	**Field**	**IN**	**RFC 5280 Ref.**	**CE**	**O/M**	**CO**	**Value**	**Comment**
PrivateKeyUsagePeriod					O	F S	15 years	This shall be the usage period of the private key as per RFC 5280
certificatePolicies[5]			4.2.1.4	False	O			
	PolicyIdentifier				M	S	2.5.29.32.0 (anyPolicy)	According to rfc5280: " *PolicyInformation SHOULD only contain an OID.* *In a CA certificate, these policy information terms limit the set of policies for certification paths which include this certificate. When a CA does not wish to limit the set of policies for certification paths which include this certificate, it MAY assert the special policy anyPolicy, with a value of { 2 5 29 32 0 }"*
	policyQualifierID				O	S	Id-qt-1 (CPS)	
	qualifier					S	http:// [URL to be defined]	
	policyQualifierID					S	Id-qt-2 (User Notice)	
	noticeNumbers							
	DisplayText							

[5] [CAB EV Guidelines] indicates that Root CA Certificates SHOULD NOT contain the certificatePolicies extensions.

NR-CA Certificate Profile								
Attribute	**Field**	**IN**	**RFC 5280 Ref.**	**CE**	**O/M**	**CO**	**Value**	**Comment**
PolicyMappings			4.2.1.5		X			
	BasicConstraints		4.2.1.9	True	MC			This extension MUST be marked CRITICAL
	cA				M		True	TRUE for CA Certificates
	pathLenConstraint[6]				M		0	In all cases, including link certificates
NameConstraints			4.2.1.10		X			
PolicyConstraints			4.2.1.11		X			

[6] [CAB EV Guidelines] indicates that the pathLenConstraint field SHOULD NOT be present.

7.1.1 Certificate extensions

X.509 v3 extensions are supported and used as indicated in the Certificates profiles as described in section 7.1.1 of the present CPS.

7.1.2 Algorithm object identifiers

Algorithms OID are conforming to IETF RFC 3279 and RFC 5280.

7.1.3 Name forms

Name forms are in the X.500 distinguished name form as implemented in RFC 3739.

The following Subject Attributes are used:

- Country (country codes MUST follow the format of two letter country codes, specified ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions – 1997.)
- Organization.
- Organizational-unit.
- Common name.

7.1.4 Name constraints

Name constraints are supported as per RFC 5280.

7.1.5 Certificate policy object identifier

Certificate policy object identifiers are used as per RFC 3739 & RFC 5280.

7.1.6 Usage of Policy Constraints extension

Usage of Policy Constraints extension is supported as per RFC 5280.

7.1.7 Policy qualifiers syntax and semantics

The use of policy qualifiers defined in RFC 5280 is supported.

7.1.8 Processing semantics for the critical Certificate Policies

Not applicable.

7.2 CRL Profile

In conformance with the IETF PKIX RFC 5280, the NR-CA supports CRLs compliant with:

- Version numbers supported for CRLs
- CRL and CRL entry extensions populated and their criticality.

The profile of the CRL is provided in the table below:

Certificate List Component	Section in RFC 5280	Country Signing CA CRL	COMMENTS
CertificateList	5.1.1	m	
tBSCertList	5.1.1.1	m	see next part of the table
signatureAlgorithm	5.1.1.2	m	value inserted here dependent on algorithm selected
signatureValue	5.1.1.3	m	value inserted here dependent on algorithm selected
tBSCertList	5.1.2		
version	5.1.2.1	m	MUST be v2
signature	5.1.2.2	m	value inserted here dependent on algorithm selected / RSA with SHA-256 and PSS padding
issuer	5.1.2.3	m	The issuer field is defined as the X.501 type Name, and MUST follow the encoding rules for the issuer name field in the certificate
countryName		m	Value : QA Will be encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationalUnitName		o	CSPs-PMA
organizationName		o	Value: ictQATAR UTF8 encoded

commonName		o	Value : Qatar National Root CAs UTF8 encoded
thisUpdate	5.1.2.4	m	Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime

			<creation time>
nextUpdate	5.1.2.5	m	Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime <creation time + 184 days>
revokedCertificates	5.1.2.6	m	When there are no revoked certificates, the revoked certificates list MUST BE absent (as per RFC 5280)
userCertificate			<certificate serial number>
revocationDate			<revocation time>
extensions	5.1.2.7	m	
authorityKeyIdentifier	5.2.1	m	This MUST be the same value as the subjectKeyIdentifier field in the CRL Issuer's certificate. Non-critical <subject key identifier CA>
issuerAlternativeName	5.2.2	x	

cRLNumber	5.2.3	m	Non-critical <CA assigned unique number>inversion avec AKI
deltaCRLIndicator	5.2.4	x	
issuingDistributionPoint	5.2.5	x	
freshestCRL	5.2.6	x	
CRL Entry Extensions			
reasonCode	5.3.1	x	
holdInstructionCode	5.3.2	x	
invalidityDate	5.3.3	x	
certificateIssuer	5.3.4	x	

7.2.1 Version number(s)

See section 7.2.

The NR-CA will support X.509 version 2 CRLs.

7.2.2 CRL entry extensions

See section 7.2.

8 Compliance Audit and Other Assessments

The CSPs-PMA acting as CSP with regards to the NR-CA activities organizes compliance audits to ensure that it meets requirements, standards, procedures and service levels according to this CPS at least on an annual basis. The CSPs-PMA accepts this auditing of its own practices and procedures and will make the audit report publicly available no later than three months after the end of the audit period.

The CSPs-PMA PAA evaluates the results of such audits before further implementing them.

To carry out the audits there will be an independent auditor appointed who will not be affiliated directly or indirectly in any way with the CSPs-PMA, the NR-CA Operator nor any person having any conflicting interests thereof.

These audits will be performed by a Qualified Conformity Assessement body that fulfills the following requirements:

- Be an independent public accounting firm that has proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function and be licensed according to the laws and policies for assessors in the jurisdiction of the CA; and
- Be a member of the American Institute of Certified Public Accountants (AICPA), or a non-US equivalent that requires that audits be completed under defined standards that include the possession of certain skill sets, quality assurance measures such as peer review, competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education; and
- Maintain Professional Liability/Errors and Omissions insurance, with policy limits of at least one million US dollars in coverage.
- Accredited by the CAABA.

These audits will be performed by Qualified Auditors that fulfils the following requirements:

- Sufficient familiarity with the provisions of the Law and its Bylaw as well as all guidelines, controls, standards and instructions issued by Public Key Management and Digital Identity Section in relation to certification services.
- Holding a Certified Information Systems Auditor (CISA) certificate, Certified Information Technology Professional (CPA.CITP) certificate, Certified Internal Auditor (CIA) certificate or an accredited information security auditor certificate.
- Be able to conduct technical audit in compliance with ISO 27000 standards, particularly ISO (27001:2005) regarding information systems – security technologies – information systems management, as well as ISO (272002) regarding codes of practicing information security management.
- Must have sufficient experience in the fields of electronic signatures, electronic certification certificates, electronic programs, information security tools and technology, security and financial reviews rules and specialized audit technologies.

The audit addresses the following aspects:

- Compliance of the NR-CA operating procedures and principles with the procedures and service levels defined in the CPS.
- A full ETSI EN 319 411-1 V1.2.2 audit
- Ensure that all systems, processes, procedures, employees, apparatuses, equipment, products and services meet the approved controls, standards and requirements based on the ISO standards (27000)
- Management of the infrastructure that implements NR-CA services.
- Management of the physical site infrastructure.
- Adherence to the CPS.
- Adherence to relevant Qatar law and Bylaw.
- Asserting agreed service levels.
- Inspection of audit trails, logs, relevant documents etc.
- Cause of any failure to comply with the conditions above.

If irregularities are detected, the auditor will submit a report to the CSPs-PMA PAA, stating the measures that will be taken to rectify the situation and ensure compliance. If the proposed measures are deemed insufficient a second audit will be carried out to ensure compliance.

9 Other Business and Legal Matters

Certain Legal conditions apply to the issuance of certificates issued by the NR-CA under this CPS as described in this section.

9.1 Fees

An entity can only apply for a certificate issued by the NR-CA if in possession a valid license as per the Qatari CSPs Licensing Scheme established in the context of the E-Commerce Law and the asscociated Bylaw. Fees may be applicable to obtain such license.

9.2 Financial Responsibility

9.2.1 Insurance coverage

Each PKI Participant, except the Relying Parties, will maintain appropriate insurance to meet its obligations under this CPS and will maintain a sufficient amount of insurance coverage for its liabilities to other Participants, including Subscribers and Relying Parties.

9.2.2 Other assets

Not applicable.

9.2.3 Insurance or warranty coverage for end-entities

Not applicable.

9.3 Confidentiality of Business Information

Provisions relating to the treatment of confidential information that PKI Participants may communicate to each other, and in particular relating to the scope of what is considered as information within or not within the scope of confidential information, to the responsibility to protect confidential information, and to disclosure conditions are ruled by private agreements with the CSPs-PMA acting as CSP with regards to the NR-CA activities.

The CSPs-PMA acting as CSP with regards to the NR-CA activities guarantees the confidentiality of any data not published in the certificates issued by the NR-CA, according to the applicable laws on privacy.

9.4 Privacy of Personal Information

The CSPs-PMA acting as CSP with regards to the NR-CA activities observes personal data privacy rules and confidentiality rules as described in this CPS. Confidential information includes:

- Any personal identifiable information on citizens, other than that contained in a certificate.
- Exact reason for the revocation of a certificate.

- Audit trails.
- Logging information for reporting purposes, such as logs of requests by the RA.
- Correspondence regarding NR-CA services.
- NR-CA Private key(s).

The following items are not confidential information:

- Certificates and their content.
- Status of a certificate.

The CSPs-PMA does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the CSPs-PMA owes a duty to keep information confidential with regards to the NR-CA activities. It owes such a duty to the RA and promptly responds to any such requests.
- A court order.

Parties requesting and receiving confidential information are granted permission on the condition that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties.

Also these parties are bound to observe personal data privacy rules in accordance with the law.

The NR-CA will respect all applicable privacy, confidential information, and trade secret laws and regulations, as well as its published privacy policy, in the collection, use, retention, and disclosure of non-public information.

Disclosure Conditions

Non-confidential information can be disclosed to any subscriber and relying party under the conditions below:

- The status of a single certificate is provided per inquiry by a subscriber or relying party.
- A subscriber can consult non-confidential information the CSPs-PMA holds about it in the context of the NR-CA activities.

Confidential information will not be disclosed by the CSPs-PMA to subscribers nor relying parties with the exception of information about:

- Themselves.

- Persons in their custody.

Only the RA is permitted to access confidential information.

The CSPs-PMA acting as CSP with regards to the NR-CA activities properly manages the disclosure of information to the NR-CA personnel.

The CSPs-PMA authenticates itself to any party requesting the disclosure of information by:

- Presenting an authentication certificate at the request of the citizen or relying party
- Signing responses to OCSP requests and CRLs.

Next to the information retained by the CSPs-PMA, information pertaining to the subscribers' certificates can also be retained by the RA.

9.5 Intellectual Property Rights

The Public Key Management and Digital Identity Section owns and reserves all intellectual property rights associated with its own databases, web sites, the NR-CA digital certificates and any other publication whatsoever originating from the NR-CA including this CPS.

When the CSPs-PMA acting as CSP with regards to the NR-CA activities uses software from suppliers, it is possible that this software remains intellectual property of the supplier. This is defined in the license agreement of contract of this supplier.

9.6 Representations and Warranties

The CSPs-PMA acting as CSP with regards to the NR-CA activities uses this CPS to convey legal conditions of usage of certificates to subscribers and relying parties.

The NR-CA warrants to the Subject, Subscriber, Relying parties and all Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Certificate in software distributed by such Application Software Suppliers:

9.7 Disclaimers of Warranties

Within the limitations of the laws of the State of Qatar, the CSPs-PMA acting as CSP with regards to the NR-CA activities cannot be held liable (except in cause of fraud or deliberate abuse) for:

- Profit loss
- Loss of data
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificate or digital signatures

- Any liability incurred in any case if the error in such verified information is the result of fraud or willful misconduct of the applicant or if it is the result of negligence or with intent to deceive the CSPs-PMA, the NR-CA, or any person receiving or relying on the certificate.
- Any liability incurred as a result of the applicant breaking any laws applicable in the State of Qatar including those related to intellectual property protection, viruses, accessing computer systems etc.
- Other damage

9.8 Indemnities

Not applicable.

9.9 Term and termination

This CPS remains in force until notice of the opposite is communicated by the CSPs-PMA on its document repository.

Notified changes are appropriately marked by an indicated version. Changes are applicable [30] days after publication.

9.10 Individual notices and communications with participants

Notices related to this CPS can be addressed to CSPs-PMA contact address as stated in section 1.5.

9.12 Amendments

Minor changes to this CPS that do not materially affect the assurance level of this CPS are indicated by version number that contains a decimal number e.g. version 1.1 for a version with minor changes as opposed to e.g. version 2.0 that addresses major issues.

Minor changes to this CPS do not require a change in the CPS OID or the CPS pointer qualifier (URL) that might be communicated by the CSPs-PMA. Major changes that may materially change the acceptability of certificates for specific purposes, may require corresponding changes to the CPS OID or CPS pointer qualifier (URL).

9.13 Dispute Resolution Procedures

All disputes associated with this CPS will be handled in a first instance by the Grievance and Disputes Resolution Committee set out in Article No. (64) of the eCommerce Act.

The decision issued by the Grievances Committee in the settlement of disputes shall be final, and those concerned may challenge this decision before the Administrative Department at the Court of First Instance.

All disputes associated with this CPS will be in all cases resolved according to the laws of the State of Qatar.

9.14 Governing Law

The laws of Qatar shall govern the enforceability, construction, interpretation, and validity of the present CPS.

9.15 Compliance with applicable law

The present CPS and provision of NR-CA certification services are compliant to relevant and applicable laws of the State of Qatar.

9.16 Miscellaneous provisions

The CSPs-PMA acting as CSP with regards to the NR-CA activities incorporates by reference the following information in all digital certificates it issues:

- Terms and conditions in this CPS.
- Any other applicable certificate policy as may be stated on a certificate issued by the NR-CA.
- The mandatory elements of applicable standards.
- Any non-mandatory but customized elements of applicable standards.
- Content of extensions and enhanced naming not addressed elsewhere.
- Any other information that is indicated to be so in a field of a certificate.

To incorporate information by reference the CSPs-PMA acting as CSP with regards to the NR-CA activities uses computer-based and text-based pointers that include URLs, OIDs, etc.

9.17 Other Provisions

Not applicable.