SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

NIC GOVERNMENT-CA 2

PKI DISCLOSURE STATEMENT

Document Classification:

Public

Version Number: 1.2

Issue Date: May 22, 2023

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	10/03/2022	NCDC	First Draft
1.1	15/06/2022	Dr Deoraj	Review
1.2	22/05/2023	Ammar Alsofyani	Update the PDS with NIC policies

Document Control

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

Digitally Signed Copy of this document shall be stored at NIC Document Store.

Table of Contents

1. NOTICE

This PKI Disclosure Statement does not substitute or replace NIC Government-CA 2 Certificate Policy (Government-CA 2 CP) under which NIC Government Certification Authority (Government-CA 2) digital certificates are issued. You must read the Government-CA 2 CP published at (https://ca.nic.gov.sa) before you apply for or rely on a certificate issued by the Government-CA 2.

The full Government-CA 2 CP is defined by two documents:

- This document, the Government-CA 2 PKI Disclosure Statement (Government-CA 2 PDS); and
- The Government-CA 2 CP.

The purpose of this document is to summarize and present the key points of the Government-CA 2 CP in a more readable and understandable format for the benefit of Subscribers and Relying Parties.

The Government-CA 2 is owned by the National Information Center. The Government-CA 2 is a Certification Authority under the Saudi National Root-CA. This is achieved by the Saudi National Root-CA issuing a digitally signed CA Certificate that authenticates the Public Key of the Government-CA 2. The Government-CA 2 is responsible for issuing and managing Digital Certificates to Government employees, Citizens, organisation entities and non-human entities (like Servers and Network Devices) within the Government domain, through Digital Trust Service Providers (DTSPs) within the framework.

The Government-CA 2 Policy Authority (Government-CA 2 PA) is responsible for the governance of the Government-CA 2. Its members are appointed by NIC and may include members from Government DTSPs.

The DTSP is an entity which issues and manages digital certificates, electronic signature tools and methods and any other associated services, which operates with or without its own physical certification authority (CA).

The Government-CA 2, subject to the approval of NIC, shall designate specific DTSPs which in turn appoint RAs to perform the Subscriber Identification and Authentication and Certificate request and revocation functions defined in Government-CA 2 CP and related documents.

The Government-CA 2 is hosted in the National Information Center's - PKI Centre (NIC-PKIC) which is responsible for managing Government-CA 2 operations as per the agreed service levels.

The terms used in this document shall have the meanings as defined in NIC PKI Glossary section 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 certificate types supported by Government-CA 2 are covered under Appendix-A in the Government-CA 2 CP document.

The Government-CA 2 signing key is permitted only for signing certificates and CRLs for their defined user communities. For subscribers, key usage depends on type of the certificate.

Certificates issued from the Government-CA 2 to Government employees are normally used by individuals to sign and encrypt e-mail, data and to authenticate to applications (client authentication).

The individual certificate may also be used for other general or specific Government purposes which are not covered explicitly above, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by (1) law of Saudi Arabia, (2) the Government-CA 2 CP and CPS under which the certificate has been issued and (3) Subscriber Agreement.

4. RELIANCE LIMITS

The Government-CA 2 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 the Government-CA 2 PA to:

- Ensure that 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;
- Generate CA private key using multi-person control “m-of-n” split key knowledge scheme;
- Backing up of the CA signing Private Key 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:

- Provide accurate and complete information at all times to the DTSP, both in the certificate request and verification process defined by the DTSP for specific Certificate type to be supplied by the Government-CA 2;
- Review the issued Certificate to confirm the accuracy of the information contained within it before installation and first use;
- Obtain a certificate; make only true and accurate representation of the required information to the DTSP;
- Use the Certificate for legal purposes and restrict to those authorized purposes detailed by the Government-CA 2 CP;

- Notify the DTSP in the event of any information in the Certificate is, or becomes, incorrect or inaccurate; and
- Notify the DTSP immediately of a suspected or known key compromise in accordance with the procedures laid down in the Government-CA 2 Certificate Policy.

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:

- Ensure that reliance on Certificates issued under Certificate Policy is restricted to appropriate uses (see "Certificate Type, Validation Procedures and Usages" which are covered under Appendix-A in the Government-CA 2 CP document);
- Verify the Validity by ensuring that the Certificate has not expired;
- Ensure 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
- Determine that such Certificate provides adequate assurances for its intended use.

7. LIMITED WARRANTY AND DISCLAIMER/LIMITATION OF LIABILITY

The Government-CA 2 warrants and promises to:

- Provide certification and repository services consistent with the CP, CPS and other NIC PKI Operations Policies and Procedures;
- Use its private signing key only to sign certificates and CRLs and for no other purpose;
- At the time of Certificate issuance, the Government-CA 2 implemented procedures for verifying accuracy of the information contained within it before installation and first use;
- Implement a procedure for reducing the likelihood that the information contained in the Certificate is not misleading;
- Maintain 24 x 7 publicly-accessible repositories with current information and replicates Government-CA 2 issued certificates and CRLs;
- Perform authentication and identification procedures in accordance with DTSP agreement and NIC PKI Operations Policies and Procedures;
- Provide certificate and key management services including certificate issuance, publication, revocation and re-key in accordance with the Government-CA 2 CP and CPS; and
- Subscribers or Relying Parties for making no direct warranties or promises.

The Government-CA 2 does not liable for any loss of the 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 Government-CA 2 CP for the certificates issued by the Government-CA 2.

Limitations on Liability:

- The Government-CA 2 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 Government-CA 2 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 Government-CA 2 from and against any such liability and costs and claims arising there from;
- The Government-CA 2 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 and 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 Government-CA 2;
- Subscribers to compensate a Relying Party which incurs a loss as a result of the Subscribers breach of Subscriber's agreement;
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations described in the Relying Party agreement;
- Digital Trust Service Providers (DTSPs) shall bear the consequences of their failure to perform the Registration Authorities obligations described in the DTSP agreement; and
- Government-CA 2 denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

8. APPLICABLE AGREEMENTS, CP, CPS

Subscriber Agreement is submitted with the Subscriber's Request Form to the DTSP in order to obtain valid certificate.

Government-CA 2 PDS, Government-CA 2 CP and Government-CA 2 CPS can be found at (https://ca.nic.gov.sa).

The DTSP Agreement and Relying Party Agreement shall only be available subject to approval of a formal application in writing to the Government-CA 2 PA.

9. PRIVACY POLICY

The Government-CA 2 respects need to appropriately control individual's personal information and to know how such information may be used. The Government-CA 2 take reasonable care to ensure that the information submitted during the certificate application, authentication of identity and certification processes will be kept private. The Government-CA 2 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 subscriber's prior consent, unless otherwise required by law, or except as may be necessary for the performance of NIC services, for auditing requirements, or as part of the regulatory compliance. For details please see NIC PKI Privacy Policy at (https://ca.nic.gov.sa).

10. REFUND POLICY

Currently, no fees are charged by Government-CA 2 for Digital Certificates, although Government-CA 2 reserves the right to change this in the future. Digital Certificates for which no charge is made, no refunds are possible. In addition a Government DTSP may charge fees for its service.

11. APPLICABLE 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 Government-CA 2 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 DTSPs wish to join the Government-CA 2 are granted a non-exclusive license solely for the operations under the Government-CA 2.

The Government-CA 2 shall be subjected to periodic compliance audits which are no less frequent than once a year and after each significant change to the deployed procedures and techniques. Moreover, NIC may require ad-hoc compliance audits of any CA's operation to validate that it is operating in accordance with the applicable CP, CPS, Audit and Compliance Policy and NIC PKI Operations Policies and Procedures. Similarly, the Government-CA 2 PA has the right to require periodic inspections of its DTSPs to validate that the DTSPs are operating in accordance with the Government-CA 2 CP and DTSP agreement. The Government-CA 2 shall internally audit each delegated third party's (DTSP, RA & TA) compliance against defined requirements on an annual basis.

NIC shall also be performing self-audits at least on a quarterly basis against a randomly selected sample for monitoring adherence and service quality.

13. APPROVED DTSP AND REGISTRATION AUTHORITIES

The application process for DTSPs under Government-CA 2 would be as per the Government DTSP Joining Process and NIC shall decide on the acceptance or rejection of the DTSP application request based on fulfillment of requirements. All RA(s) under the approved DTSPs shall be operational only after satisfying NIC RA compliance requirements.

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 Government-CA 2; and
- The certificate revocation list (CRL) for Government-CA 2.

15. ELIGIBLE SUBSCRIBERS

The Government-CA 2 is responsible for issuing and managing Digital Certificates to Government employees, Citizens, organization entities, non-human entities (like Servers and Network Devices) within the Government domain. These certificates are given through the Digital Trust Service Providers (CSPs) within the framework.

NIC DTSP shall be entitled for issuing digital certificates to any organization operating in the Kingdom of Saudi Arabia; with prior approval of CA PA to address business requirements.

16. CERTIFICATE STATUS INFORMATION

The Government-CA 2 will publish its CRLs at least once every 24 hours, and at the time of any Certificate revocation of its subscribers.

17. IDENTIFICATION OF THIS CERTIFICATE POLICY

This document has been registered with Government-CA 2 and has been assigned an object identifier as below:

Government-CA 2 PDS Document: 2.16.682.1.101.5000.1.3.1.1.3

All Government-CA 2 PKI participants shall refer to NIC Government-CA 2 CP for further detailed information.