وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

NR-CA Certificate Policy

Document Name:	NR-CA Certificate Policy
Document Reference:	CS-PI-CSP-PMA-POL-0002
Issue:	1.0
Issue Date:	15/05/2019
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
14/11/2018	0.1	First draft for review	PKI Team
20/11/2018	0.2	First internal review	PKI Team
29/03/2019	0.3	Second internal review	Public Key Management Section and Digital Identity Section
09/05/2019	0.4	Document Formatting	PKI Team
11/05/2019	0.5	External Review	Samir Pawaskar
15/05/2019	0.9	Document for approval	PKI Team
	1.0	Final Document	Fahad Saeed J S Abdulla

Contents

1 Scope

The present **CS-PI-CSP-PMA-POL-0002** is the "CSP-PMA National Root-CA (NR-CA) **Certificate Policy**". It is part of the CSP-PMA NR-CA documentation made of a series of documents closely linked to the present key management policy, the "**Certification Practices Statement** for the CSP-PMA National Root CA" (here after referred to as the NR-CA CPS) and its accompanying documents[1], and the **"key ceremony procedures".**

The present document describes the policies applicable to the handling of the NR-CA keys in a generic way, independent of the underlying technology. It details the NR-CA Keys requirements addressed on a high-level within the public NR-CA CPS and states "**what**" must be achieved in terms of security for the NR-CA Key(s). The present document is completed by the key ceremony procedures. The key ceremony procedures describes "**how"** to manage the NR-CA Key(s) with regards to the creation (generation), the usage of such key(s) for root-signing licensed CSPs, for creating cross-certificates and for issuing revocation lists, and with regard to deprecation of such keys.

The "key ceremony procedures" implements rationales required by the present Key Management Policy and instantiates the Key Policy in terms of the underlying technology (i.e. Entrust and Luna CA4). It is a confidential document. It is accompanied by a series of Key Ceremony Log sheets provided to all persons present during any key ceremony for the sake of recording any action on the NR-CA Key on one hand, and providing a clear step wise procedure to these persons.

1 The detailed list of documentation related to the NR-CA certification services can be found in the NR-CA CPS

2 Introduction

The NR-CA certification services and activities fall under the responsibility of the CSP-PMA acting as certification service provider and is further ruled by the CSP-PMA Policy Approval Authority (PAA). The PAA is responsible for the NR-CA activities, and in particular for the handling of its signing key and the related certificate. The PAA is the authority approving the present document and the authority entitled to modify it.

In order to provide a very high level of security to the NR-CA keys and also to allow a sound control on this CA, several persons are required for every key management related action, in such a way that in no way a single person can act on these keys (copy, erase, use, …).

For this purpose an M out of N scheme is set-up. The M out of N feature provides a means by which the NR-CA (employing cryptographic modules for sensitive operations), can enforce multi-person control over access to the cryptographic module. This will require at least M persons out of a series of N persons (called custodians) for any action on the key. One also leverages on the fact that the NR-CA is an off-line CA and restarting the NR-CA will necessarily always require the presence of M persons out of the N custodians.

The NR-CA is an off-line CA. It means that it is only instantiated at certain occasions (see the NR-CA CPS for more details), which are:

- The issuance of Certificate Revocation lists (CLRs), also called Authority Revocation Lists (ARLs) in the case of the NR-CA since certificates are issued to CSPs every 6 months in normal mode or as soon as a request for revoking a CSPs had been approved, in emergency mode, (see conditions in the NR-CA CPS)
- The re-key of the NR-CA, occurring every 15 years or exceptionally in case of a disaster requiring a new NR-CA Key
- In case of a disaster recovery (e.g. the site where the NR-CA is hosted underwent serious damage and is not up and running anymore, see the NR-CA CPS for more details)
- The issuance (and the subsequent re-key under conditions expressed in the NR-CA CPS and in CSP-PMA documentation specifying the Licensing Scheme) of certificates:
    - to root-sign a licensed CSP (once the CSP-PMA has taken the decision to endorse the CSP).
    - for creating cross-certificates with a foreign CSP (according to international agreements) .

The NR-CA keys are stored on a HSM. Among the operations performed on hardware devices are:

- Secure generation and secure storage of the NR-CA signing private key
- Signing of certificates and CRL's

3 Key management policy

3.1 Physical Security Controls

CSP-PMA acting as NR-CA CSP undertakes all its key management tasks within secure premises.

Physical protection is achieved through the creation of clearly defined security perimeters around and within the key management facilities.

Physical access to PKI key management facilities is protected by secure access control mechanisms, in accordance with CSP-PMA Physical Access Control Policy [CSP-PMA-POL-0006].

Access control mechanisms are permanently implemented within the secured premises at all times.

Access to NR-CA key management facilities is only granted to members of PKI staff in trusted roles and, optionally, to other members of staff or entitled auditors who have provided satisfactory credentials (i.e. have been vetted and provided with authorization by concerned persons).

Access control is also implemented through organizational security provisions describing and where and when needed, limiting: access hours, external visitors regulation, trusted role staff access conditions, security officer's tasks.

3.2 Environmental security controls

The rooms hosting the NR-CA are appropriately protected from environmental hazards, in accordance with the NR-CA CPS and CSP-PMA Physical and Environmental Security Policy.

Physical and Environmental security measures address among others, physical access control, fire safety factors, protection against break in (proper walls, ceiling, floors), external influences (flood, ground water, rain, wind, sun, earthquake, electromagnetic radiations, etc..), internal influences (energy pipes and lines (water, gas, heating, steam, sprinkler installation)).

3.3 Personnel Security controls

3.3.1 Personnel background

Personnel employed for NR-CA key management possesses the knowledge, experience and qualifications necessary for the PKI services that CSP-PMA acting as NR-CA CSP provides, in accordance with CSP-PMA Personnel Security Policy. This is valid for CSP-PMA personnel and for the personnel of other organizations to which NR-CA tasks have delegated or any contracting staff.

CSP-PMA personnel with NR-CA key management responsibilities acting in the context of NR-CA activities possesses expertise in the electronic signature technology.

CSP-PMA personnel with security responsibilities are familiar with security procedures.

The background of all personnel, including the personnel of other organizations to which NR-CA tasks have delegated or any contracting staff, is checked before they are contracted by CSP-PMA acting as NR-CA CSP, in accordance with its Personnel Security Policy.

CSP-PMA NR-CA staff authorized to carry out NR-CA key generation is strictly limited to those requiring to do so. They are allocated with a trusted role (see next section) by the CSP-PMA PAA.

- NR-CA key generation is undertaken by CSP-PMA NR-CA staff in trusted roles, under, at least, dual control.

- CSP-PMA NR-CA staff is required to provide satisfactory evidence of their trusted role; these persons must be nominated by the CSP-PMA PAA in official documents.

NR-CA key generation is overseen by:

- a member from the CSP-PMA acting as NR-CA CSP, in management role (the key manager). No delegation to any other organization is allowed for this witnessing role.

- An external Qualified Auditor as defined in the NR-CA CPS, to observe the process and the controls over the integrity and confidentiality of the Root CA Key Pairs produced.

3.3.2 Role and responsibilities

Security roles and responsibilities are documented in job descriptions, in accordance with "CSP-PMA acting as NR-CA CSP - Roles and Responsibilities security policy" document. Trusted roles are clearly identified in job descriptions.

Roles related to the NR-CA operations:

- PKI director
- Key manager
- The NR-CA operator is responsible for operating the actual hosting and certification operations including issuance, certificates status, and repository services. It have to be internal to CSP-PMA working under the supervision of the key manager.
- The NR-CA Security Officer administrates the CA and is responsible for installing, configuring and maintaining the CA trustworthy systems for registration, certificate generation and revocation management. His/her responsibilities include implementing and supervising security measures to protect data and conduct of personnel in relation to the protection of assets
- The NR-CA System Administrators are responsible for installing, configuring and maintaining the CA infrastructure (databases, directory, OS, etc). They are responsible for NR-CA operations and the system backup and recovery.
- The System Auditors are responsible for viewing and maintaining archives and audit logs of trustworthy systems

Roles related to the NR-CA key management:

The key generation is undertaken by selected persons in trusted roles, according to an M out of N scheme.

- The HSM Security Officer (SO) implements and supervises security operations related to the HSM protecting the NR-CA Keys.

- The HSM Key Partition Owner (PO) implements security operations related to the NR-CA Key within the HSM

- The Key Manager is responsible for implementing and monitoring the security procedures and practices as set forth in this document. This person is accountable for any actions handling the NR-CA key.

These 3 roles are exclusive, meaning that a different person must be in charge of each role. In addition, the Key Manager role cannot be delegated to an external to CSP-PMA organization. The Key Manager shall be a CSP-PMA staff in management role. The SO and PO are trusted operatives.

- Key custodians are N trusted persons selected to share the control on the NR-CA Keys. These persons must be distinct from the trusted operatives and the Key Manager.

- The NR-CA's Qualified Auditor. This is an auditor 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.
    - 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.
    - Maintain Professional Liability/Errors and Omissions insurance, with policy limits of at least 5 million Qatari Reals in coverage.
    - Accredited by the CABAA.
    - Sufficient familiarity with the provisions of the Law and its Bylaw as well as all policies, standards, guidelines, controls and instructions issued by MOTC 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.

After the generation of new NR-CA keys and certificate, the Qualified Auditor will issue a report opining that the CA, during its Root CA Key Pair and Certificate generation process:

- Documented its Root CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement.

- Included appropriate detail in its Root Key Generation Script.
- Maintained effective controls to provide reasonable assurance that the Root CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script.
- Performed, during the Root CA key generation process, all the procedures required by its Root Key Generation Script.

The Qualified Auditor will do this independently and not necessarily during the ceremony or in the NR-CA facilities.

3.4 Hardware Security Modules

NR-CA key generation is carried out using appropriate cryptographic devices that meet the requirements of FIPS PUB 140-2 level 3 or higher. Hardware and software mechanisms prevent NR-CA private keys from leaving key generation devices unencrypted.

It is supposed that the HSM is new when used for the first time by the NR-CA. Unwrapping should occur in the presence of the persons with a role related to the NR-CA key management and the external qualified auditor, as first step of initialization.

Prior to any **initial** key generation, the hardware security module must be initialized. The initialization process consists in setting up the necessary identities, authentication and ownership that are to be associated with the HSM. This process involves the configuration of physical and/or logical tokens. Between uses, access keys are stored in safe(s) within the NR-CA premises. Keys of safes protecting access keys are left in the custody of different CSP-PMA NR-CA staff in trusted roles. The HSM must be initialized in the presence of the HSM trusted operatives, the Key Manager and the Key custodians.

During the first initialization process, the necessary backup tokens required for the CA keys back-up will also be generated.

3.5 Records

For all events related to the NR-CA operations records will be kept that include all information related to that event that can be useful for auditing purposes. This will include a video of the whole event. Records can be electronic, in which case all records (including video) should have time information within the record and protected by an adequate integrity control system.

Records will then be stored on the NR-CA secure storage. The NR-CA secure storage will ensure their integrity and confidentiality and protect them against tampering.

All electronic records will be stored in a that will be likely to be supported by software in the long future (for text files PDF-A or raw utf8 encoded text, for video for instance MP4 or raw).

It is the responsibility of the NR-CA Operator to make sure that the records will continue to be available and readable during their whole archival period.

3.6 NR-CA Key Generation

The CSP-PMA NR-CA Key Generation Ceremony will be witnessed by the CA's Qualified Auditor and by the Key Manager.

The other persons present are:

- The trusted operatives
- N Key Custodians
- The NR-CA Security Officer.

NR-CA key generation is performed using recognized algorithms providing appropriate guarantees on the randomness and security of generated keys.

In accordance with FIPS PUB 140-2, the HSM generates public key parameters using FIPS approved generation algorithms, guaranteeing their randomness and quality.

NR-CA key length, lifetime and cryptographic algorithm are recognized as being fit for the purposes of the NR-CA keys. This will be in accordance with the NR-CA CPS.

A record is kept of each NR-CA key generation, which logs:

- the key generation context (date, NR-CA key purpose);
- the name and function (trusted role) of all attendees and the credentials they have provided;

- the custody of access keys and safes keys;
- the key algorithm and length;
- technical key generation information (share data, brand, model and serial number of the key generation device, primary storage media).

All attendees sign the key generation record at the end of the NR-CA key generation.

All NR-CA key generation records are kept in a safe for later retrieval, together with key backups.

3.7 NR-CA Certificate Generation

3.7.1 Personnel

Staff authorized to carry out public NR-CA key certification is strictly limited to those requiring to do so.

NR-CA public key certification is undertaken by CSP-PMA NR-CA staff in trusted roles (the trusted operative). CSP-PMA NR-CA staff in trusted roles is required to provide satisfactory evidence of their management role; these persons must be nominated by the CSP-PMA PAA in official documents.

NR-CA public key certification is overseen by CSP-PMA staff in management role(s), i.e. the Key Manager.

The other persons present are:

- M Key Custodians
- The NR-CA Security Officer.

3.7.2 Certificate profile

The CSP-PMA acting as NR-CA CSP and public key holders agree specifications of certificate formats, profiles and contents before any certification task is undertaken, as specified in the NR-CA CPS.

- Key usage is constrained as specified in the NR-CA CPS. .
- The CSP-PMA acting as NR-CA CSP only issues NR-CA certificates whose profiles comply with recognized standards, as specified in the NR-CA CPS.
- The CSP-PMA acting as NR-CA CSP issues NR-CA certificates whose format complies with X.509 Version 3.

3.7.3 Public key certification

NR-CA certificates are signed using hardware signing modules that meet the requirements of FIPS PUB 140-2 level 3 or higher.

The NR-CA certificate is self-signed. Self-signed certificates are generated by releasing and activating the private key linked to the public key to be signed and by using it as signing key for the signing algorithm to sign the certificate containing the public key.

3.7.4 Records

A record is kept of each NR-CA public key certification, which logs:

- the certification context (date, NR-CA key purpose);
- the name and function (trusted role) of all attendees and the credentials they have provided;
- the NR-CA certificate;
- technical certification information (shares used, brand, model and serial number of the HSM).

All attendees sign the certification record at the end of the NR-CA public key certification.

All paper based NR-CA public key certification records are kept in the safe for later retrieval, together with the NRCA key HSM and the related access tokens .

All electronic based NR-CA public key certification records should include precise time information and securely saved (with integrity tapering detection).

3.8 NR-CA key storage, backup and recovery

3.8.1 Personnel

NR-CA key backup, storage and recovery tasks are undertaken by CSP-PMA NR-CA staff in trusted roles (the trusted operative). CSP-PMA NR-CA staff in trusted roles is required to provide satisfactory evidence of their trusted role.

NR-CA public key certification is overseen by CSP-PMA staff in management role(s), i.e. the Key Manager.

The other persons present are the M Key Custodians.

3.8.2 Key backup

NR-CA keys are backed up by CSP-PMA NR-CA staff in trusted roles, under the supervision of CSP-PMA staff, in management role, with the same controls in place as during the key generation controls above specified.

NR-CA keys are backed up on tamper-resistant storage media. This can be a clone of the primary HSM.

NR-CA key backups (or cloned HSM) are kept in a safe for later retrieval, different from the safe where the primary HSM is stored, together with key generation and certification records.

The safes custody is left to M out of the N key custodians.

The integrity of NR-CA key backups is controlled immediately after keys are backed up.

The integrity of NR-CA key backups is verified on an annual basis by CSP-PMA NR-CA staff in trusted roles.

3.8.3 Key recovery

CSP-PMA NR-CA staff verifies the integrity of NR-CA keys stored on tamper-resistant storage media before recovering NR-CA keys.

NR-CA keys are recovered by CSP-PMA NR-CA staff in trusted roles, under the supervision of CSPsPMA staff, in management roles with the same controls in place as the key generation controls specified above.

3.8.4 Records

A record is kept of each NR-CA key backup, which stores:

- the backup context (date);
- the name of all attendees;
- technical backup information (HSM access key used, which token is in the hand of which custodians, where the related password are stored etc).

All attendees sign the backup record at the end of the NR-CA key backup.

All NR-CA key backup records are kept in a safe for later retrieval, together with key backups.

A record is kept of each NR-CA key recovery, which logs:

- the recovery context (date);
- the name of all attendees;
- technical recovery information (HSM access key used, which token is in the hand of which custodians, where the related password are stored etc).

All attendees sign the recovery record at the end of the NR-CA key backup.

All NR-CA key recovery records are kept in a safe for later retrieval, together with key backups.

3.9 NR-CA key update and changeover

In due time, in normal circumstances, the CSP-PMA acting as NR-CA CSP generates new private and public keys and corresponding certificate to replace previous key pair within a two (2) months period 15 years after it has been generated (see the NR-CA CPS), allowing the previous key pair to stop signing activities sufficiently in advance so that any subordinate operational certificate is issued with a required expiry date no later than that of the issuing NR-CA certificate.

3.10 Key activation and deactivation

Key are activated at the beginning of each ceremony and deactivated at the end of the ceremony.

3.10.1 Key activation

Activation of NR-CA private keys by key generation devices is protected by means of M out of N based security mechanisms. The presence of M key custodians, with the access key they have been allocated, is thus required to activate the NR-CA private key.

3.10.2 Key deactivation

NR-CA keys are deactivated and removed from volatile memory by shutting the HSM power off.

3.11 End of NR-CA key life cycle

3.11.1 Key archival

At the end of their lifetime, NR-CA private keys are destroyed.

At the end of their lifetime, NR-CA certificates are archived in plain-text form, on read-only, tamper resistant storage media.

Archived NR-CA certificates are kept in a safe for later retrieval.

3.11.2 Key destruction

NR-CA private keys are destroyed by deletion of the key in both the primary and the cloned HSM.

NR-CA keys are deleted by CSP-PMA NR-CA staff in trusted roles, with the same controls in place as the key generation controls specified above.

3.11.3 NR-CA certificate revocation

In case of compromise of a NR-CA private key, the certificate associated to the NR-CA key is revoked.

After revoking a NR-CA certificate, if needed, all certificates subordinate to the associated NR-CA private key are revoked.

After revoking a NR-CA certificate, a new NR-CA key pair is created and the associated certificate is generated.

3.11.4 Records

A record is kept of each NR-CA key destruction, which logs:

- the destruction context (date, reason for destruction).
- the name of all attendees.
- technical destruction information (certificate associated to the destroyed key).

All attendees sign the destruction record at the end of the NR-CA key destruction.

All NR-CA key destruction records are kept in a safe for later retrieval.

A record is kept of each NR-CA certificate revocation, which logs:

- the revocation context (date, reason for revocation).
- the name of all attendees.
- technical revocation information (CRL URL).

All attendees sign the revocation record at the end of the NR-CA key destruction.

All NR-CA key revocation records are kept in a safe for later retrieval.

3.12 Life cycle management of cryptographic hardware used to sign certificates

3.12.1 General

Compliance with Level 3 of FIPS PUB 140-2 guarantees that hardware security modules are enclosed in a hard, opaque potting material to prevent any physical tampering.

3.12.2 Shipment

Hardware security modules are securely shipped by their manufacturers to CSP-PMA using tamper evident packaging procedures.

3.12.3 Storage

Hardware security modules are kept in secure storage within the CSP-PMA NR-CA premises whilst not in use.

3.12.4 Use

Hardware Security Modules holding valid NR-CA signing keys are operated by CSP-PMA NR-CA staff in trusted roles.

3.12.5 Test Service and repair

Compliance with Level 3 of FIPS PUB 140-2 ensures that Hardware Security Modules are self-tested when powered up or in specific circumstances, which guarantees that they are functioning properly.

Upon receipt of hardware security modules from manufacturers, CSP-PMA NR-CA staff in trusted roles performs acceptance testing and verification of firmware settings.

The process whereby hardware security modules are serviced with new hardware, firmware or software is performed by NR-CA System Administrators under at least dual control.

Hardware security modules are securely shipped to their manufacturers for repair, using tamper evident packaging procedures. Prior the HSM is zeroed in order to avoid manufacturer to have access to the private key.

Upon receipt of hardware security modules that have been repaired, NR-CA System Administrators perform acceptance testing and verification of firmware settings and restore the keys from the clone with the key trusted operatives and the M key custodians.

3.12.6 Records

A record with the date of occurrence and the list of persons in charge of the handling, is kept of each hardware security module life cycle management related event:

- device receipt.
- entering or removing a device from storage.
- device usage.
- designation of a device for service and repair.
- device retirement.

All attendees sign records of hardware security module life cycle management related event after it has occurred.

All hardware security module life cycle management records are kept in a safe for later retrieval.