CROSS CERTIFICATION POLICY

Document Classification:

Controlled

Version Number: 2.2

Issue Date: March 22, 2020

Table of Contents

1. POLICY STRUCTURE AND DEFINITIONS

1.1 POLICY STRUCTURE

This policy document contains the following elements:

- **Purpose**: This section clearly states the purpose of the policy with regards to cross certification with other Certification Authorities external to NCDC.
- **Scope:** This section defines various internal and external entities as well as the people to which a particular policy statement applies.
- **Policy Statements:** This section describes the Cross Certification Policy of NCDC.
- **Related Policies:** This section mentions other Policies, which the user can refer to along with this policy document.
- **Compliance:** This section contains a statement that NCDC policies will be complied with and that violations may result in disciplinary action.
- **Waiver Criteria:** This section provides a formal process for obtaining approval for a waiver to a policy. Waivers should only be used in exceptional situations when communicating non-compliance with the policy for a specific period of time.
- **Executor(s):** The person responsible for implementation of a policy.

1.2 DEFINITIONS

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

2. PURPOSE

The purpose of this document is to outline the criteria for cross-certification of an external Certification Authority with NCDC.

3. SCOPE

This Policy is applicable whenever an entity applies to cross certify with the Saudi National PKI managed by NCDC. This document is intended for NCDC managers, personnel involved in cross certification within NCDC and those parties desiring to cross-certify with the Saudi National PKI.

4. POLICY STATEMENT

4.1 GENERAL RESPONSIBILITIES

To be able to utilize and depend upon the certificates and services of NCDC an entity needs to have its CA formally recognized by the Saudi National PKI through its National Center for Digital Certification (NCDC).

NCDC will consider application for cross-certification from any organization or government operating a Certification Authority outside the Kingdom of Saudi Arabia.

Applications will be considered if they come from entities residing outside the Kingdom of Saudi Arabia, in particular:

- A commercial organization,
- A non-commercial organization,
- A government entity.

Cross certification with the Saudi National PKI will take place at the Saudi National Root-CA level.

4.2 PRE-REQUISITES

In order to proceed, an applicant should provide the following:

- Reasons for cross certification request (i.e., business, legal, convenience, etc.),
- CP and CPS,
- Security Policy and if required practices,
- Current third party Audit report,
- Certificate profiles,
- Information regarding the legal status and financial capacity of the applicant,
- The applicant will be asked to sign a Non-Disclosure Agreement, undertaking not to disclose any security-related information that NCDC may reveal in the course of facilitating cross certification.

4.3 REPRESENTATIONS

All applicants, unless otherwise exempted, must provide representations and evidence of:

- The legal status of the entity responsible for the PKI; demonstrating that the organization is in good standing under the laws of the jurisdiction in which it was created, and
- The financial capacity of organisation to manage risks associated with the operation of a PKI.

Applicants exempted from these evidentiary requirements are government entities and those exempted at the NCDC sole discretion.

4.4 POLICY MAPPING

The applicant CP will be mapped by category and element to the Saudi National Root-CA CP to evaluate the extent to which the applicant PKI demonstrates policies, practices and procedures consistent with those of the Saudi National Root-CA and NCDC. Depending on the requirements, additional policies and practices may need to be reviewed especially in the areas of identity proofing and certificate issuance.

4.5 TECHNICAL INTEROPERABILITY

Technical interoperability testing is used to ensure technical interoperability between the Saudi National Root-CA and the applicant's CA. At a minimum, the technical interoperability test will demonstrate:

- The directories of the Saudi National Root-CA and the applicant are interoperable;
- Network connectivity is achieved using all required protocols;
- The cross-certificate is correctly constructed by the Saudi National Root-CA, exchanged with, and recognized by the applicant Certification Authority;
- The cross-certificate is correctly constructed by the applicant Certification Authority, exchanged with, and recognized by the Saudi National Root-CA;
- A test transaction, using a test subscriber of the applicant PKI, can be successfully validated; and
- The ability to share revocation information between the Saudi National PKI and the applicant PKI.

4.6 OVERALL EVALUATION

The overall evaluation of the applicant's PKI compliance involves an assessment of the information collected in the technical interoperability testing and the results of the policy mapping. If these results reveal that applicant PKI meets the requirements of Saudi National PKI assurance level, NCDC may start negotiations for the purpose of entering into a Cross Certification Agreement.

Upon execution of NCDC Cross Certification Agreement, the Saudi National Root-CA and the applicant CA will generate, sign and exchange certificates.

4.7 RENEWING, TERMINATING AND REVOKING THE CROSS CERTIFICATE

At any time, either party may ask to renew or renegotiate the agreement.

At any time, either the applicant or NCDC can initiate the process to terminate the cross certification agreement. Once a mutually agreeable termination date is agreed on, the two parties carry out the termination procedures. NCDC has the right to terminate the agreement and revoke the cross certificate in any of the following cases:

- Any of the information in the Cross Certificate has changed;
- The applicant has failed to meet its obligations under the Saudi National Root-CA CP or any other applicable Agreements, regulations, or laws;
- Cross Certificate private key is compromised or suspected to be compromised;
- NCDC suspects or determines that revocation of the Cross Certificate is in the best interest of the integrity of the Saudi National PKI; and
- The CA determines that the Cross Certificate was not issued correctly in accordance with the Saudi National Root-CA CP.

5. RELATED NCDC POLICIES AND PROCEDURES

- Saudi National Root-CA CP
- Saudi National Root-CA CPS

6. COMPLIANCE

Compliance with this policy is mandatory and will be reviewed periodically by Trust Services Governance General Department. Violations of NCDC policies, standards, and procedures will result in corrective action by NCDC management. Disciplinary action will be consistent with the severity of the incident, as determined by an investigation, and may include, but not be limited to:

- Loss of access privileges to information assets.
- Other actions as deemed appropriate by NCDC management, Business Support department, and Trust Services Governance General Department.

7. WAIVER CRITERIA

Requested waivers must be formally submitted to NCDC, including justification and benefits attributed to the waiver, and must be approved by NCDC Chief Executive Officer. The waiver should only be used in exceptional situations when communicating non-compliance with the policy for a specific period of time (subject to a maximum period of 1 year). At the completion of the time period the need for the waiver should be reassessed and re-approved, if necessary. No policy should be provided waiver for more than three consecutive terms. The waiver should be monitored to ensure its concurrence with the specified period of time and exception. All exceptions to this policy must be communicated through the Policy Waiver Request Form.

8. EXECUTOR(S)

The implementation of this policy is the responsibility of NCDC Trust Services Governance General Department, teams formed for the technical, policy and legal evaluation of cross certification.