SAUDI NATIONAL ROOT-CA

PKI DISCLOSURE STATEMENT

Document Classification:

Public

Version Number: 2.4

Issue Date: May 22, 2023

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
1.3	15/06/2010	Dr Deoraj	NPA is replaced with NCDC , Glossary link, NCDC Copyright statement, Policies & Regulations Department and other agreed changes made
1.4	07/01/2012	Dr Deoraj , Naif	Updated as per WebTrust recommendations and reformat the document with other minor changes
1.5	26/3/2011	Dr. Deoraj and Naif	Changes related to SHA 256 and CAB requirements.
1.6	28/05/2015	Dr Deoraj and Naif	Annual review
1.7	16/05/2016	Dr. Deoraj and Naif	Annual review
1.8	23/05/2017	Dr. Deoraj and Naif	Annual review
1.9	23/05/2018	Dr. Deoraj and Khalid Bin Kulaib	Annual review
2.0	04/07/2019	Dr. Deoraj and Meshal M. Al-shahrani	Annual review, removed fax
2.1	15/04/2020	Dr. Deoraj and Abdullah Aldhuwayhi	Annual review
2.2	20/06/2021	Abdullah Aldhuwayhi	Annual review
2.3	15/06/2022	Dr. Deoraj	Annual review
2.4	22/05/2023	Ammar Alsofyani	Update the PDS with NIC policies

Table of Contents

1. Notice

This PKI Disclosure Statement does not substitute or replace the Saudi National Root-CA Certificate Policy (Saudi National Root-CA CP) under which Saudi National Root Certification Authority (Saudi National Root-CA) digital certificates are issued. You must read the Saudi National Root-CA CP published at (https://ca.nic.gov.sa) before you apply for or reply on a certificate issued by the Saudi National Root-CA.

The full Saudi National Root-CA CP is defined by two documents:

- This document, the Saudi National Root-CA PKI Disclosure Statement (Saudi National Root-CA PDS); and
- The Saudi National Root-CA CP.

The purpose of this document is to summarize and present the key points of the Saudi National Root-CA CP in a more readable and understandable format for the benefit of Subscribers and Relying Parties.

The Saudi National 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 National Information Center (NIC). NIC owns and operates the Saudi National Root-CA which serves as the head or root of the trust (Anchor of trust) of PKI infrastructure for the Kingdom of Saudi Arabia. The Saudi National Root-CA provides digital certification services to only those subordinate Certification Authorities that are approved by NIC. These approved CAs in turn, provide security and trust services to defined communities by issuing of Digital Certificates to Subscribers, Relying parties, Registration Authorities, and DTSPs. The Digital Government Authority (DGA) is the regulator of Digital Trust Services in the Kingdom of Saudi Arabia. Together all of these components and participants form the “Saudi National PKI”.

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

For purposes of this Saudi National Root-CA PDS, all terms used shall have the meanings set forth in NIC PKI Glossary which can be found at (https://ca.nic.gov.sa).

2. Contact Information

Queries regarding this PKI Disclosure Statement shall be directed at:

Email: pki@nic.gov.sa

Telephone: +966 11 8081013

3. Certificate Type, Validation Procedures and Usages

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

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

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

4. RELIANCE LIMITS

The Saudi National 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. For additional information, refer to “Limited Warranty and Disclaimer/Limitation of Liability” section.

5. OBLIGATIONS

It is the responsibility of NIC to:

- Review the issued Certificate to confirm the accuracy of the information contained within it before installation and first use;
- For the Saudi National Root-CA and subordinate CAs, 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 unauthorized 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; and
- 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 Saudi National Root-CA CP; and
- Notify the Registration Authority immediately of a suspected or known key compromise in accordance with the procedures laid down in the Saudi National Root-CA CP.

For the device or organization 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, unauthorized persons could sign fraudulently produced certificates with the key and commit the Issuing Authority to unauthorized obligations and liabilities.

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 the Saudi National Root-CA CP 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; and
- Determining that such Certificate provides adequate assurances for its intended use.

7. Limited Warranty and Disclaimer/Limitation of Liability

The Saudi National Root-CA warrants and promises to:

- Provide certification and repository services consistent with the Saudi National Root-CA CP, CPS and other Operations Policies and Procedures;
- Perform authentication and identification procedures in accordance with applicable agreements and NIC Operations Policies and Procedures;
- Provide certificate and key management services including certificate issuance, publication, revocation and re-key in accordance with the Saudi National Root-CA CP and CPS;
- The Saudi National Root-CA makes no direct warranties or promises to Subscribers or Relying Parties;
- All Application Software Suppliers with whom the Saudi National Root-CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
- Ensure for the performance and warranties of the subordinate CAs that CAs operations will comply with all stipulated requirements, liabilities and obligations.

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

- Due to war, natural disasters, etc.; and
- Due to unauthorized use of certificates or using it beyond the prescribed use defined by the Saudi National Root-CA CP and CPS for the certificates issued by the Saudi National Root-CA.

Limitations on Liability:

- The Saudi National 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 Saudi National Root-CA assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under the Saudi National Root-CA CP for any use other than in accordance with the Saudi National Root-CA CP. Subscribers will immediately indemnify the Saudi National Root-CA from and against any such liability and costs and claims arising there from;
- The Saudi National 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, DTSPs are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by DTSPs or Saudi National 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; and
- Saudi National Root-CA denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

8. APPLICABLE AGREEMENTS, CP, CPS

This document (Saudi National Root-CA PDS), Saudi National Root-CA CP and Saudi National Root-CA CPS can be found at (https://ca.nic.gov.sa).

9. PRIVACY POLICY

The Saudi National Root-CA respects need to appropriately control individual's personal information and to know how such information may be used. The Saudi National 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 Saudi National 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 NIC PKI services, for auditing requirements, or as part of the regulatory compliance. For details please see NIC Privacy Policy at (https://ca.nic.gov.sa).

10. REFUND POLICY

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

11. APPLICATION LAW AND DISPUTE RESOLUTION

Applicable laws are the laws and regulations of the Kingdom of Saudi Arabia. NIC will act in accordance with current legislation in the Kingdom of Saudi Arabia, in particular the e-Transactions Act and its bylaws.

Applicable laws and dispute resolution provisions are in accordance with applicable Saudi National Root-CA Policies and Agreements. NIC PKI Dispute Resolution Policy can be found at (https://ca.nic.gov.sa).

12. CA AND REPOSITORY LICENSES, TRUST MARKS, AND AUDIT

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, NIC may require ad-hoc compliance audits of Saudi National Root-CA and any subordinate CA operation to validate that it is operating in accordance with the respective CP, CPS, and other supporting operational policies and procedures.

13. Approved Registration Authorities

The following Registration Authorities has been designated by the Saudi National Root-CA to register subscribers under the Saudi National Root-CA CP:

- Saudi National Root-CA RA.

14. Approved Repositories

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

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

15. Eligible Subscribers

The following types of subscribers are eligible to be issued with certificates by the Saudi National Root-CA under the Saudi National Root-CA CP:

- Subordinate CAs (level One), subject to approval by ~~DGA and~~ NIC;
- Cross certifying with CAs at the international level; and
- Certificates required by the supportive PKI components and functions for the Saudi National Root-CA operations within Saudi National PKI.

16. Certificate Status Information

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

17. Identification of this Certificate Policy

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

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

All Saudi National PKI participants shall refer to the Saudi National Root-CA CP for further detailed information.