

National Center for Digital Certification

Root CA PKI DISCLOSURE STATEMENT

March 06, 2009

Version 1.22

Document Classification:

Public

Document Reference

Item	Description
Document Title:	NCDC Root CA PKI Disclosure Statement
Department:	NCDC Policy, Rules & Regulations Department
Version No.:	1.22
Status:	Final
File Name:	NCDC Root CA PKI Disclosure Statement v1.22
Type:	MS Word Document

Author(s)	Dr. Deoraj B. M.
	NCDC Policy, Rules & Regulations Department
	Signature/Date

Reviewed by	Mohammed E. AlGhamdi
	NPA
	Signature/Date

Approved by	Dr. Fahad A. AlHoymany
	NPA Chairperson/ NCDC Director
	Signature/Date

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	25/11/2008	Dr Deoraj	First Draft
1.1	28/12/2008	Dr Deoraj	Incorporated comments from Mohammed
1.2	12/01/2009	Dr Deoraj	Links Updated
1.21	17/01/2009	Dr Deoraj	Copyright statement changed
1.22	06/03/2009	Dr Deoraj	Fax no and other review comments with Mohammed

Document Control

This document shall be reviewed annually and an update by the NPA may occur earlier if internal or external influences affect its validity.

Copies of this document will be held by:

1. NPA
2. NCDC Policy, Rules & Regulations Department
3. Operations Department

Table of Contents

1.	NCDC-Root-CA PKI Disclosure Statement	5
1.1	NOTICE	5
1.2	CONTACT INFORMATION	5
1.3	CERTIFICATE TYPE, VALIDATION PROCEDURES AND USAGES	6
1.4	RELIANCE LIMITS	6
1.5	OBLIGATIONS	6
1.6	CERTIFICATE STATUS CHECKING OBLIGATIONS OF RELYING PARTIES	7
1.7	LIMITED WARRANTY & DISCLAIMER/LIMITATION OF LIABILITY	7
1.8	APPLICABLE AGREEMENTS, CP, CPS.....	8
1.9	PRIVACY POLICY	8
1.10	REFUND POLICY	9
1.11	APPLICABLE LAW AND DISPUTE RESOLUTION	9
1.12	CA AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT	9
1.13	APPROVED REGISTRATION AUTHORITIES	9
1.14	APPROVED REPOSITORIES	10
1.15	ELIGIBLE SUBSCRIBERS.....	10
1.16	CERTIFICATE STATUS INFORMATION	10
1.17	IDENTIFICATION OF THIS CERTIFICATE POLICY:.....	10

1. NCDC-Root-CA PKI Disclosure Statement

1.1 Notice

This PKI Disclosure Statement does not substitute or replace the National Center for Digital Certification's Root CA Certificate Policy (NCDC-Root-CA-CP) under which NCDC Root Certification Authority (NCDC-Root-CA) digital certificates are issued. You must read the NCDC-Root-CA-CP published at <http://web.ncdc.gov.sa/> before you apply for or reply on a certificate issued by the NCDC-Root-CA.

The full NCDC-Root-CA Certificate Policy is defined by two documents:

- This document, the 'NCDC-Root-CA PKI Disclosure Statement', and
- The ' National Center for Digital Certification's Root CA Certificate Policy (NCDC-Root-CA-CP).

Certificates issued by NCDC-Root-CA directly reference this document and consequently the NCDC-Root-CA-CP.

The purpose of this document is to summarize and present the key points of the NCDC-Root-CA's Certificate Policy in a more readable and understandable format for the benefit of Subscribers and Relying Parties

The NCDC-Root-CA operates as a closed business system model in the sense that access and participation is only open to those who are approved by the NPA. It utilizes Digital Certificates issued by Certification Authorities (CAs) meeting rules established by the NCDC's governing body the National Policy Authority (NPA). The NCDC owns and operates the Root Certification Authority which serves as the head or root of the trust (Anchor of trust) infrastructure of the Kingdom of Saudi Arabia. The NCDC-Root-CA provides digital certification services to only those subordinate Certification Authorities that are approved by NPA. These approved CAs in turn, provide security and trust services to defined communities by issuing of NCDC Digital Certificates to Subscribers, Relying parties, Registration Authorities, and CSPs. Together all of these components and participants form the "Saudi National PKI."

The NCDC-Root-CA certifies its subordinate Issuing Authorities by digitally signing their CA certificates. The NCDC-Root-CA self-signs its own Certificate using carefully designed, monitored and audited procedures thus act as a root in Saudi PKI.

For purposes of this NCDC-Root-CA PKI Disclosure Statement, all terms used shall have the meanings set forth in the NCDC System Documentation Glossary which can be found at <http://www.ncdc.gov.sa/Glossary>.

1.2 Contact information

Any questions about this PKI Disclosure Statement should be directed at the address below. This department is also responsible for the NCDC-Root-CA-CP and associated CPS.

Mailing Address:

E-mail: PKI@ncdc.gov.sa

Tel: +966 1 452 2197 / +966 1 452 2349

Fax: +966 (1) 4522043

1.3 Certificate type, validation procedures and usages

The NCDC-Root-CA issues certificates and Certificate Revocation Lists (CRLs) only to the Licensed CSP CAs, certificates required by the supportive PKI components and functions for the Root-CA operations within Saudi PKI.

The signing keys of NCDC-Root-CA and its subordinated issuing CSPs CAs are the only keys permitted for signing certificates and CRLs for their individually defined user communities.

The Root-CA Certificate has been self-generated and self-signed. When the Root-CA receives a request for a CSP CA Certificate or an entity wishing to cross certify with the Saudi PKI, the Root CA does not issue a Certificate before the applicant accepts the terms of a Agreement, accepts to adapt to the Saudi National PKI Policy, successfully completes the CSP or Cross Certifying Entity registration formalities, obtains the required license from the CITC (for commercial CSPs), and gets final approval from the NPA.

1.4 Reliance limits

None specified. NCDC-Root-CA does not set reliance limits for Certificates issued under this policy. Reliance limit may be set by other policies, application controls and Saudi applicable law or by Relying Party Agreement. See Limitation of Liability, below.

1.5 Obligations

It is the responsibility of the NPA to:

- Review the issued Certificate to confirm the accuracy of the information contained within it before installation and first use
- For the Root CA and the CSP CA's, the Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the CA keys and take reasonable precautions to prevent any loss, disclosure, or unauthorised use of the private key
- CA private key is generated using multi-person control "m-of-n" split key knowledge scheme.
- Backing up of the CA signing Private Key is under the same multi-person control as the original Signing Key.
- Keep confidential, any passwords, PINs or other personal secrets used in obtaining authenticated access to PKI facilities and maintain proper control procedures for all such personal secrets

- It is the responsibility of the Subscriber to: obtain a certificate make only true and accurate representation of the required information to the Registration Authority
- use the Certificate for legal purposes and restricted to those authorized purposes detailed by the NCDC-Root-CA Certificate Policy
- notify the Registration Authority immediately of a suspected or known key compromise in accordance with the procedures laid down in the NCDC-Root-CA Certificate Policy

For the device or Function certificate the authorized representative represented during the registration process must accept these responsibilities.

WARNING: The CA's private key is the primary means by which its subscribers are certified. This must be protected as its most valuable asset. If this private key is compromised, unauthorised persons could sign fraudulently produced certificates with the key and commit the Issuing Authority to unauthorised obligations and liabilities.

1.6 Certificate status checking obligations of relying parties

If a Relying Party is to reasonably rely upon a Certificate it shall be:

- Ensuring that reliance on Certificates issued under this Policy is restricted to appropriate uses (see "Certificate Type, validation procedures and usage", above for a summary of approved usages).
- Verifying the Validity by ensuring that the Certificate has not Expired
- Ensuring that the Certificate has not been suspended or revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon
- Determining that such Certificate provides adequate assurances for its intended use

1.7 Limited warranty & disclaimer/Limitation of liability

The NCDC-Root-CA warrants and promises to:

- Provide certification and repository services consistent with the CP, CPS and other operational policies and procedures.
- Perform authentication and identification procedures in accordance with CSP agreement and Operation policies and procedures.
- Provide certificate and key management services including certificate issuance, publication, revocation and re-key in accordance with the NCDC-Root-CA- CP and CPS.
- The NCDC-Root-CA makes no direct warranties or promises to Subscribers or Relying Parties.

The NCDC-Root-CA does not liable for any loss of the Saudi PKI service:

- Due to war, natural disasters, etc;

- Due to unauthorized use of certificates or using it beyond the prescribed use defined by the NCDC-Root-CA-CP and CPS for the certificates issued by the NCDC-Root-CA;

Limitations on Liability

- The NCDC-Root-CA will not incur any liability to Subscribers or any person to the extent that such liability results from their negligence, fraud or willful misconduct.
- The NCDC-Root-CA assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under Certificate Policy for any use other than in accordance with Certificate Policy. Subscribers will immediately indemnify the NCDC-Root-CA from and against any such liability and costs and claims arising there from.
- The NCDC-Root-CA will not be liable to any party whosoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services.
- End-Users, RAs, CSPs are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been verified by CSPs or NCDC-Root-CA.
- Subscribers to compensate a Relying Party which incurs a loss as a result of the Subscriber's breach of Subscriber agreement.
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations described in the Relying Party agreement.
- Registration Authorities shall bear the consequences of their failure to perform the Registration Authorities obligations described in the Registration Authorities agreement.
- NCDC-Root-CA denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

1.8 Applicable Agreements, CP, CPS

Subscriber Agreement can be found at: <http://www.ncdc.gov.sa/>,

Relying Party Agreement can be found at: <http://www.ncdc.gov.sa/>,

This document (NCDC Root CA PKI Disclosure Statement) can be found at: <http://www.ncdc.gov.sa/>,

The NCDC-Root-CA-CP can be found at: <http://www.ncdc.gov.sa/>,

The CSP Agreement and NCDC-Root-CA-CPS shall only be available subject to approval of a formal application in writing to the NPA.

1.9 Privacy policy

The NCDC-Root-CA respects need to appropriately control individual's personal information and to know how such information may be used. The NCDC-Root-CA take reasonable care to ensure that the information submitted during the certificate application, authentication of identity, and certification processes will be kept private. The NCDC-Root-CA will use that

information only for the purpose of providing PKI services. The private information will not be sold, rented, leased, or disclosed in any manner to any person or third party without entity prior consent, unless otherwise required by law, or except as may be necessary for the performance of the NCDC services, for auditing requirements, or as part of the regulatory compliance. For details please see NCDC Privacy Policy at: <http://www.ncdc.gov.sa/>.

1.10 Refund Policy

Not applicable for this Policy.

Currently, no fees are charged by NCDC-Root-CA for Digital Certificates, although NCDC-Root-CA reserves the right to change this in the future. For Digital Certificates for which no charge is made, no refunds are possible.

1.11 Applicable law and dispute resolution

Applicable laws are the laws and regulations of the Kingdom of Saudi Arabia. NCDC will act in accordance with current legislation in the Kingdom of Saudi Arabia, in particular the Telecom law and the Electronic Transactions Act.

Applicable laws and dispute resolution provisions are in accordance with applicable NCDC-Root-CA policies and Agreements. The NCDC Dispute Resolution Policy can be found at: <http://www.ncdc.gov.sa/>.

1.12 CA and Repository Licenses, Trust Marks, and Audit

The NPA grants to the CSP a non-exclusive license solely for their operations under the approved CA.

The CSP CA if it is going to offer a commercial for-profit certification authority, prior to commencing operations, and after having received approval of its application from the National Policy Authority, it is required to obtain a license from the Communications and Information Technology Commission before operating as a CSP CA within the Saudi National PKI.

The CAs shall be subjected to periodic compliance audits to maintain security and trust accreditation. These are no less frequent than once in twelve months and after each significant change to the deployed procedures and techniques. Moreover, the NPA may require ad-hoc compliance audits of NCDC-Root-CA and any CSP CA operation to validate that it is operating in accordance with the respective CP, CPS, and other supporting operational policies and procedures.

1.13 Approved Registration Authorities

The following Registration Authorities has been designated by the NCDC-Root-CA to register subscribers under this policy:

- NCDC-Root-CA-RA

1.14 Approved Repositories

The NCDC Public LDAP directory <http://www.ldap.ncdc.gov.sa> and the NCDC website <http://web.ncdc.gov.sa/CRL/nrcapart<n>.crl>, <http://web.ncdc.gov.sa/CRL/nrcacomb<n>.crl> are the only authoritative sources for:

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

1.15 Eligible Subscribers

The following types of subscribers are eligible to be issued with certificates by NCDC-Root-CA under this policy:

- Subordinate CSPs CAs(level 1), subject to approval by the NPA
- cross certifying with CAs at the international level
- Certificates required by the supportive PKI components and functions for the Root CA operations within Saudi PKI

1.16 Certificate Status Information

The NCDC-Root-CA will publish its CRL no less frequently than once every fourteen months and at the time of any Certificate revocation of its CSP CAs or cross certified CAs.

1.17 Identification of this Certificate Policy:

This document has been registered with NCDC-Root-CA and has been assigned an object identifier as below:

Saudi-National-Root-CA (NCDC-Root-CA) PDS Document: 2.16.682.1.101.5000.1.2.1.3