SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

NIC GOVERNMENT-CA 2

CERTIFICATE POLICY

Document Classification:

Public

Version Number: 1.3

Issue Date: July 25, 2023

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	10/03/2022	NCDC	Initial Document
1.1	15/06/2022	Dr Deoraj	Review
1.2	11/10/2022	Ammar Alsofyani	Update the CP with NIC policies
1.3	25/07/2023	Ammar Alsofyani	Update on section 5.1.2 (add the security guard control for any CA activity)

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. INTRODUCTION

The Government of Saudi Arabia has embarked on an ambitious e-transaction program, recognizes that there is a tremendous opportunity to better utilize information technology to improve the quality of care/service, lower the cost of operations, and increase customer satisfaction. To ensure the secure, efficient transmission and exchange of information electronically, the Kingdom of Saudi Arabia has created a National Public Key Infrastructure. at National Information Center (NIC). National Information Center (NIC) is an entity under the Saudi Data and AI Authority in the Kingdom of Saudi Arabia. The national PKI at NIC is created by an act of law and its mandate is stipulated in the Saudi e-Transactions Act and its bylaws.

NIC provides trust services to secure the exchange of information between key stakeholders. Participants include:

- Government
- Citizens
- Businesses

The Government Certification Authority 2 (henceforth referred as Government-CA 2) is owned by the Saudi Data and AI Authority (SDAIA). 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 is hosted in the National Information Center – PKI Center (NIC-PKIC) which is responsible for managing Government-CA 2 operations as per the agreed service levels.

This CP shall define the policies by which the Government-CA 2 operates. This CP complies with the Saudi National PKI Policy and in line with Internet Request for Comment (RFC) 3647 [RFC 3647]. 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.

1.1 OVERVIEW

This CP defines different level of certificate trust and assurance for use by all Government-CA 2 PKI participants.

Assurance level is determined by a number of factors, including the:

- Strength of the binding between a Public Key and the individual whose Subject name is cited in the Certificate;
- Mechanisms used to control the use of the Private Key; and
- Security provided by the PKI itself.

The certificate types supported by the Government-CA 2 under Saudi National PKI framework are covered under Appendix-A. This defines the requirements and criteria for issuance and management of PKI certificates asserting distinct Levels of Assurance as advised to subscriber and any Relying Parties.

This CP has been developed under the direction of the Government-CA 2 Policy Authority (PA) and that group has the responsibility for directing the development, approval and update of the Government-CA 2 CP.

Any use of or reference to this CP outside the context of the Government-CA 2 and Saudi National PKI is completely at the using party's risk. The terms and provisions of this CP shall be interpreted under and governed by the Government-CA 2 CPS and NIC PKI Operations Policies and Procedures.

As described in this CP, the Government-CA 2 will establish a hierarchical trust with the self-signed off-line Saudi National Root-CA.

It is the responsibility of all parties applying for or using a Digital Certificate issued under this CP, to read this CP and the PKI Disclosure Statement (PDS) to understand the practices established for the lifecycle management of the Certificates issued by the Government-CA 2. Any application for Digital Certificates or reliance on validation services of the Government-CA 2 issued Certificates signifies understanding and acceptance of this CP and its supporting policy documents.

1.1.1 CERTIFICATE POLICY

X.509 certificates issued by Government-CA 2 to subscribers will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party (RP) to decide whether a Certificate is trusted for a particular purpose. Subscriber Certificates issued by the Government-CA 2 will identify the applicable policy in the certificate policies extension by including applicable OID(s).

1.1.2 RELATIONSHIP BETWEEN THE CP AND THE CPS

The Government-CA 2 CP states what assurance can be placed in a certificate issued by Government-CA 2 to subscriber participating in the Saudi National PKI. The Certificate Practice Statement (CPS) states how the Government-CA 2 meets the requirements of this CP.

The CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by Government-CA 2 as governed by this CP and related documents which describe NIC requirements and use of Certificates.

1.1.3 INTERACTION WITH OTHER PKIS

NIC will decide on issues related to cross-certification with other Certification Authorities as per the NIC PKI Cross Certification Policy.

1.1.4 SCOPE

This CP applies to all certificates issued by the Government-CA 2. The Government-CA 2 is a subordinate CA in the Saudi National PKI hierarchy, maintained and operated by NIC in an online environment for issuance and management of Subscriber certificates and revocation lists. More specifically, the Government-CA 2 issues Subscriber certificates and certificates for its DTSPs.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the Government-CA 2 Certificate Policy (CP), and is identified by the object identifier (OID):

OID: 2.16.682.1.101.5000.1.3.1.2.1

Please refer to the latest OID Allocation document available on https://ca.nic.gov.sa.

1.3 PKI PARTICIPANTS

The following are roles relevant to the administration and operation of the Government-CA 2 under the Government-CA 2 CP.

1.3.1 CERTIFICATION AUTHORITIES

The term CA refers to any entity approved by NIC to join the Saudi National PKI, directly under the Saudi National Root-CA. On successfully joining the Saudi National PKI; CA is entitle to issue certificates after mapping to one of the policy OIDs listed in the NIC OID Allocation document, which can be found at https://ca.nic.gov.sa. CAs will issue subscriber certificates, OCSP responder certificates and other certificates required by PKI components. CAs, acting on behalf of DTSPs, will issue certificates to Subscribers in accordance with their DTSP Agreement, Subscriber Agreement, Relying party Agreement, their respective CP/CPS, and, the Saudi National PKI Policy. The CA will describe which subscriber types they will support, which certificate types they will issue and determine the level of warranties and liabilities.

The Government-CA 2 is responsible for:

- Control over the designation of RAs;
- Control over the designation of DTSPs;
- The Certificate generation process;
- Publication of Subscriber Certificates;
- Revocation of Subscriber Certificates;
- Publication of revocation information;
- Re-key of Subscribers;
- Conduct regular internal security audits;
- Conduct compliance reviews of its DTSPs;
- Assist in audits conducted by or on behalf of NIC; and
- Performance of all aspects of the services, operations and infrastructure related to the Government-CA 2.

1.3.2 REGISTRATION AUTHORITIES

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 this CP and related documents.

The DTSP RA is obligated to perform certain functions pursuant to an RA Agreement including the following:

- Process Certificate application requests in accordance with this CP, Government-CA 2 CPS and applicable RA Agreement, and other policies and procedures with regard to the Certificates issued;
- Maintain and process all supporting documentation related to the Certificate application process;
- Process Certificate Revocation requests in accordance with Government-CA 2 CP and CPS, applicable RA Agreement, and other relevant operational policies and procedures with respect to the Certificates issued. Without limitation to the generality of the foregoing, the RA shall request the revocation of any Certificate that it has approved for issuance according to the conditions described later in section 4.9.1;
- Comply with the provisions of its RA Agreement and the provisions of the Government-CA 2 CP and CPS including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements; and
- Follow NIC PKI Privacy policy in accordance with Government-CA 2 CP and CPS and applicable RA Agreement.

1.3.3 SUBSCRIBERS

Subscribers are individuals (end users) and entities (organizations) to whom certificates are issued. Subscribers are bound by the conditions of use of certificates as contained in the Subscribers Agreement. In general, the subscriber asserts that he or she uses the key and certificate in accordance with the Government-CA 2 CP.

1.3.4 SUBJECTS

A Subject is the entity named or identified in a certificate and who/which holds or controls a private key corresponding to the public key listed in the Certificate. A Subject may also be a Subscriber.

1.3.5 RELYING PARTIES

A Relying Party is the entity that relies on the validity of the binding of the subscriber's identity to a public key. The Relying Party is responsible for checking the validity of the certificate by examining the appropriate certificate status information, using validation services provided by the Government-CA 2. A Relying Party's right to rely on a certificate issued under this CP, requirements for reliance, and limitations thereon, are governed by the terms of the Government-CA 2 CP and the Relying Party Agreement.

Relying Parties shall use the Saudi National PKI, and rely on a certificate that has been issued under the Government-CA 2 CP if:

- The certificate has been used for the purpose for which it has been issued, as described in the Government-CA 2 CP, and applicable Subscriber Agreement;
- The Relying Party has verified the validity of the digital certificate, using procedures described in the Relying Party Agreement;
- The Relying Party has accepted and agreed to the Relying Party Agreement at the time of relying on the certificate; it shall be deemed to have done so by relying on the certificate; and

- The relying party accepts in totality, the certificate policy applicable to the certificate, which can be identified by reference of the certificate policy OID mentioned in the certificate.

1.3.6 OTHER PARTICIPANTS

1.3.6.1 Government-CA 2 Policy Authority (Government-CA 2 PA)

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. Its tasks include:

- Ensuring the operation of the Government-CA 2 comply with the requirements of the Government-CA 2 CP, PDS, CPS and NIC PKI Operations Policies and Procedures;
- Review and approve the Subscriber Agreement, Relying Party Agreement and other related Agreements based on the Government-CA 2's specific business requirements;
- Seeking resolution of disputes between participants operating in its domain;
- Establishing and implementing its own CP, PDS and CPS in conjunction with the Saudi National PKI Policy document; and
- Act as liaison with NIC.

1.3.7 DIGITAL TRUST SERVICE PROVIDER (DTSP)

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 DTSP is owned by an organization which is approved by Government-CA 2 PA and NIC to be remotely connected to the Government-CA 2 to facilitate certificate life cycle management to its own class of subscribers.

The DTSP comprise of Policy Administrator (PA), Registration Authority (RA), and Local Registration Authority (LRA) (if needed).

1.3.7.1 Policy Administrator (DTSP PA)

Policy Administrator (PA) is responsible for the governance of the DTSP. These Policy Administrators are located at various Government DTSPs. Its tasks include:

- Ensuring DTSP operations complying with Government-CA 2 CP requirements;
- Ensuring RA operations complying with Government-CA 2 CP and RA security requirements;
- Conduct compliance reviews of its RAs;
- Assist in audits conducted by or on behalf of NIC;
- Establishing and implementing policies and procedures as required by Government-CA 2 and NIC; and
- Act as liaison with Government-CA 2 and NIC.

1.3.8 TRUSTED AGENT

Trusted Agents (TAs) can perform the identity proofing duties of an RA when authorized to do so by a PA. TAs are obligated to operate in accordance with the TA Agreement, Government-CA 2 CP, CPS and NIC PKI Operations Policies and Procedures.

1.3.9 DEVICE SPONSOR

The Device Sponsor shall serve as the representative of a Device to a DTSP in order to register the device as a Subject with the Government-CA 2. The requirements for device Sponsors in the Government-CA 2 are set forth under Appendix-A.

1.3.10 ONLINE CERTIFICATE STATUS PROTOCOL RESPONDER

Online Certificate Status Protocol (OCSP) Responders and Simple Certificate Validation Protocol (SCVP) status providers may provide revocation status information or full certification path validation services respectively. The Government-CA 2 may make their Certificate status information available through an OCSP responder in addition to any other mechanisms they wish to employ. The Government-CA 2 shall publish status information for the certificates it issues in a Certificate Revocation List (CRL).

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The Government-CA 2 may issue some or all of the following types of certificates:

- Confidentiality certificates, where the certificate is used for encryption to ensure the confidentiality and secrecy of data;
- Signatures certificates, where the certificate is used to assure the message integrity, bind the signer to the document or transaction and provide Non-repudiation (the elimination of deniability); and
- Authentication certificates, where certificates are used to identify/authenticate the subscriber to services and applications.

The Government-CA 2 issues certificates under this CP only to those Government end entities who have signed their acceptance of a Subscriber Agreement in the appropriate form and whose application for certificates has been approved by DTSP.

The following certificate assurance levels are supported for end-entity certificates issued by the Government-CA 2. The Government-CA 2 will assess the risk and apply the appropriate rating.

Assurance Level	Description and Assurance Level
Low	This level provides little confidence in the accuracy or legitimacy of the claimed identity as it requires no or low assurance of the binding between the identity of the entity named in the certificate and the Subscriber. It is intended for Subscribers handling information of little or no value within minimally secured environments. Identity

	assertions at this level are appropriate for transactions with minimal consequences to Relying Parties from the registration of a fraudulent identity. Digital certificates at this level require no or low assurance of the binding between the identity of the entity named in the certificate and the Subscriber. The keys and certificates can only be generated in a software security module and be stored in a software form factor. Given the limited assurance provided, a Key Usage of non-repudiation is not permitted, nor are Extended Key Usages of smartcard logon or code signing.
Medium	This level provides medium confidence in the accuracy or legitimacy of the claimed identity. It is intended for Subscribers handling information of medium value within substantially secured environments. Identity assertions at this level are appropriate for transactions with serious (substantial) consequences to Relying Parties from the registration of a fraudulent identity. The keys and certificates at this level can be generated in either a software or hardware security module and can be stored in either a software or hardware form factor. User consent is required each time the private key is activated.
High	This level provides a high confidence in the accuracy or legitimacy of the claimed identity. It is intended for Subscribers handling information of high value within highly secured environments. Identity assertions at this level are appropriate for transactions with catastrophic consequences to Relying Parties from the registration of a fraudulent identity. Digital certificates at this level require very high assurance of the binding between the identity of the entity named in the certificate and the certificate holder. The keys and certificates can only be generated in a hardware security module and can only be stored in a hardware form factor. Authenticated-user's consent or PIN unlocks are required each time the private key is activated.

1.4.1.1 Certificate Issued to Employees

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).

Following are some of the common usage of the certificate:

- Inter-Government Correspondence;
- Information Publication;
- Forms Submission;
- Application work-flow; and

- e-Tendering.

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 the CPS under which the certificate has been issued and (3) Subscriber's agreement.

1.4.1.2 Certificate Issued to Organizational Entity

Certificates issued to Organizational entities assure the identity of the Subscriber based on a confirmation that the Subscriber organization does in fact exist, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Subscriber was authorized to do so. These certificates can be used for the purposes covered under employee certificate in the previous paragraph.

1.4.1.3 Certificate Issued to Device

If the Certificate subject is a device, then the device shall have a sponsor authorized by the device sponsor to apply for a certificate as mentioned in section Appendix-A.

1.4.2 PROHIBITED CERTIFICATE USES

Certificates issued under this CP shall not be authorized for use in any circumstances or in any application which could lead to death, personal injury or damage to property, or in conjunction with on-line control equipment in hazardous environments such as in the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control or direct life support machines, and the Government-CA 2 shall not be liable for any claims arising from such use.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

This CP is administered by the Government-CA 2 PA (see section 1.3.6.1).

1.5.2 CONTACT PERSON

Queries regarding Government-CA 2 CP shall be directed at:

Email: pki@nic.gov.sa

Telephone: +966 11 8081013

Any formal notices required by this CP shall be sent in accordance with the notification procedures specified in section 9.12.2 of this CP.

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The Government-CA 2 PA is responsible for approving the Government-CA 2 CPS and establishing that the Government-CA 2 conforms to the requirements of this CP in accordance with policies and procedures specified by NIC.

1.5.4 CPS APPROVAL

Changes or updates to the Government-CA 2 CPS document must be made in accordance with the stipulations of Saudi e-Transactions act and bylaws and the provisions contained in this CP and are subject to Government-CA 2 Policy Authority approval.

1.6 DEFINITIONS AND ACRONYMS

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. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Government-CA 2 issued certificates and certificate revocation lists (CRLs) will be published in repositories. NIC shall operate Repositories to support the Government-CA 2's operations. The repositories shall be directories that provide access through an appropriate standard-based access protocol.

Repositories shall support operations on a 24x7 basis as determined by the applicable agreements and NIC PKI Privacy Policy (and subject to routine maintenance) and replicate Government-CA 2 issued certificates, CRLs and Authority Revocation Lists (ARLs) repositories in order to enhance the overall performance and provide high availability for its validation services.

2.1.1 REPOSITORY OBLIGATIONS

Repositories shall support:

- An appropriate standard-based access protocol;
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP and Government-CA 2 CPS; and
- Access control mechanisms, when necessary to protect the repository availability and information as described in later sections.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

The Government-CA 2 shall publish in the appropriate repository: CA Certificates, subscriber Certificates, and CRLs.

Government-CA 2 PA will decide on directory access restrictions to prevent misuse and unauthorized harvesting of information.

2.2.2 PUBLICATION OF CA INFORMATION

This CP shall be made available to all Government-CA 2 PKI participants at NIC website https://ca.nic.gov.sa. This web site is the only source for up-to-date documentation and Government-CA 2 reserves the right to publish newer versions of the documentation without prior notice.

Additionally, the Government-CA 2 will publish an approved, current and digitally signed version of the Government-CA 2 CPS and its PDS. This CP, CPS an PDS are provided as public information documents and are only valid if they are published as a PDF, digitally signed by NIC.

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.

2.2.3 INTEROPERABILITY

Repositories used to publish CA certificates, CRLs, and Subscriber Certificates shall employ standard-based scheme for directory objects and attributes, at least, LDAPv3.

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificates shall be published promptly following their generation and issuance. CRL information shall be published as set in section 4.9.7.

This CP and any subsequent changes should be made available to the participants as set forth in section 2.2.2 within two week of approval by the Government-CA 2 PA and NIC.

This CP and PDS are provided as public information on NIC official web site. Public documents are only valid if they are published as a PDF, digitally signed by NIC.

2.4 ACCESS CONTROLS ON REPOSITORIES

The Government-CA 2 shall protect repository information not intended for public dissemination or modification through the use of strong authentication, access controls, and an overall Information Security Management System that prevents unauthorized access to information.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

Each Certificate must have a unique identifiable Distinguished Name (DN) according to the X.500 standard. Naming conventions for the Government-CA 2 are approved by the Saudi National Root-CA, while Government-CA 2 approves RAs and DTSPs. The subscriber's name is approved by DT

SPs.

Details of these are found in the Certificate Types under Appendix-A in this CP.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The Subscriber's certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates are understood and used by Relying Parties.

The subject name contained in the Government-CA 2 certificate must be meaningful in the sense that the Saudi National Root-CA is provided with proper evidence of the association existing between the name and the entity to which it belongs.

The Government-CA 2 DN (LDAP Notation) in the Issuer field of all certificates and CRLs that are issued will be:

CN=Government CA 2, O=National Center for Digital Certification, C=SA

The certificate types supported by Government-CA 2 are covered in Certificate Types under Appendix-A.

Pilot/Test DTSPs are identified by including the word "TEST" in the DTSP name which is included in the subject DN as an Organizational Unit. Thus Certificates issued by Pilot/Test DTSPs are not subject to follow all verification/identification policies and procedures, and thus should not be relied upon.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The use of anonymous certificates is prohibited. The Government-CA 2 may issue pseudonymous certificates pursuant to the approval of NIC.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

The naming convention used by Government-CA 2 is ISO/IEC 9595 (X.500) Distinguished Name (DN). The Government-CA 2 may further stipulate how names are to be interpreted by publishing such rules in the Government-CA 2 CPS.

3.1.5 UNIQUENESS OF NAMES

All distinguished names shall be unique across the Government-CA 2.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

Certificate applicants are prohibited from using names in their certificate application that infringe upon the Intellectual Property Rights of others. The Government-CA 2, DTSPs, however, does not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application.

Any name collisions or disputes regarding Certificates issued by the Government-CA 2 shall be resolved as per NIC PKI Dispute Resolution Policy. The Government-CA 2 PA is responsible for ensuring name uniqueness through its DTSPs.

The Government-CA 2 shall have the right to revoke a Certificate upon receipt of a properly authenticated order from NIC, a DTSP, an arbitrator or court of competent jurisdiction requiring the revocation of a Certificate or Certificates containing a Subject name in dispute.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

The Certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the certificate.

Where keys are generated on behalf of the Subscriber by the Government-CA 2 e.g., when using centralised signing, the Certificate Authority shall perform proof of possession on behalf of the Subscriber.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

Entities wishing to join Saudi National PKI hierarchy or cross certify with the Saudi National Root-CA shall be authenticated in accordance with NIC specifications and requirements. In all cases, NIC personnel will verify the information in the application, the authenticity of the requesting representative and the representative's authorization to act in the name of the requesting CA.

3.2.3 AUTHENTICATION OF INDIVIDUAL IDENTITY

The DTSP will ensure that the Applicant's identity information is verified. Minimal procedures for RA authentication of Subscribers shall be described in the Government-CA 2 CPS and respective verification process applicable to specific certificate types is provided in Appendix-A of this document, which is mandated.

If the Certificate subject is a device, then the device shall have a human sponsor authorized by the device owner to apply for a certificate. The Government-CA 2 will authenticate, through an approved DTSP, the identity of the sponsor applying for the device Certificate.

The Government-CA 2 may specify additional requirements including proof that the device sponsor applying for the device certificate is authorised to apply for a device certificate for that particular device apart from the standard process mentioned above and covered in the respective agreement. Respective verification process applicable to specific certificate types is provided in Appendix -A of this document, which is mandated.

If the Certificate subject is an organizational entity, then an authorized representative of the entity applies for a certificate. The Government-CA 2 will authenticate, through an approved

DTSP, the identity and authorization of this representative. The identity of the representative must be authenticated and their authority to represent the organisation must be validated. Authentication processes must include face-to-face authentication with the representative of the organisation, or other form of direct registration by a representative of the organisation.

For RA certificates under a DTSP an NIC Representative will strongly validate the identity of the requestor by ensuring the authenticity of the RA through validating his identity.

Respective verification process applicable to specific certificate types is provided in Appendix -A of this document, which is mandated.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Non-verified information shall not be included in strong assurance certificates issued under Government-CA 2, unless specifically mentioned in the Certificate Types section in Appendix-A.

3.2.5 VALIDATION OF AUTHORITY

See section 3.2.3

3.2.6 CRITERIA FOR INTEROPERATION

No stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Subscribers shall identify themselves to the Government-CA 2 using their current Authentication Keys.

Routine re-key of RA Certificate shall follow the NIC Level-One CA Operations Policy section 8.

For re-key of a Government-CA 2, a representative shall provide proper information to authorize the required information to authorise the request in accordance with the Saudi National Root-CA Operations Policy section 11.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

If a Subscriber Certificate is revoked, the Subscriber shall go through the initial identity-proofing process again for the respective certificate type to obtain a new certificate.

If a Government-CA 2 certificate is revoked for any reason, a representative of the Government-CA 2 shall provide sufficient information to prove his authorization for re-key and NIC shall re-assess, whether the requirements listed are still valid, before a re-keying is initiated, in accordance with the Saudi National Root-CA Operations Policy section 11.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Prior to the revocation of a Certificate, a Government-CA 2 shall verify that the revocation has been requested by an entity authorized to request revocation. Acceptable procedures for authenticating the revocation requests are described in the CPS.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

This section specifies the requirements for initial application for certificate issuance by the Government-CA 2. The DTSP will perform the following steps when an applicant applies for a certificate:

- Establish the applicant's authorization to obtain a certificate;
- Establish and record the identity of the applicant; and
- Transmit to the Government-CA 2 a confirmation that the Applicant has met the authentication requirements and the information which is to appear in the Certificate.

The Government-CA 2 will perform the following steps when it receives the confirmation and certificate information from the DTSP:

- Verify that the transmission is from an authorized DTSP;
- Generate the Certificate relating to that Applicant; and
- Transmits the Certificate to the Applicant and/or to the requesting DTSP.

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

Subscriber certificate applicants, including those applying for a device or entity certificate, will follow the application process specified in respective certificate type of Appendix-A. Certificate applications may be requested by:

- The Government-CA 2 for its CA certificate;
- A subscriber for his individual certificate;
- A sponsor for a device certificate; or
- An authorized representative for an Organizational Certificate.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

4.1.2.1 Subscribers

Subscribers shall follow the procedures published by the DTSPs for certificate application.

4.1.2.2 DTSP Certificates

An entity wishing to become DTSP under the Government-CA 2 shall agree to the terms of the DTSP Agreement as part of the application process. The DTSP applicants shall provide their credentials to demonstrate their identity and contact information during the application process.

All applicants shall agree to the terms and conditions of the applicable Agreement, such as: Subscriber, Relying Party, Registration Authority, Local Registration Authority or Trusted Agent Agreements.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

DTSPs shall perform identification and authentication of all required Subscriber information as described in Appendix-A of this CP.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

The DTSP will approve an application for a subscriber certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information as described in Appendix-A of respective certificate type.

The DTSP will reject a certificate application if:

- Identification and authentication of all required Subscriber information cannot be completed;
- The Subscriber fails to furnish supporting documentation upon request;
- The Subscriber fails to respond to notices within a specified time; or
- The DTSP believes that issuing a certificate to the Subscriber may bring the Government-CA 2 into disrepute.

Policies specific to each certificate type have been detailed in the Certificate Types section in Appendix-A. It is mandatory to comply with all policies specific to the respective certificate type.

For RA certificate under DTSP, the DTSP shall ensure that its RA which is applying for certification meets the entitlement requirements for RA certification, in accordance with the NIC Level-One CA Operations Policy section 7.

The application process for DTSPs under the 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.

NIC shall reject a certificate if the requested Public Key has a weak Private Key.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

The time to process certificate applications is specified in the relevant Agreement between the PKI participants.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

When DTSPs receive a request for Certificate, it shall not be issued before the applicant accepts the terms of a Subscriber Agreement, and successfully completes the application form.

Following successfully completion of the registration process, the Government-CA 2 shall create and sign the certificate if all certificate requirements have been met, and make the certificate available to the subscriber.

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE

Subscriber certificates shall be issued directly using a controlled process where the Subscriber takes immediate receipt of the certificate. This provides direct notification of certificate issuance.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Certificate acceptance is governed by the agreements set out between the DTSP and Applicants, any requirements imposed by Government-CA 2 CP and CPS and the relevant agreements under which the certificate is being issued.

The use of a Certificate or the reliance upon a Certificate signifies acceptance by that person of the terms and conditions of the CP and applicable agreements by which they irrevocably agree to be bound.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

Certificates will be published, once accepted, in the appropriate repository as described in section 2.1.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

NIC shall be notified upon the issuance of Government-CA 2 Certificate by the Saudi National Root-CA.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscribers shall use their Certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of the Subscriber Agreement, this CP, and applicable laws. Subscribers shall protect their Private Keys from access by any other party and shall notify the DTSP upon the compromise of the private key or any reasonable suspicion of compromise.

Subscribers shall discontinue use of private key(s) following expiration or revocation of the associated certificate except for decryption private key(s).

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

The Relying Party Agreement becomes effective when an RP relies on information provided by the Government-CA 2 or a subscriber regarding a specific transaction that the RP uses to accept or reject their participation in the transaction. The RP's use of the Repository, or any CRL or OCSP services is governed by the RP Agreement and Government-CA 2 CP. The RP

is solely responsible for deciding whether or not to rely on the information in a certificate provided by Government-CA 2. The RP bears the legal consequences of any failure to comply with the obligations set in the RP agreement.

4.6 CERTIFICATE RENEWAL

Certificate renewal is the issuance of a new certificate without changing the public key or any other information in the certificate. Certificate renewal is not supported for Government-CA 2 issued certificates.

4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL

See section 4.6.

4.6.2 WHO MAY REQUEST RENEWAL

See section 4.6.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

See section 4.6.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See section 4.6.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

See section 4.6.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

See section 4.6.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

See section 4.6.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate (key update) refers to the issuance of new certificate with a different key pair and serial number while retaining other subject information from old certificate.

The new Certificate may be assigned a different validity period and/or signed using a different issuing CA private key.

4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

Manual Certificate re-key may take place after a certificate is revoked and the subscriber information is still accountable. Manual Certificate re-key may also be performed within one-month of certificate expiry, or after certificate expiry.

Automatic updates of managed digital IDs and any or all the certificates constituting the digital ID may be performed on or after reaching 70% of the certificate lifetime.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

In accordance with the conditions specified in previous section, Certificate re-key may be requested by:

- The Government-CA 2 for its CA certificate;
- A subscriber for his individual certificate;
- A sponsor for a device certificate; or
- An authorized representative for an Organizational Certificate.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

Only after verifying a re-key request from subscriber or authorized representative shall processing of a certificate re-keying request be initiated.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Subscriber certificates shall be issued directly to Subscribers using a Subscriber controlled process. This provides direct notification of certificate issuance.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Conduct constituting acceptance of a re-keyed certificate is same as listed in section 4.4.1.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

After successful completion of the re-key process, certificate shall be published in appropriate repositories.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Generally, Government-CA 2 does not notify other entities of a re-keyed certificate apart from requesting DTSP.

4.8 CERTIFICATE MODIFICATION

Certificate modification for all applicants will be accomplished through Certificate re-key as specified in section 4.7.

The Government-CA 2 CP does not support other forms of Certificate modification.

4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION

See Section 4.8.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

See Section 4.8.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

See Section 4.8.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

See Section 4.8.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

See Section 4.8.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

See Section 4.8.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

A Certificate shall be revoked/suspended when the binding between the Subject and the Subject's Public Key defined within a Certificate is no longer considered valid.

The CA and/or DTSP will notify subscribers of certificate revocation or suspension using any of the below methods:

- Access to the CRL in the CA repository;
- Email notification to subscriber (Such notification is deemed complete, once the email is sent by NIC to the subscriber's registered email address.); or
- Telephonic notification to subscriber.

The CA will notify other participants of certificate revocation or suspension through access to the CRL in the CA repository.

4.9.1 CIRCUMSTANCE FOR REVOCATION

A Certificate Authority shall revoke Certificates of the Subscriber for the following reasons:

- Contravened any provisions of the Saudi e-Transactions Act and Bylaws made there under;
- The Subject has failed to meet its obligations under this CP or any other applicable Agreements, regulations, or laws;
- NIC suspects or determines that revocation of a Certificate is in the best interest of the integrity of NIC;

- The Government-CA 2 determines that a Certificate was not issued correctly in accordance with this CP;
- There has been an improper or faulty issuance of a certificate due to:
  - A material prerequisite to the issuance of the Certificate not being satisfied;
  - A material fact in the Certificate is known, or reasonably believed, to be false.
- The CA is made aware of a material change in the information contained in the Certificate;
- The subscriber of the Certificate asks for his Certificate to be revoked due to:
  - The Subscriber's private key is suspected to be compromised;
  - The cryptographic storage device of the Subscriber is lost or stolen;
  - If he no longer wishes to use the certificate.
- For SMIME certificates, any reason not provided above, but specified in Section 6.2 of the Mozilla Root Store Policy.

4.9.2 WHO CAN REQUEST REVOCATION

The following entities can request revocation of a certificate:

- NIC can request the revocation of any certificates issued by any CA participating in the Saudi National PKI;
- The Government-CA 2 PA can request the revocation of any certificates issued under its authority;
- The Government-CA 2 can request the revocation of any RA or LRA certificates;
- A DTSP, RA, or LRA can request the revocation of any of their Subscribers Certificate;
- The RA for their own certificate, if any suspected misuse has been attributed to their given Certificates;
- Subscribers, if any suspected misuse has been attributed to their given Certificates, can request a revocation; and
- A legal, judicial or regulatory agency in Saudi Arabia, can request certificate revocation, within applicable laws and in coordination with NIC.

If any request for revocation cannot be resolved, the request is subject to the Dispute Resolution process described in NIC PKI Dispute Resolution Policy.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The CA or RA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements. For Revocation of RA Certificates refer to NIC Level-One CA Operations Policy section 9.

4.9.4 REVOCATION REQUEST GRACE PERIOD

Revocation request grace period is not permitted once a revocation request has been verified.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

The Government-CA 2 shall process authorized revocation requests within 24 hours.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

Relying Parties should comply with the signature validation requirements defined in the Relying Party Agreement.

4.9.7 CRL ISSUANCE FREQUENCY

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.

4.9.8 MAXIMUM LATENCY FOR CRLS

CRLs shall be published in the Repositories within 10 minutes of Certificate revocation. Certificate status information is updated within 30 minutes of certificate revocation.

4.9.9 ONLINE REVOCATION/STATUS CHECKING AVAILABILITY

Government-CA 2 may provide access to an OCSP Responder covering the certificates they issue.

4.9.10 ONLINE REVOCATION CHECKING REQUIREMENTS

The Government-CA 2 may make its Certificate status information available through an OCSP responder.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

The Government-CA 2 will not provide other forms of revocation advertisements.

4.9.12 SPECIAL REQUIREMENTS RE KEY COMPROMISE

If NIC discovers, or has a reason to believe, that there has been a compromise of the private key of the Government-CA 2, NIC will immediately declare a disaster and invoke NIC PKI business continuity plan. NIC will (1) determine the scope of certificates that must be revoked, (2) publish a new CRL at the earliest feasible time, (3) use reasonable efforts to notify DTSPs, subscribers and potential relying parties that there has been a key compromise, and (4) generate new CA key pair as per NIC Level-One CA operations policies and procedures.

4.9.13 CIRCUMSTANCES FOR SUBSCRIBER CERTIFICATE SUSPENSION

The Government-CA 2 has the option to suspend Certificates under the circumstances described in section 4.9.1.

4.9.14 WHO CAN REQUEST SUSPENSION

The following entities can request suspension of a Certificate:

- NIC can request the suspension of any certificates issued by any CA participating in the Saudi National PKI;
- The PA can request the suspension of any certificates issued under its authority;
- The Government-CA 2 can request the suspension of any RA or LRA certificates;
- A CA, RA, or LRA can request the suspension of one of their Subscribers Certificate;
- The RA for their own certificate, if any suspected misuse has been attributed to their given Certificates;
- Subscribers, if any suspected misuse has been attributed to their given Certificates, can request a suspension; and
- A legal, judicial or regulatory agency, can request a suspension.

If any request for suspension cannot be resolved, the request is subject to the Dispute Resolution process described in the Dispute Resolution Policy.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

A request to suspend a certificate shall identify the certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated (e.g., digitally or manually signed). The CA or RA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements. For suspension of RA Certificates refer to NIC Level-One CA Operations Policy section 11.

4.9.16 LIMITS ON SUSPENSION PERIOD

The maximum period for which a Certificate can be suspended will be defined by the Government-CA 2 Policy Authority but shall not exceed ninety (90) days.

4.9.16.1 Circumstances for Terminating Suspended Certificates

A suspended Certificate is reactivated when the entity which requested the suspension of a Certificate is satisfied that the circumstances leading to the suspension are no longer valid. Once reactivated, the certificate will be valid for the remainder of its initial life time.

A suspended Certificate is revoked when the entity which requested the suspension of a Certificate is satisfied that the circumstances leading to the suspension are indeed valid.

When the period for suspension has reached its maximum duration without resolution, the certificate will be revoked.

4.9.16.2 Procedure for Terminating the Suspension of a Certificate

A request to unsuspend a certificate shall identify the certificate to be unsuspended, explain the reason for unsuspension, and allow the request to be authenticated (e.g., digitally or manually signed). The Government-CA 2 or RA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements.

4.10 CERTIFICATE STATUS SERVICES

4.11 OPERATIONAL CHARACTERISTICS

The status of public certificates is available from CRLs in the repositories and via an OCSP responder (where available).

4.12 SERVICE AVAILABILITY

99.99% minimum.

4.13 OPTIONAL FEATURES

No stipulation.

4.14 END OF SUBSCRIPTION

No stipulation.

4.15 KEY ESCROW AND RECOVERY

When data-encryption is supported, the Government-CA 2 must maintain a backup of the private decryption keys to support accessing data encrypted with an unavailable Key.

The Subscriber's Decryption Private Key can be recovered for the Subscriber or for a third party under following conditions:

- The Subscriber can request recovery at any time;
- An authorized individual belonging to the Subscriber organization (if the Subscriber has left the company or some other valid reason); and
- Compliance or Legal office can request recovery with consent of the NIC.

4.15.1 KEY ESCROW POLICY AND PRACTICES

The Government-CA 2 does not offer key escrow services to Subscribers.

4.15.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

No stipulation.

5. FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

5.1.1 SITE LOCATION AND CONSTRUCTION

The location and construction of the facility housing the Government-CA 2 and NIC-PKIC equipment shall consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors shall provide robust protection against unauthorized access to the CA equipment and records.

RA equipment shall be protected from unauthorized access by the DTSPs. The security mechanisms shall be commensurate with the level of threat in the CA environment.

5.1.2 PHYSICAL ACCESS

CA equipment shall always be protected from unauthorized access. The physical security mechanisms at a minimum shall be in place to:

- Permit no unauthorized access to the hardware;
- Store all removable media and paper containing sensitive plain-text information in secure containers;
- Monitor, either manually or electronically, for unauthorized intrusion at all times, and
- Maintain and periodically inspect an access log.

For any Government CA activity which requires opening the racks of the CA, a security guard shall be present to physically protect the CA from unauthorized physical access to the CA during the activity.

A security check of the facility housing the CAs equipment shall be undertaken on a regular basis. The facility shall never be left unattended.

5.1.3 POWER AND AIR CONDITIONING

The CA equipment shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Any of the CA on-line servers (e.g., CAs hosting directories) shall be provided with Uninterrupted Power sufficient for a minimum of six hours operation in the absence of commercial power, to support a smooth shutdown of the CA operations.

5.1.4 WATER EXPOSURE

The Government-CA 2 shall ensure that CA equipment is installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

5.1.5 FIRE PREVENTION AND PROTECTION

The CA equipment shall be housed in a facility with appropriate fire suppression and protection systems.

5.1.6 MEDIA STORAGE

Government-CA 2 shall ensure that CA media is stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive or backup information is duplicated and stored in a location separate from the CAs.

5.1.7 WASTE DISPOSAL

Sensitive media and documentation that are no longer needed for operations are destroyed using appropriate disposal processes.

5.1.8 OFF-SITE BACKUP

Full system backups of CAs, sufficient to recover from system failure, shall be made on a periodic schedule as described in NIC PKI Operations Policies and Procedures.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the Government-CA 2. The following are the trusted roles for Government-CA 2:

- CA Master
- CA Officer
- CA Administrator
- CA Operator
- CA Auditor

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

NIC shall ensure separation of duties for critical CA functions to prevent one person from maliciously using the PKI systems without detection. Each user's system access is limited to those actions for which they are required to perform in fulfilling their responsibilities. Separate individuals shall fill each of the roles specified in NIC PKI Trusted Roles document. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over the system operation.

A single person may be sufficient to perform tasks associated with a role, except for the activation of the CA certificate signing Private Key. Activation, backup, storage and recovery of the CA certificate signing Private Key shall require actions by at least two individuals.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

An individual shall identify and authenticate himself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 ROLES REQUIRING SEPARATION OF ROLES

Individual CA personnel are specifically designated to the five roles defined in section 5.2.1 of this CP and NIC PKI Trusted Roles document. The Government-CA 2 shall ensure that no individual will be assigned more than one Trusted Role.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE AND CLEARANCE REQUIREMENTS

All persons filling trusted roles are selected on the basis of skills, experience, loyalty, trustworthiness, and integrity. CA Master trusted roles must be held by citizens of the Kingdom of Saudi Arabia. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA are set forth in the NIC PKI Trusted Roles document and NIC PKI Organization Structure document. While performing any critical operation one of the trusted roles should be held by the Saudi citizen.

5.3.2 BACKGROUND CHECK AND CLEARANCE PROCEDURES

NIC shall conduct background investigations for all NIC personnel including trusted roles and management positions. Background check shall take into account the following:

- Availability of satisfactory character reference, i.e. one business and one personal;
- A check (for completeness and accuracy) of the applicant's CV;
- Confirmation of claimed academic and professional qualifications;
- Independent identity check (National ID card, Passport or similar document);
- Interviews with references shall be done as required; and
- More detailed checks, such as security clearance.

Security clearance shall be repeated every 3 years for personnel holding trusted roles.

5.3.3 TRAINING REQUIREMENTS

The Government-CA 2 shall ensure that all personnel receive appropriate training. Such training shall address relevant topics such as security requirements, operational responsibilities and associated procedures.

The RA Administrator(s) engaged in Certificate issuance shall be given detailed training to perform their tasks. Government-CA 2 shall design examination based on the training which is to be qualified by each RA Administrator.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

Individuals responsible for PKI roles shall be made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

The Government-CA 2 shall review and update its training program at least once a year to accommodate changes in the CA system.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

No stipulation.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

NIC shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions (i.e., not permitted by the CP, CPS and/or other procedures) involving the CA or its repository.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

Contractor personnel employed to perform functions pertaining to the CA shall be under adequate supervision and perform only assigned tasks. Contractor personnel shall be subject to the same sanctions as other personnel as set forth in Section 5.3.6, the relevant training and skills requirements from Section 5.3.3. and the event logging requirements of Section 5.4.1.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

Government-CA 2 shall make available to its personnel its CP, CPS, and any relevant documents required to perform their jobs.

5.4 AUDIT LOGGING PROCEDURES

Audit log files are generated for all events relating to the security of the Government-CA 2, and other associated components. The security audit logs for each auditable event defined in this section shall be maintained in accordance with onsite retention period and for archive.

5.4.1 TYPES OF EVENTS RECORDED

The Government-CA 2 PA shall ensure recording in audit log files all events relating to the security of the CA system hosted in NIC-PKIC. All security audit capabilities of the CA operating system and CA applications shall be enabled. Such events include, but are not limited to:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of certificate requests;
    e. Issuance of Certificates; and

f. Generation of Certificate Revocation Lists and OCSP entries.

3. Security events, including:
   a. Successful and unsuccessful PKI system access attempts;
   b. PKI and security system actions performed;
   c. Security profile changes;
   d. System crashes, hardware failures, and other anomalies;
   e. Firewall and router activities; and
   f. Entries to and exits from the CA facility.

Log entries MUST include the following elements:

- Date and time of entry;
- Identity of the person making the journal entry; and
- Description of the entry.

All logs, whether electronic or manual, must contain the date and time of the event and the identity of the Entity which caused the event. The CA shall also collect, either electronically or manually, security information not generated by the CA system such as:

- Physical access logs;
- System configuration changes and maintenance;
- CA personnel changes;
- documentation relating to certificate requests and the verification;
- documentation relating to certificate revocation;
- Discrepancy and No compromise reports;
- Information concerning the destruction of sensitive information;
- Current and past versions of all Certificate Policies;
- Current and past versions of Certification Practice Statements;
- Vulnerability Assessment Reports;
- Threat and Risk Assessment Reports;
- Compliance Inspection Reports; and
- Current and past versions of Agreements.

5.4.2 FREQUENCY OF PROCESSING DATA

Audit logs shall be processed in accordance with NIC PKI Audit and Compliance Policy.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

The Government-CA 2 shall retain all system generated (electronic) and manual audit records onsite for a period not less than six months from the date of creation.

5.4.4 PROTECTION OF AUDIT LOG

The Government-CA 2 shall protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction.

5.4.5 AUDIT LOG BACKUP PROCEDURES

Government-CA 2 shall back up all audit logs and audit summaries.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

The audit collection system is detailed in NIC PKI Audit and Compliance Policy.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

Event-causing subject are not notified.

5.4.8 VULNERABILITY ASSESSMENTS

Routine vulnerability assessments of security controls shall be performed by the Government-CA 2 for its CA, RA and other systems hosted in NIC-PKIC.

Government-CA 2 security program must include an annual Risk Assessment which includes identification of foreseeable internal and external threats, assess the likelihood and potential damage of these threats and assess the sufficiency of the policies, procedures, information systems and technology.

Based on the Risk Assessment exercise, the Government-CA 2 shall develop, implement, and maintain a security plan to control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF RECORDS ARCHIVED

CA archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA. The CA shall make these audit logs available to its Qualified Auditor upon request.

5.5.2 RETENTION PERIOD FOR ARCHIVE

The minimum retention periods for archive data shall be established in accordance with applicable regulatory guidance, laws, Agreements, and as specified by the Government-CA 2 PA. NIC’s minimum retention period for archive data is established at 10 years.

The Government-CA 2 shall ensure that DTSPs shall retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least ten years after any Certificate based on that documentation ceases to be valid.

5.5.3 PROTECTION OF ARCHIVE

Only authorized individuals shall be permitted to review the archive. The contents of the archive shall not be released except as determined by NIC, Government-CA 2 PA, or as required by law. Records and material information relevant to use of, and reliance on, a certificate shall be archived. Archive media shall be stored in a secure storage facility separate from the component itself. Any secondary site must provide adequate protection from environmental threats such as temperature, humidity and magnetism.

5.5.4 ARCHIVE BACKUP PROCEDURES

Only one copy of the archive is maintained. In other words, archive itself is not backed up.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Certificates, CRLs, and other revocation database entries shall contain time and date information. System logs shall be time stamped and systems use a dedicated time server to maintain synchronized time.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The type of Archive Collection System, whether internal or external, is specified in NIC PKI Archival Policy.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

As specified in NIC PKI Archival Policy.

5.6 KEY CHANGEOVER

The CA system utilized by the Government-CA 2 supports key rollover, allowing CA keys to be changed periodically as required to minimize risk to the integrity of the Government-CA 2. Once changed the new key shall be used for certificate signing purposes. The unexpired older keys are used to sign CRL's until all certificates signed by the unexpired older private key have expired.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

The Government-CA 2 shall have incident response and disaster recovery plans, and associated procedures meeting the requirements specified in Section 5.7.4.

If the Government-CA 2 detects a potential hacking attempt or other form of compromise to a CA, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Saudi National Root-CA Operations Policy section 12-13 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

Government-CA 2 maintains backup copies of hardware, system, databases, and private keys in order to rebuild the CA capability in case of software and/or data corruption.

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

Recovery procedure is as specified in Saudi National Root-CA Operations Policy section 14.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

A business continuity plan for the Government-CA 2 shall be designed to deal with any disruption to services and shall ensure managed, progressive recovery of components used to provide the services.

Critical PKI services at the primary site shall be established within 24 hours in the event of service non-availability. A geographically separate backup facility shall be established to provide full recovery of critical PKI services within five days following a disaster at the primary site.

5.8 CA OR RA TERMINATION

5.8.1 CA TERMINATION

No stipulation.

5.8.2 RA TERMINATION

If DTSP terminates operation for convenience, contract expiration, re-organization, or other non-security related reason, the Agreement between NIC and the DTSP shall set forth what actions are to be taken to ensure continued support for certificates previously issued by the Government-CA 2.

Upon termination of the RA Agreement, the RA certificate shall be revoked and the tasks performed by the RA must be handled by another RA or by the DTSP.

NIC will be the custodian of CA/RA archival records in case of termination.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

Key pair generation for CAs will be witnessed and attested to by a party separate from the CA operator or the CA administrator as mentioned in the NIC Level-One CA Key Generation Ceremony Policy.

Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. CA's shall use Hardware Security Modules (HSMs) for CA key generation and storage. HSM's should be minimum FIPS 140-2 Level 3 validated.

RA key pairs shall be generated in cryptographic modules at least compliant to FIPS 140-2 Level 2 or higher.

Subscriber key pairs are generated based on the Assurance Level. If subscriber key pairs are generated using cryptographic modules, then the cryptographic modules shall be at least compliant to FIPS 140-2 Level 2 or higher.

The Government-CA 2 may carry out central key generation service on behalf of the Subscriber. The Government-CA 2 will generate the keys in a trustworthy system and environment and ensure that the Private Key is not tampered with.

For Subscribers using a centralized signing platform, signing keys shall be generated using FIPS 140-2 Level 3 or higher certified hardware security module.

Government-CA 2 key pair generation is performed by multiple trusted personnel using trustworthy systems and processes that provide security and required cryptographic strength for the generated keys.

The Government-CA 2 key pair is generated in pre-planned Key Generation Ceremony in accordance with the requirements of NIC. The activities performed in Key Generation Ceremony are video recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by Government-CA 2 management.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

If key pairs are generated by the Subscriber, then delivery is not required, otherwise, the private keys shall be delivered to the Subscriber electronically using industry standard secure protocols. In case the Signing Private keys are generated by the CA or RA, then the CA or RA shall not retain any copy of the Signing Private Keys after delivery to the Subscriber. In addition, the Subscriber shall acknowledge receipt of the private key(s).

For Subscribers using centralized signing platform, Signing keys are generated using FIPS 140-2 Level 3 or higher certified hardware security module and stored in an encrypted database on the central storage. Key wrapping is accepted for the centralized signing platform subscribers. The signing keys are under the control of Subscriber and used through key activation data provided by Subscriber during every transaction.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Applicant public keys must be delivered for certificate issuance using industry standard secure protocol.

In respect of Server certificate, the Applicant's Public Key which will be generated by the Applicant must be transferred to Government-CA 2 using a method designed to ensure that:

- The Public Key is not changed during transit; and
- The sender possesses the Private Key that corresponds to the transferred Public Key.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The Government-CA 2 shall ensure that its Subscribers and Relying Parties receive and maintain the trust anchor in a trustworthy fashion. Methods for trust anchor delivery may include:

- A trusted role loading the trust anchor onto Tokens delivered to Subscribers via secure mechanisms;
- Distribution of trust anchor through secure out-of-band mechanisms;
- Calculation and comparison of trust anchor hash or fingerprint against the hash made available via authenticated out-of-band sources; or
- Downloading trust anchor from web sites secured with a currently valid certificate of equal or greater assurance level than the Certificate being downloaded and the site trust anchor already on the Subscriber system via secure means.

6.1.5 KEY SIZES

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. Key sizes are described as below for Government-CA 2. All FIPS-approved signature algorithms shall be considered acceptable. If NIC determines that the security of a particular algorithm may be compromised, it shall direct the CA to revoke the affected certificates.

All certificates issued shall use at least 2048 bit RSA, with Secure Hash Algorithm version (SHA-256) in accordance with FIPS 186-2 or equivalent.

TLS or another protocol providing similar security to accomplish any of the requirements of this CP shall use triple-DES or AES (minimum 128 bit key strength) for symmetric keys, and at least 2048 bit RSA or equivalent for asymmetric keys.

The current Government-CA 2 key lengths as per NIC standard for minimum key sizes are;

- Government-CA 2 Key Pair: 2048 bits
- Subscriber Key Pairs: 2048 bits
- OCSP Key Pair: 2048 bits

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The HSM pseudo-random number generator is validated by NIST. Public key parameters prescribed are generated in accordance with industry best practices.

6.1.7 KEY USAGE PURPOSES

Public keys that are bound into certificates shall be certified for use in authenticating, signing or encrypting, as specified by the Government-CA 2. The use of a specific key is determined by the key usage extension in the X.509 certificate. Government-CA 2 key is used for certificate and CRL signing.

6.2 PRIVATE KEY PROTECTION AND CRYPTO-MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

Cryptographic modules employed in NIC shall comply with FIPS-PUB 140-2 “Security Requirements for Cryptographic Modules”, or its successors.

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

The use of any CA Private signing keys shall require action by multiple persons. Government-CA 2 keys can only be accessed on the physical and logical level by adhering to multi persons control.

6.2.3 PRIVATE KEY ESCROW

CA Private Keys shall never be escrowed. The Government CA 2 does not escrow end-user Subscriber private keys with any third party.

6.2.4 PRIVATE KEY BACKUP

6.2.4.1 Backup of CA Signing Private Key

Government-CA 2 signing Private Key shall be backed up under the same multi-person control as the original Signing Key. A second copy may be kept at the CA backup location identified as business continuity location. A third copy may be kept at the CA backup location identified as disaster recovery location. Procedures for Government-CA 2 signing Private Key backup shall be detailed in NIC Level-One CA Backup and Restore Policy.

Government -CA private keys that are physically transported from one facility to another shall remain confidential and maintain their integrity.

Government-CA 2 hardware containing CA private keys, and associated activation materials, shall be transported in a physically secure environment by authorized personnel in trusted roles, using multiple person controls, and using sealed tamper evident packaging.

Government-CA 2 keys and associated activation materials shall be transported in a manner that prevents the key from being activated or accessed during the transportation event; and CA key transportation events shall be logged.

6.2.4.2 Backup of Subscriber Private Keys

Subscriber’s Decryption Keys shall be backed up. Except for the centralized signing platform Subscribers, signing Private Keys and authentication Private keys shall not be backed up.

6.2.5 PRIVATE KEY ARCHIVAL

The Government-CA 2 shall provide the capability to archive private decryption keys to provide authorized access to encrypted information. A complete history of all decryption private keys and certificates issued must be maintained.

The Government-CA 2 shall maintain controls to provide reasonable assurance that archived CA keys remain confidential, secured, and shall never be put back into production.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

The cryptographic modules implemented by NIC shall be validated to FIPS 140-2 Level 3, or its successors, ensuring that the CA keys cannot be exported to less secure media.

The Government-CA 2 keys can be cloned for secure backup from the master hardware cryptographic module to other hardware cryptographic module(s) using secure mechanisms so that they can be recovered if a major catastrophe destroys the productive set of keys.

RA, LRA and Subscriber private keys shall not be transferred from the module they are generated in.

The Government-CA 2 keys migrated from one secure cryptographic device to another, other than for the purposes of routine backup and restoration shall be completed in a physically secure environment by those in Trusted Roles under multi-person control.

The hardware and software tools used during any Government-CA 2 key migration process shall be tested by the CA prior to the migration event. Government-CA 2 key migration events shall follow a documented script and be logged.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

CA's Private Key shall be stored on FIPS 140-2 Level 3 validated cryptographic module in encrypted form.

Subscriber/RAs private keys shall be stored in cryptographic modules validated to FIPS 140-2 level 2 or higher.

6.2.8 METHOD OF ACTIVATING PRIVATE KEYS

A CA's private key shall be activated by the main stakeholders and authorized personnel, as defined in NIC Level-One CA Operations Policy section 5, supplying their activation data. Such activation data shall be held on secure media and shall require the successful completion of a multi-person authentication process.

Subscribers must be authenticated to the cryptographic module before the activation of any private key (s). Acceptable means of authentication includes but is not limited to passwords and PINs. Entry of activation data shall be protected from disclosure.

6.2.9 METHODS OF DEACTIVATING PRIVATE KEYS

A CA's private key shall be deactivated by the main stakeholders and authorized personnel following use, as defined in NIC Level-One CA Operations Policy section 6 by removing their secure media and storing it in a secure container or environment when not in use.

If a cryptographic token is used to generate and securely store Subscriber private keys, the deactivation can be achieved through manual logout procedure, or automatically after a period of inactivity as configured.

6.2.10 METHODS OF DESTROYING PRIVATE KEYS

Copies of Government-CA 2 keys that no longer serve a valid business purposes or copies of CA keys that are at the end of the key pair life cycle shall be destroyed as per NIC Cryptographic Devices Lifecycle Management Policy and Procedure.

The Government CA 2 makes no expiry for end entity decryption key, thus doesn't destroy it. In addition, the means of destroying subscriber's private key are not defined as currently there's no business need for it.

6.2.11 CRYPTOGRAPHIC MODULE RATING

As described in section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVE

The Public Key is archived as part of the certificate archive process.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY USAGE PERIODS

The table below details key usage, length and certificate lifetime for the corresponding keys:

Key/Certificate	Key Length in Bits	Maximum Validity Period
Government CA 2 signing key and certificate	2048	120 months or valid not beyond 2030, whichever is earlier.
End Entity signing, sealing, and non-repudiation key and Certificate	2048	Up to 36 months
End Entity Encryption Certificate	2048	Up to 36 months
End Entity Decryption Key	2048	No Expiry

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Activation data may be user selected.

6.4.2 ACTIVATION DATA PROTECTION

If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

The computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards.

At a minimum NIC-PKIC shall have following controls to ensure security of the systems:

- Hardened operating system;
- Software packages are only installed from a trusted software repository;
- Minimal network connectivity;
- Authentication and authorization for all functions;
- Strong authentication and role-based access control for all vital functions;
- Disk and file encryption for all relevant data; and
- Proactive patch management.

6.5.2 COMPUTER SECURITY RATING

The CA software shall be certified under the Common Criteria or ITSEC to a level equivalent to Common Criteria EAL 4.

6.6 LIFE-CYCLE TECHNICAL CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

The Government-CA 2 shall maintain controls to provide reasonable assurance that CA systems development, maintenance activities, patching, and changes to CA systems shall be documented, tested, authorized, and properly implemented to maintain CA system integrity.

The Government-CA 2 design, installation, and operation shall be documented by qualified personnel. NIC PKI operations personnel, with oversight by the Government-CA 2 PA, will develop and produce appropriate qualification documentation establishing that Government-CA 2 components are properly installed and configured, and operate in accordance with the technical specifications.

6.6.2 SECURITY MANAGEMENT CONTROLS

The Government-CA 2 shall maintain controls to provide reasonable assurance that changes to CA systems operating systems, databases, applications, network devices, and hardware

shall be documented, tested, authorized, and properly implemented to maintain CA system integrity.

The configuration of the Government-CA 2 systems as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to software or configuration. A formal configuration management methodology shall be used for installation and on-going maintenance of the system.

6.6.3 LIFE CYCLE SECURITY CONTROLS

The Government-CA 2 shall employ:

- appropriate security measures to ensure they are guarded against denial of service and intrusion attacks.
- network security and firewall management, including port restrictions and IP address filtering.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

6.7 NETWORK SECURITY CONTROLS

The Government-CA 2 shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Also it shall employ network security and firewall management, including port restrictions and IP address filtering.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

6.8 TIME STAMPING

Time stamping shall be supported for the Certificates, CRLs, and other revocation database entries containing time and date information.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

This section contains the rules and guidelines followed by this CA in populating X.509 certificates and CRL extensions.

7.1.1 VERSION NUMBERS

The Government-CA 2 shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 CERTIFICATE EXTENSIONS

NIC critical private extensions shall be interoperable in their intended community of use. Subordinate and Subscriber certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

Government-CA 2 shall sign Certificates using:

sha256WithRSAEncryption algorithm (1.2.840.113549.1.1.11).

The algorithm identifier of the subject Public Key shall be:

rsaEncryption (OID: = 1.2.840.113549.1.1.1).

7.1.4 NAME FORMS

Certificates issued by Government-CA 2 contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names are in the form of an X.501 printable string.

7.1.5 NAME CONSTRAINTS

No Stipulation.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

Subscriber Certificates issued under this CP shall assert a certificate policy OID.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

It is expected that all members of the Government-CA 2 apply to this policy.

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

No stipulation.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION

Processing semantics for the critical certificate policy extension shall conform to X.509 certification path processing rules.

7.2 CRL PROFILE

The Government-CA 2 combined CRL Profile is as below:

Field	Content	Comment
Version	2	
Algorithm	SHA256withRSA	
Issuer	CN=Government CA 2 O=National Center for Digital Certification C=SA	
This update	*<issue date>*	
Next update	*<issue date + 24 hours>*	
AuthorityKeyIdentifier	20 byte SHA-1 hash of the signing CA's public key	Critical = FALSE
CRL number	<sequential number starting at 1>	Critical = FALSE
Revocation Reason		Critical = FALSE

The Government-CA 2 partitioned CRL Profile is as below:

Field	Content	Comment
Version	2	
Algorithm	SHA256withRSA	
Issuer	CN=Government CA 2 O=National Center for Digital Certification C=SA	
This update	*<issue date>*	
Next update	*<issue date + 24 hours>*	
AuthorityKeyIdentifier	20 byte SHA-1 hash of the signing CA's public key	Critical = FALSE
CRL number	<sequential number starting at 1>	Critical = FALSE

Issuing Distribution Point	URL=http://web.ncdc.gov.sa/gca2/crl/gca2part<n>.crl onlyContainsUserCerts = Yes onlyContainsCACerts= No indirectCRL= No	Critical =TRUE
Revocation Reason		Critical = FALSE

7.2.1 VERSION NUMBERS

The Government-CA 2 shall issue X.509 version two (v2) CRLs (populate version field with integer "1").

7.2.2 CRL AND CRL ENTRY EXTENSIONS

Critical private extensions shall be interoperable in their intended community of use.

7.3 OCSP PROFILE

OCSP requests and responses shall be in accordance with RFC 6960.

7.3.1 VERSION NUMBER(S)

The version number for request and responses shall be v1.

7.3.2 OCSP EXTENSIONS

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The Government-CA 2 PA shall be responsible for overseeing compliance of the Government-CA 2, DTSPs, the Government-CA 2 CP and CPS. NIC-PKIC and the Government-CA 2 PA shall ensure that the requirements of the Government-CA 2 CP and CPS and the provisions of applicable Agreements with NIC are implemented and enforced.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENTS

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. NIC shall also perform internal audit on at least a quarterly basis against a randomly selected sample for monitor adherence and service quality. Moreover, NIC may require ad-hoc compliance audits of any DTSP's operation to validate that it is operating in accordance with the applicable CP, PDS, CPS, Audit 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/or 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.

8.2 IDENTITY / QUALIFICATIONS OF ASSESSOR

The audit under Saudi National PKI shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme; and
- Bound by law, government regulation, or professional code of ethics.

NIC shall appoint Qualified Auditor who shall be Licensed WebTrust Practitioner to perform such compliance audits as a primary responsibility.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

To provide an unbiased and independent evaluation, the auditor and audited party shall not have any current or planned financial, legal or other relationship that could result in a conflict of interest.

8.4 TOPICS COVERED BY ASSESSMENT

The compliance audits shall verify whether the CA PKI operations environment is in compliance with the applicable CP, CPS and supporting operational policies and procedures. The term CA PKI Operations environment defines the total environment and includes:

- All documentation, records;
- Contracts/agreements;
- Compliance with applicable Law;
- Physical and logical controls;
- Personnel and approved roles/tasks;
- Hardware (e.g. servers, desktops, hardware security modules, network devices and security devices); and
- Software and information.

The auditor shall provide the Government-CA 2 PA and/or NIC with a compliance report highlighting any discrepancies.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If irregularities are found by the auditor, the audited party shall be informed in writing of the findings. The audited party must submit a report to the auditor or directly to NIC or Government-CA 2 PA, as determined by NIC, as to any remedial action the audited party will take in response to the identified deficiencies. This report shall include a time for completion to be approved by the auditor, or by NIC as appropriate.

Where an audited party fails to take remedial action in response to the identified deficiencies, NIC shall be informed by the auditor and shall take the appropriate action, according to the severity of the deficiencies.

8.6 COMMUNICATION OF RESULTS

An Audit Compliance Report, including identification of corrective measures taken or being taken by the audited party, shall be provided to the Government-CA 2 PA and/or NIC as applicable.

The Government-CA 2 shall make the Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, an explanatory letter is to be signed by the Qualified Auditor.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

Currently, no fees are charged by Government-CA 2 for Certificate issuance and renew, although Government-CA 2 PA reserves the right to change this in the future. In addition, a Government DTSP may charge fees for its services.

9.1.2 CERTIFICATE ACCESS FEES

The Government-CA 2 may not charge for access to any certificates.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEE

No fee is charged for Digital Certificate revocation or status information access.

9.1.4 FEES FOR OTHER SERVICES

The Government-CA 2 may charge for other services depending on business needs and subject to NIC approval.

9.1.5 REFUND POLICY

Refunds are not possible for the Digital Certificates for which no fees are charged.

9.2 FINANCIAL RESPONSIBILITY

The Government-CA 2 disclaims all liability implicit or explicit due to the use of any certificates issued by the Government-CA 2 which certify public keys of subscribers.

9.2.1 INSURANCE COVERAGE

The Government-CA 2 acts within the bounds of laws in Saudi Arabia, under the administration of NIC.

9.2.2 OTHER ASSETS

Governmental-CA shall have sufficient financial resources to maintain their operations and perform their duties.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

As specified in the relevant agreements.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Information pertaining to the CA and not requiring protection may be made publicly available at the discretion of NIC or Government-CA 2 PA. Specific confidentiality requirements for business information are defined in the NIC PKI Privacy Policy and the applicable Agreements.

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

Any corporate or personal information held by NIC, Government-CA 2, or DTSPs related to the application and issuance of Certificates shall be considered confidential.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

Such information as specified by the Government-CA 2 PA, NIC PKI Privacy Policy, NIC Document Control Policy, NIC PKI Operations Policies and procedures and applicable Agreements.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

All Saudi National PKI participants shall be responsible for protecting the confidential information they possess in accordance with NIC PKI Privacy Policy and applicable laws and Agreements.

9.4 PRIVACY OF PERSONAL INFORMATION

Any personal identifying information collected by a Government DTSPs shall be protected in accordance with the NIC PKI Privacy Policy. The DTSPs shall use reasonable measures to protect personal identifying information from disclosure to any third party.

9.4.1 PRIVACY PLAN

All Subscribers identifying information as defined by the NIC PKI Privacy Policy shall be protected from unauthorized disclosure.

9.4.2 INFORMATION TREATED AS PRIVATE

Any information about Subscribers that is not publicly available through the content of the issued certificate, repository and online CRL's shall be treated as private.

9.4.3 INFORMATION NOT DEEMED PRIVATE

Information appearing in Subscriber Certificates such as the name, organization affiliation and pubic key shall not be deemed private. NIC PKI Privacy Policy identifies the personally identifiable information that can be collected to enable issuance of a certificate.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

Access to Government-CA 2 held private information shall be restricted to those with an official need-to-know basis in order to perform their official duties.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

Requirements for notice and consent to use private information shall be defined in the respective Agreements and NIC PKI Privacy Policy.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

Any disclosure shall be handled in accordance with NIC PKI Privacy Policy.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Any disclosure shall be handled in accordance with NIC PKI Privacy Policy.

9.5 INTELLECTUAL PROPERTY RIGHTS

The Government-CA 2 PA retains exclusive rights to any products or information developed under or pursuant to this CP.

9.6 CA REPRESENTATIONS AND WARRANTIES

9.6.1 GOVERNMENT-CA 2'S REPRESENTATIONS AND WARRANTIES

The Government-CA 2 provides representations and warranties in accordance with this CP, respective agreements and applicable laws and regulations as below:

- Providing the operational infrastructure and certification services;
- Making reasonable efforts to ensure it conducts an efficient and trustworthy operation. "Reasonable efforts" include but are not limited to operating in compliance with:
    - Documented CP, PDS and CPS;
    - Documented NIC PKI Operations Policies and Procedures; and
    - Within applicable agreements, Saudi Law and regulations.
- Maintaining 24 x 7 publicly-accessible repositories with current information and replicates Government-CA 2 issued certificates and CRLs;
- For the 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 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;
- 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;
- Use its private signing key only to sign certificates and CRLs and for no other purpose;
- Perform authentication and identification procedures in accordance with applicable Agreement and NIC PKI Operations Policies and Procedures;

- Provide certificate and key management services in accordance with the CP and CPS; and
- Ensure that CA personnel use private keys issued for the purpose of conducting CA duties only for such purposes.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

RA's discharge their obligations in accordance with the practices outlined in overview of this CP, the Government-CA 2 CPS and the RA Agreement.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

Subscribers are Government employees, entities, non-human subscribers (like Servers and Network Devices) within the Government domain to which certificates are issued.

It is the responsibility of the Subscriber to:

1. Subscriber is obligated 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 and verify the Certificate contents for accuracy;
   - Secure private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key;
   - Use Subscriber Certificate only for its intended uses as specified by the DTSPs;
   - Notify the DTSP in the event of any information in the Certificate is, or becomes, incorrect or inaccurate;
   - Notify the DTSP in the event of a key compromise immediately whenever the Subscriber has reason to believe that the Subscriber's private key has been lost, accessed by another individual, or compromised in any other manner;
   - Use the Subscriber Certificate that does not violate applicable laws in the Kingdom of Saudi Arabia; and
   - Upon termination of Subscriber Agreement, revocation or expiration of the Subscriber Certificate, immediately cease use of Private Key corresponding to the Public Key included in the Subscriber Certificate.
2. Subscriber agrees that any use of the Subscriber Certificate to sign or otherwise approve the contents of any electronic record or message is attributable to Subscriber. Subscriber agrees to be legally bound by the contents of any such electronic record or message.
3. Subscriber shall indemnify and hold a DTSP harmless from and against any and all damages (including legal fees), losses, lawsuits, claims or actions arising out of:
   - Use of Subscriber's Certificate in a manner not authorized by the DTSP or otherwise inconsistent with the terms of this Subscriber Agreement or the Government-CA 2 CP and PDS;
   - A Subscriber Certificate being tampered with by the Subscriber; or

- Inaccuracies or misrepresentations contained within the Application. A Subscriber shall indemnify and hold the DTSP harmless against any damages and legal fees that arise out of lawsuits, claims or actions by third parties who rely on or otherwise use Subscriber's Certificate, where such lawsuit, claim, or action relates to a Subscriber's breach of its obligations outlined in this Subscriber Agreement or the Government-CA 2 CP and PDS, a Subscriber's use of or reliance upon a Subscriber Certificate in connection with its business operations, a Subscriber's failure to protect its private key, or claims pertaining to content or other information or data supplied, or required to be supplied, by Subscriber.

9.6.4 RELYING PARTIES REPRESENTATIONS AND WARRANTIES

Relying Parties who rely upon the certificates issued under Saudi National PKI shall:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Verify the Validity by ensuring that the Certificate has not expired;
- Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 amendment;
- 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
- Determining that such Certificate provides adequate assurances for its intended use.

9.6.5 REPRESENTATION AND WARRANTIES OF OTHER PARTIES

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

NIC, through its associated components, seeks to provide digital certification services according to international standards and best practices, using the most secure physical and electronic installations.

The Government-CA 2 provides no warranty, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of the Government-CA 2 or for the legal validity, acceptance or any other type of recognition of its own certificates, those issued by it through other Subordinate entity, any digital signature backed by such certificates, and any products provided by NIC. The Government-CA 2 further disclaims any warranty of merchantability or fitness for a particular purpose of the above-mentioned certificates, digital signatures and products.

9.8 LIMITATIONS OF LIABILITY

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.

9.9 INDEMNITIES

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, the CA SHALL defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

The DTSPs shall indemnify, defend and hold harmless the following parties:

- NIC, its CA PA, officers, employees, agents, consultants, and subsidiaries from any and all claims, damages, costs (including, without limitation, attorney's fees), judgments, awards or liability;
- The DTSP's own employees, arising from any of the DTSP's operations and activities as a DTSP , of any entity or services subordinated or outsourced by the DTSP; and
- Any parties relying on the DTSP's Certificates, or arising as a result of an infringement or violation of any patents, copyrights, trade secrets, licenses, or other property rights of any third party.

9.10 TERM AND TERMINATION

9.10.1 TERM

This CP shall be effective upon approval by NIC. Once the CP becomes effective it is published in the repository. Amendments to this CP upon approval become effective and replace the older version in the repository.

9.10.2 TERMINATION

This CP as amended from time to time shall remain in force until it is replaced by a new version. The latest version of the Government-CA 2 CP can be found at: https://ca.nic.gov.sa.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this CP, all Government-CA 2 participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

All communication between NIC, PA, Saudi National Root-CA, DTSPs, RAs and LRAs shall be in writing or via digitally signed communication. If in writing, the communication shall be signed on the appropriate organization letterhead. If electronically, a Digital Signature shall be made using a Private Key whose companion Public Key is certified using a Certificate meeting this CP Certificate assurance level.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

The Government-CA 2 PA shall review this CP at least once per year. Errors, updates, or suggested changes to this CP shall be communicated to the Government-CA 2 PA and/or NIC. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change. Any technical changes in the Government-CA 2 shall be managed as per the NIC PKI Change Management Policy.

Subject to the approval of NIC, the Government-CA 2 PA reserves the right to change this CP from time to time. The Government-CA 2 PA will incorporate any such change into a new version of this CP and, upon approval, publish the new version. The new CP will carry a new version number.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

This CP and any subsequent changes shall be made available to the Government-CA 2 participants within two weeks of approval. The Government-CA 2 PA reserves the right to amend this CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URL's, and changes to contact information. All the Saudi PKI participants and other parties designated by the Government-CA 2 PA shall provide their comments to the Government-CA 2 PA in accordance with NIC rules. The Government-CA 2 PA's decision to designate amendments as material or non-material shall be at the PA's sole discretion.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

The policy OID shall only change if the change in the CP results in a material change to the trust by the relying parties, as determined by the Government-CA 2 PA and shall only change pursuant to a decision from NIC.

9.13 DISPUTE RESOLUTION PROCEDURES

The use of certificates issued by the Government-CA 2 is governed by contracts, agreements, and standards set forth by NIC. Those contracts, agreements and standards include dispute resolution policy and procedures that shall be employed in any dispute arising from the issuance or use of a certificate governed by this CP. Dispute Resolution mechanism is described in NIC PKI Dispute Resolution Policy.

9.14 GOVERNING LAW

This CP is governed by the laws of the Kingdom of Saudi Arabia.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP is subject to applicable national, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

No stipulation.

9.16.2 ASSIGNMENT

Except where specified by other contracts, no party may assign or delegate this CP or any of its rights or duties under this CP, without the prior written consent of the Government-CA 2 PA.

9.16.3 SEVERABILITY

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4 ENFORCEMENT (ATTORNEY FEES AND WAIVER OF RIGHTS)

This document shall be treated according to laws of Kingdom of Saudi Arabia. Legal disputes arising from the operation of the Government-CA 2 will be treated according to laws of Kingdom of Saudi Arabia.

9.16.5 FORCE MAJEURE

The Government-CA 2 shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and reasons beyond provisions of the governing law.

9.17 OTHER PROVISIONS

9.17.1 FIDUCIARY RELATIONSHIPS

Nothing contained in this CP shall be deemed to constitute either the Government-CA 2, or any of its subcontractors, agents, officers, suppliers, employees, partners, principals, or CA PA to be a partner, Affiliate, trustee, of any Relying Party or any third party, or to create any fiduciary relationship between the Government-CA 2 and any Relying party, or any third party, for any purpose whatsoever.

Nothing in this CP or any Agreement between a third party and a Relying Party shall confer on any Subscriber, Customer, Relying Party, Registration Authority, Applicant or any third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of the Government-CA 2.

9.17.2 ADMINISTRATIVE PROCESSES

As specified in NIC PKI Operations Policies and applicable Agreements.

APPENDIX- A: CERTIFICATE TYPES

This section details different certificate types issued under the Government CA 2 and their respective policies and certificate profiles.

For issuance of a particular certificate type, DTSP shall submit request to NIC. Based on NIC approval, a DTSP is authorized to issue particular certificate type. It is mandatory to comply with all requirements applicable to the respective certificate type, as well as, any additional restrictions or conditions communicated to the DTSP by NIC.

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.

1. NAME ID (MANAGED)

The Name ID is a digital ID issued to a person's name, which is a combination of three key-pairs, namely Signing, Authentication and Encryption.

1.1 NAME SIGNING (NON-REPUDIATION) CERTIFICATE

1.1.1 NAME SIGNING (NON-REPUDIATION) CERTIFICATE POLICY

S. No.	Attribute	Name Signing (Non-Repudiation) Certificate
1	Policy Name	Name Signing (Non-Repudiation) Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.3.1.2.1.1.1.1
3	Subject	"cn=<English-Firstname> <English-Secondname> <English-Thirdname> <English-Lastname> <Arabic-Lastname> <Arabic-Thirdname> <Arabic-SecondName> <Arabic-FirstName> *, OU=<optional searchbase(s)>, O = National Center for Digital Certification, C = SA" * Optional unverified nickname may be added at the end of the CN to achieve uniqueness of the subject.
4	Certificate Profile	See below after the table.
5	Application Usage	**If subscriber wants to engage in legal signing he/she is advised to use Name Signing certificates/keys only. Digital Signatures made using this certificate type should be considered compliant to chapter four of the Saudi e-Transactions Law (Royal Decree No. (M/8), and thus considered valid in the court of law.** Every Participant acknowledges and agrees, to the extent permitted by applicable law, that where a transaction is required to be in writing, a message or other record bearing a digital signature verifiable with reference to an Government- CA 2 issued Name Signing Certificate is valid, effective, and enforceable to an extent no less than had the same message or record been written and signed on paper. Government-CA 2 issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA 2 issued Name Certificate should honour Key Usage. Following are some of the common usage of the certificate • Inter Government correspondence; • Public Information Posting by Authorized Government Personnel; • Departmental Forms Submission; • PKI enabled Application work-flow; and • E Tendering The Name 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 as per the Government- CA 2 practices, Subscribers agreement and not otherwise prohibited by the law of Saudi Arabia.
6	Verification Process	**1.** Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents. **2.** The following will be considered valid identity documents: **3.** National ID / passport for citizens. **4.** Residence permit / passport for residents.

S. No.	Attribute	Name Signing (Non-Repudiation) Certificate
		5. Letter from an authorized party (as prescribed by the DTSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process **6.** The domain name for the email address requested on the certificate should be verified to be owned by the issuing DTSP organization. **7.** If the name ID certificate need to have the subscriber Email added on the SAN then Email address shall be verified. In order to verify the email the RAs will send an email for certificate issuance confirmation have authorization code and the subscriber shall confirm his/her email by responding to the email or provide copy of the mail. **8.** During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics. Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types.
7	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys, subscriber shall use Hardware Security device like smart card / tokens for key generation and storage. **All Name ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA 2 CP.** The Name Signing Private keys must be generated and stored on FIPS 140-2 Level 2 or higher certified hardware token or smart card, and the RA shall not retain any copy of the subscriber Private Keys. In addition, the Subscriber shall acknowledge receipt of the private key(s).
8	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber will be present at the RA for face-to-face identity verification • The RA will validate the documents submitted by the subscriber • The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner. • The subscriber will go to the RA customization center • The Subscriber will plug his smart card / USB token into the customization device. • The Subscriber will enter the PIN of the smart card / USB token • The Subscriber will enter reference number and an authorization code to generate keys and download certificates. • The Client Software will generate the Subscriber's keys securely on his smart card / USB token. • The CA will authenticate the Subscriber using the reference number and authorization code and receive the certificate signing request using a secure protocol such as PKIX-CMP. Upon successful authentication, the CA shall create the Subscribers certificates and transport them securely onto the Subscriber's smart cards / USB tokens.

S. No.	Attribute	Name Signing (Non-Repudiation) Certificate
9	Key Usage	Name Signing certificate and keys can be used for data integrity, and non-repudiation based on name only.
10	Private Key Protection	Subscribers shall protect their private keys in a FIPS 140-2 Level 2 or higher certified smart card or other hardware token/module. Subscriber is obligated to secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key. Generation and/or Storage of name signing private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.
11	Certificate Life Time	36 months
12	Key Backup	The DTSP or CA shall not take any backup of the private keys of this certificate type.
13	Asymmetric Key Length	Minimum 2048 bits RSA
14	Certificate Re-key	Certificate re-key shall take place after a certificate is revoked and the subscriber information is still accountable or if a certificate has expired or is nearing expiry. In case of certificate's revocation and/or after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall be required to physically attend to the RA for identity validation and submission of supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed automatically by a supported client without revocation of the existing certificate. The certificate re-key can be done transparently when the subscriber logs in to the client software using his Digital ID.
15	Assurance Level	High

1.1.2 NAME SIGNING (NON-REPUDIATION) CERTIFICATE PROFILE

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = <English FirstName> <English SecondName> <English ThirdName> <English LastName> <Arabic LastName> <Arabic ThirdName> <Arabic SecondName> <Arabic FirstName> * OU= <optional searchbase(s)> C = SA (Encoding should be in UTF8 only) * Optional unverified nickname may be added at the end of the CN to achieve uniqueness of the subject.	V1 Field
Serial Number	Unique serial number generated by the CMS	NO

Field / x.509 extension	Value or Value Constant	Critical
Subject Alternative Name	RFC822 Name=<end-entity's verified email address> (should be verified to be the same as written in the subject) Note: Subject Alternative Names other than the RFC822 Name (email address) are not permitted to be included here.	NO
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/gca2/crl/gca2part<n>.crl Directory Address=(DN of the CRL entry in LDAP) [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/gca2/crl/gca2comb.crl	NO
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Government CA 2 (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.2.1.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa/gca2/policies [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA 2 Certification Policy and associated documentation available at http://web.ncdc.gov.sa/gca2/policies is hereby	NO

Field / x.509 extension	Value or Value Constant	Critical
	incorporated into your use or reliance on this Certificate.	
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ncdc.gov.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://web.ncdc.gov.sa/certs/gca2.crt	NO
Key Usage	NonRepudiation DigitalSignature	NO
Extended Key Usage	emailProtection (1.3.6.1.5.5.7.3.4)	NO

1.2 NAME AUTHENTICATION CERTIFICATE

1.2.1 NAME AUTHENTICATION CERTIFICATE POLICY

S. No.	Attribute	Name Authentication Certificate
1	Policy Name	Name Authentication Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.3.1.2.1.1.1.2
3	Subject	"cn=<English-Firstname> <English-Secondname> <English-Thirdname> <English-Lastname> <Arabic-Lastname> <Arabic-Thirdname> <Arabic-SecondName> <Arabic-FirstName> *, OU=<optional searchbase(s)>, C = SA" * Optional unverified nickname may be added at the end of the CN to achieve uniqueness of the subject.
4	Certificate Profile	See below after the table.
5	Application Usage	Government- CA 2 issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA 2 issued Name Certificate should honour Key Usage. The Name Authentication certificate should be used for client authentication and may also be used to verify data integrity. For Legal-Signing, it is required to use the Name Signing Certificate. Following are some of the common usage of the certificate • Inter Government correspondence; • Public Information Posting by Authorized Government Personnel; • Departmental Forms Submission; • PKI enabled Application work-flow; and • E Tendering The Name certificate may also be used for other general or specific Government purposes which are not covered explicitly above, provided that a

S. No.	Attribute	Name Authentication Certificate
		Relying Party is able to reasonably rely on that certificate and the usage is as per the Government- CA 2 practices, Subscribers agreement and not otherwise prohibited by law of Saudi Arabia.
6	Verification Process	**1.** Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents. **2.** The following will be considered valid identity documents: **3.** National ID / passport for citizens. **4.** Residence permit / passport for residents. **5.** Letter from an authorized party (as prescribed by the DTSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process **6.** The domain name for the email address requested on the certificate should be verified to be owned by the issuing DTSP organization. **7.** If the name ID certificate need to have the subscriber Email added on the SAN then Email address shall be verified. In order to verify the email the RAs will send an email for certificate issuance confirmation have authorization code and the subscriber shall confirm his/her email by responding to the email or provide copy of the mail. **8.** During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types.
7	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys, subscriber shall use Hardware Security device like smart card / tokens for key generation and storage. **All Name ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA 2 CP.** The Name Authentication Private keys must be generated and stored on FIPS 140-2 Level 2 or higher certified hardware token or smart card, and the RA shall not retain any copy of the subscriber Private Keys. In addition, the Subscriber shall acknowledge receipt of the private key(s).
8	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber will be present at the RA for face-to-face identity verification • The RA will validate the documents submitted by the subscriber • The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner. • The subscriber will go to the RA customization center • The Subscriber will plug his smart card / USB token into the customization device. • The Subscriber will enter the PIN of the smart card / USB token • The Subscriber will enter reference number and an authorization code to generate keys and download certificates.

S. No.	Attribute	Name Authentication Certificate
		• The Client Software will generate the Subscriber's keys securely on his smart card / USB token. • The CA will authenticate the Subscriber using the reference number and authorization code and receive the certificate signing request using a secure protocol such as PKIX-CMP. Upon successful authentication, the CA shall create the Subscribers certificates and transport them securely onto the Subscriber's smart cards / USB tokens.
9	Key Usage	Name Authentication certificate and keys shall be used for authentication of/by name only.
10	Private Key Protection	Subscribers shall protect their private keys in a FIPS 140-2 Level 2 or higher certified smart card or other hardware token/module. Subscriber is obligated to secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key. Generation and/or Storage of name authentication private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.
11	Certificate Life Time	36 months
12	Key Backup	The DTSP or CA shall not take any backup of the private keys of this certificate type.
13	Asymmetric Key Length	Minimum 2048 bits RSA
14	Certificate Re-key	Certificate re-key shall take place after a certificate is revoked and the subscriber information is still accountable or if a certificate has expired or is nearing expiry. In case of certificate's revocation and/or after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall be required to physically attend to the RA for identity validation and submission of supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed automatically by a supported client without revocation of the existing certificate. The certificate re-key can be done transparently when the subscriber logs in to the client software using his Digital ID.
15	Assurance Level	High

1.2.2 NAME AUTHENTICATION CERTIFICATE PROFILE

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = <English FirstName> <English SecondName> <English ThirdName> <English LastName> <Arabic LastName> <Arabic ThirdName> <Arabic SecondName> <Arabic FirstName> *	V1 Field

Field / x.509 extension	Value or Value Constant	Critical
	OU=<optional searchbase(s)> C = SA (Encoding should be in UTF8 only) * Optional unverified nickname may be added at the end of the CN to achieve uniqueness of the subject.	
Serial Number	Unique serial number generated by the CMS	NO
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/gca2/crl/gca2part<n>.crl Directory Address=(DN of the CRL entry in LDAP) [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/gca2/crl/gca2comb.crl	NO
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Government CA 2 (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.2.1.1.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa/gca2/policies [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier:	NO

Field / x.509 extension	Value or Value Constant	Critical
	Notice Text= Government CA 2 Certification Policy and associated documentation available at http://web.ncdc.gov.sa/gca2/policies is hereby incorporated into your use or reliance on this Certificate.	
Authority Information Access	http://web.ncdc.gov.sa/certs/gca2.crt	NO
Key Usage	Digital Signature	NO
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2)	NO

1.3 NAME ENCRYPTION CERTIFICATE PROFILE

1.3.1 NAME ENCRYPTION CERTIFICATE POLICY

S. No.	Attribute	Name Encryption Certificate
1	Policy Name	Name Encryption Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.3.1.2.1.1.1.3
3	Subject	"cn=<English-Firstname> <English-Secondname> <English-Thirdname> <English-Lastname> <Arabic-Lastname> <Arabic-Thirdname> <Arabic-SecondName> <Arabic-FirstName> *, OU=<optional searchbase(s)>, C = SA" * Optional unverified nickname may be added at the end of the CN to achieve uniqueness of the subject.
4	Certificate Profile	See below after the table.
5	Application Usage	Government- CA 2 issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA 2 issued Name Certificate should honour Key Usage. The Name Encryption certificate should be used for data encryption. Following are some of the common usage of the certificate • Inter Government correspondence; • Public Information Posting by Authorized Government Personnel; • Departmental Forms Submission; • PKI enabled Application work-flow; and • E Tendering The Name 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 as per the Government- CA 2 practices, Subscribers agreement and not otherwise prohibited by law of Saudi Arabia.
6	Verification Process	**1.** Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents. **2.** The following will be considered valid identity documents: **3.** National ID / passport for citizens. **4.** Residence permit / passport for residents.

S. No.	Attribute	Name Encryption Certificate
		5. Letter from an authorized party (as prescribed by the DTSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process **6.** The domain name for the email address requested on the certificate should be verified to be owned by the issuing DTSP organization. 7. If the name ID certificate need to have the subscriber Email added on the SAN then Email address shall be verified. In order to verify the email the RAs will send an email for certificate issuance confirmation have authorization code and the subscriber shall confirm his/her email by responding to the email or provide copy of the mail. **8.** During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types.
7	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys, subscriber shall use Hardware Security device like smart card / tokens for key storage. **All Name ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA 2 CP.** The Name Encryption Private and public keys shall be generated by the CA and securely transferred onto a FIPS 140-2 Level 2 or higher certified hardware token or smart card. In addition, the Subscriber shall acknowledge receipt of the private key(s).
8	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber will be present at the RA for face-to-face identity verification • The RA will validate the documents submitted by the subscriber • The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner. • The subscriber will go to the RA customization center • The Subscriber will plug his smart card / USB token into the customization device. • The Subscriber will enter the PIN of the smart card / USB token • The Subscriber will enter reference number and an authorization code to generate keys and download certificates. • The CA will authenticate the Subscriber using the reference number and authorization code, generate the encryption key-pair, and securely transfer the encryption key and certificate onto the subscriber smart card / USB token.
9	Key Usage	Name Encryption certificate and keys shall be used for data encryption.
10	Private Key Protection	Subscribers shall protect their private keys in a FIPS 140-2 Level 2 or higher certified smart card or other hardware token/module. Subscriber is obligated to

S. No.	Attribute	Name Encryption Certificate
		secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key. Storage of name encryption private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.
11	Certificate Life Time	36 months
12	Key Backup	Only Private Decryption keys are backed up by the Government-CA 2. Backups shall be protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within the CA site, such as at a secure facility off-site.
13	Asymmetric Key Length	Minimum 2048 bits RSA
14	Certificate Re-key	Certificate re-key shall take place after a certificate is revoked and the subscriber information is still accountable or if a certificate has expired or is nearing expiry. In case of certificate's revocation and/or after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall be required to physically attend to the RA for identity validation and submission of supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed automatically by a supported client without revocation of the existing certificate. The certificate re-key can be done transparently when the subscriber logs in to the client software using his Digital ID.
15	Assurance Level	High

1.3.2 NAME ENCRYPTION CERTIFICATE PROFILE

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = <English FirstName> <English SecondName> <English ThirdName> <English LastName> <Arabic LastName> <Arabic ThirdName> <Arabic SecondName> <Arabic FirstName> * OU=<optional searchbase(s)> C = SA (Encoding should be in UTF8 only) * Optional unverified nickname may be added at the end of the CN to achieve uniqueness of the subject.	V1 Field
Serial Number	Unique serial number generated by the CMS	NO
Subject Alternative Name	RFC822 Name=<end-entity's verified email address> (should be verified to be the same as written in the subject) Note: Subject Alternative Names other than the RFC822 Name (email address) are not permitted to be included here.	NO

Field / x.509 extension	Value or Value Constant	Critical
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://web.ncdc.gov.sa/gca2/crl/gca2part<n>.crl Directory Address=(DN of the CRL entry in LDAP) [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/gca2/crl/gca2comb.crl	NO
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Issuing CA (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.2.1.1.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa/gca2/policies [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA 2 Certification Policy and associated documentation available at http://web.ncdc.gov.sa/gca2/policies is hereby incorporated into your use or reliance on this Certificate.	NO
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)	NO

Field / x.509 extension	Value or Value Constant	Critical
	Alternative Name: URL=http://ocsp.ncdc.gov.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://web.ncdc.gov.sa/certs/gca2.crt	
Key Usage	Key Encipherment	NO
Extended Key Usage	emailProtection (1.3.6.1.5.5.7.3.4)	NO

2. EMAIL ID (MANAGED)

The Email ID is a digital ID issued to an email address, which is a combination of three key-pairs, namely Signing, Authentication and Encryption.

2.1 EMAIL SIGNING (NON-REPUDIATION) CERTIFICATE

2.1.1 EMAIL SIGNING (NON-REPUDIATION) CERTIFICATE POLICY

S. No.	Attribute	Email Signing (Non-Repudiation) Certificate
1	Policy Name	Email Signing (Non-Repudiation) Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.3.1.2.1.1.2.1
3	Subject	"CN = <end-entity's verified email address>, OU=<optional searchbase(s)>, C = SA" Email ID certificates should only be issued to email addresses with domains which are verified to be owned by the respective DTSP Organization.
4	Certificate Profile	See below after the table.
5	Application Usage	**If subscriber wants to engage in legal signing he/she is advised to use Email Signing certificates/keys only. Digital Signatures made using this certificate type should be considered compliant to chapter four of the Saudi e-Transactions Law (Royal Decree No. (M/8), and thus considered valid in the court of law.** Every Participant acknowledges and agrees, to the extent permitted by applicable law, that where a transaction is required to be in writing, a message or other record bearing a digital signature verifiable with reference to an Government- CA 2 issued Email Signing Certificate is valid, effective, and enforceable to an extent no less than had the same message or record been written and signed on paper. Government- CA 2 issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA 2 issued Email Certificate should honour Key Usage. Following are some of the common usage of the certificate • Inter Government correspondence; • Public Information Posting by Authorized Government Personnel; • Departmental Forms Submission; • PKI enabled Application work-flow; and • E Tendering The Email 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 as per the Government- CA 2 practices, Subscribers agreement and not otherwise prohibited by the law of Saudi Arabia.
6	Verification Process	**1.** Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents. **2.** The following will be considered valid identity documents: **3.** National ID / passport for citizens. **4.** Residence permit / passport for residents.

S. No.	Attribute	Email Signing (Non-Repudiation) Certificate
		5. Letter from an authorized party (as prescribed by the DTSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process **6.** The domain name for the email address requested on the certificate should be verified to be owned by the issuing DTSP organization. **7.** Email address shall be verified. In order to verify the email the RAs will send an email for certificate issuance confirmation have authorization code and the subscriber shall confirm his/her email by responding to the email or provide copy of the mail or verified against a DTSP-trusted database. **8.** During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types.
7	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys, subscriber shall use Hardware Security device like smart card / tokens for key generation and storage. **All Email ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA 2 CP.** The Email Signing Private keys must be generated and stored on FIPS 140-2 Level 2 or higher certified hardware token or smart card, and the RA shall not retain any copy of the subscriber Private Keys. In addition, the Subscriber shall acknowledge receipt of the private key(s).
8	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber will be present at the RA for face-to-face identity verification • The RA will validate the documents submitted by the subscriber • The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner. • The subscriber will go to the RA customization center • The Subscriber will plug his smart card / USB token into the customization device. • The Subscriber will enter the PIN of the smart card / USB token • The Subscriber will enter reference number and an authorization code to generate keys and download certificates. • The Client Software will generate the Subscriber's keys securely on his smart card / USB token. • The CA will authenticate the Subscriber using the reference number and authorization code and receive the certificate signing request using a secure protocol such as PKIX-CMP. Upon successful authentication, the CA shall create the Subscribers certificates and

S. No.	Attribute	Email Signing (Non-Repudiation) Certificate
		transport them securely onto the Subscriber's smart cards / USB tokens.
9	Key Usage	Email Signing certificate and keys can be used for data integrity, and non-repudiation based on email address only.
10	Private Key Protection	Subscribers shall protect their private keys in a FIPS 140-2 Level 2 or higher certified smart card or other hardware token/module. Subscriber is obligated to secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key. Generation and/or Storage of email signing private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.
11	Certificate Life Time	36 months
12	Key Backup	The DTSP or CA shall not take any backup of the private keys of this certificate type.
13	Asymmetric Key Length	Minimum 2048 bits RSA
14	Certificate Re-key	Certificate re-key shall take place after a certificate is revoked and the subscriber information is still accountable or if a certificate has expired or is nearing expiry. In case of certificate's revocation and/or after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall be required to physically attend to the RA for identity validation and submission of supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed automatically by a supported client without revocation of the existing certificate. The certificate re-key can be done transparently when the subscriber logs in to the client software using his Digital ID.
15	Assurance Level	High

2.1.2 EMAIL SIGNING (NON-REPUDIATION) CERTIFICATE PROFILE

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = <end-entity's verified email address> OU=<optional searchbase(s)> C = SA (Encoding should be in UTF8 only)	V1 Field
Serial Number	Unique serial number generated by the CMS	NO

Field / x.509 extension	Value or Value Constant	Critical
Subject Alternative Name	RFC822 Name=<end-entity's verified email address> (should be verified to be the same as written in the subject) Note: Subject Alternative Names other than the RFC822 Name (email address) are not permitted to be included here.	NO
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/gca2/crl/gca2part<n>.crl Directory Address=(DN of the CRL entry in LDAP) [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/gca2/crl/gca2comb.crl	NO
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Issuing CA (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.2.1.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa/gca2/policies [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA 2 Certification Policy and associated documentation available at http://web.ncdc.gov.sa/gca2/policies is hereby incorporated into your use or reliance on this Certificate.	NO

Field / x.509 extension	Value or Value Constant	Critical
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ncdc.gov.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://web.ncdc.gov.sa/certs/gca2.crt	NO
Key Usage	Digital Signature Non Repudiation	NO
Extended Key Usage	emailProtection (1.3.6.1.5.5.7.3.4)	NO

2.2 EMAIL AUTHENTICATION CERTIFICATE

2.2.1 EMAIL AUTHENTICATION CERTIFICATE POLICY

S. No.	Attribute	Email Authentication Certificate
1	Policy Name	Email Authentication Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.3.1.2.1.1.2.2
3	Subject	"CN = <end-entity's verified email address>, OU=<optional searchbase(s)>, C = SA" Email ID certificates should only be issued to email addresses with domains which are verified to be owned by the respective DTSP Organization.
4	Certificate Profile	See below after the table.
5	Application Usage	Government- CA 2 issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA 2 issued Email Certificate should honour Key Usage. The Email Authentication certificate should be used for client authentication and may also be used to verify data integrity. For Legal-Signing, it is required to use the Email Signing Certificate. Following are some of the common usage of the certificate • Inter Government correspondence; • Public Information Posting by Authorized Government Personnel; • Departmental Forms Submission; • PKI enabled Application work-flow; and • E Tendering The Email 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 as per the Government- CA 2 practices, Subscribers agreement and not otherwise prohibited by law of Saudi Arabia.
6	Verification Process	**1.** Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents. **2.** The following will be considered valid identity documents: • National ID / passport for citizens. • Residence permit / passport for residents. **3.** Letter from an authorized party (as prescribed by the DTSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process **4.** The domain name for the email address requested on the certificate should be verified to be owned by the issuing DTSP organization. **5.** Email address shall be verified. In order to verify the email the RAs will send an email for certificate issuance confirmation have authorization code and the subscriber shall confirm his/her email by responding to the email or provide copy of the mail or verified against a CSP-trusted database. **6.** During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics

S. No.	Attribute	Email Authentication Certificate
		Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types.
7	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys, subscriber shall use Hardware Security device like smart card / tokens for key generation and storage. **All Email ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA 2 CP.** The Email Authentication Private keys must be generated and stored on FIPS 140-2 Level 2 or higher certified hardware token or smart card, and the RA shall not retain any copy of the subscriber Private Keys. In addition, the Subscriber shall acknowledge receipt of the private key(s).
8	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber will be present at the RA for face-to-face identity verification • The RA will validate the documents submitted by the subscriber • The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner. • The subscriber will go to the RA customization center • The Subscriber will plug his smart card / USB token into the customization device. • The Subscriber will enter the PIN of the smart card / USB token • The Subscriber will enter reference number and an authorization code to generate keys and download certificates. • The Client Software will generate the Subscriber's keys securely on his smart card / USB token. • The CA will authenticate the Subscriber using the reference number and authorization code and receive the certificate signing request using a secure protocol such as PKIX-CMP. Upon successful authentication, the CA shall create the Subscribers certificates and transport them securely onto the Subscriber's smart cards / USB tokens.
9	Key Usage	Email Authentication certificate and keys shall be used for authentication of/by email address only.
10	Private Key Protection	Subscribers shall protect their private keys in a FIPS 140-2 Level 2 or higher certified smart card or other hardware token/module. Subscriber is obligated to secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key. Generation and/or Storage of email authentication private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.
11	Certificate Life Time	36 months
12	Key Backup	The DTSP or CA shall not take any backup of the private keys of this certificate type.

S. No.	Attribute	Email Authentication Certificate
13	Asymmetric Key Length	Minimum 2048 bits RSA
14	Certificate Re-key	Certificate re-key shall take place after a certificate is revoked and the subscriber information is still accountable or if a certificate has expired or is nearing expiry. In case of certificate's revocation and/or after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall be required to physically attend to the RA for identity validation and submission of supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed automatically by a supported client without revocation of the existing certificate. The certificate re-key can be done transparently when the subscriber logs in to the client software using his Digital ID.
15	Assurance Level	High

2.2.2 *EMAIL AUTHENTICATION CERTIFICATE PROFILE*

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = <end-entity's verified email address> OU=<optional searchbase(s)> C = SA (Encoding should be in UTF8 only)	V1 Field
Serial Number	Unique serial number generated by the CMS	NO
Subject Alternative Name	RFC822 Name=<end-entity's verified email address> (should be verified to be the same as written in the subject) Note: Subject Alternative Names other than the RFC822 Name (email address) are not permitted to be included here.	NO
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gca2part<n>.crl Directory Address=(DN of the CRL entry in LDAP) [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/gca2/crl/gca2comb.crl	NO

Field / x.509 extension	Value or Value Constant	Critical
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Issuing CA (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.2.1.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa/gca2/policies [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA 2 Certification Policy and associated documentation available at http://web.ncdc.gov.sa/gca2/policies is hereby incorporated into your use or reliance on this Certificate.	NO
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ncdc.gov.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://web.ncdc.gov.sa/certs/gca2.crt	NO
Key Usage	Digital Signature	NO
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2)	NO

2.3 EMAIL ENCRYPTION CERTIFICATE

2.3.1 EMAIL ENCRYPTION CERTIFICATE POLICY

S. No.	Attribute	Email Encryption Certificate
1	Policy Name	Email Encryption Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.3.1.2.1.1.2.3
3	Subject	"CN = <end-entity's verified email address>, OU=<optional searchbase(s)>, C = SA" Email ID certificates should only be issued to email addresses with domains which are verified to be owned by the respective DTSP Organization.
4	Certificate Profile	See below after the table.
5	Application Usage	Government- CA 2 issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA 2 issued Email Certificate should honour Key Usage. The Email Encryption certificate should be used for data encryption. Following are some of the common usage of the certificate • Inter Government correspondence; • Public Information Posting by Authorized Government Personnel; • Departmental Forms Submission; • PKI enabled Application work-flow; and • E Tendering The Email 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 as per the Government- CA 2 practices, Subscribers agreement and not otherwise prohibited by law of Saudi Arabia.
6	Verification Process	**1.** Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents. **2.** The following will be considered valid identity documents: **3.** National ID / passport for citizens. **4.** Residence permit / passport for residents. **5.** Letter from an authorized party (as prescribed by the DTSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process **6.** The domain name for the email address requested on the certificate should be verified to be owned by the issuing DTSP organization. **7.** Email address shall be verified. In order to verify the email the RAs will send an email for certificate issuance confirmation have authorization code and the subscriber shall confirm his/her email by responding to the email or provide copy of the mail or verified against a DTSP-trusted database. **8.** During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics

S. No.	Attribute	Email Encryption Certificate
		Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types.
7	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys, subscriber shall use Hardware Security device like smart card / tokens for key storage. **All Email ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA 2 CP.** The Email encryption Private and public keys shall be generated by the CA and securely transferred onto a FIPS 140-2 Level 2 or higher certified hardware token or smart card. In addition, the Subscriber shall acknowledge receipt of the private key(s).
8	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber will be present at the RA for face-to-face identity verification • The RA will validate the documents submitted by the subscriber • The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner. • The subscriber will go to the RA customization center • The Subscriber will plug his smart card / USB token into the customization device. • The Subscriber will enter the PIN of the smart card / USB token • The Subscriber will enter reference number and an authorization code to generate keys and download certificates. • The CA will authenticate the Subscriber using the reference number and authorization code, generate the encryption key-pair, and securely transfer the encryption key and certificate onto the subscriber smart card / USB token.
9	Key Usage	Email Encryption certificate and keys shall be used for data encryption.
10	Private Key Protection	Subscribers shall protect their private keys in a FIPS 140-2 Level 2 or higher certified smart card or other hardware token/module. Subscriber is obligated to secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key. Storage of email encryption private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.
11	Certificate Life Time	36 months
12	Key Backup	Only Private Decryption keys are backed up by the Government-CA 2. Backups shall be protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within the CA site, such as at a secure facility off-site.
13	Asymmetric Key Length	Minimum 2048 bits RSA

S. No.	Attribute	Email Encryption Certificate
14	Certificate Re-key	Certificate re-key shall take place after a certificate is revoked and the subscriber information is still accountable or if a certificate has expired or is nearing expiry. In case of certificate's revocation and/or after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall be required to physically attend to the RA for identity validation and submission of supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed automatically by a supported client without revocation of the existing certificate. The certificate re-key can be done transparently when the subscriber logs in to the client software using his Digital ID.
15	Assurance Level	High

2.3.2 *EMAIL ENCRYPTION CERTIFICATE PROFILE*

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = <end-entity's verified email address> OU=<optional searchbase(s)> C = SA (Encoding should be in UTF8 only)	V1 Field
Serial Number	Unique serial number generated by the CMS	NO
Subject Alternative Name	RFC822 Name=<end-entity's verified email address> (should be verified to be the same as written in the subject) Note: Subject Alternative Names other than the RFC822 Name (email address) are not permitted to be included here.	NO
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gca2part<n>.crl Directory Address=(DN of the CRL entry in LDAP) [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/gca2/crl/gca2comb.crl	NO

Field / x.509 extension	Value or Value Constant	Critical
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Issuing CA (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.2.1.1.2.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa/gca2/policies [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA 2 Certification Policy and associated documentation available at http://web.ncdc.gov.sa/gca2/policies is hereby incorporated into your use or reliance on this Certificate.	NO
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ncdc.gov.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://web.ncdc.gov.sa/certs/gca2.crt	NO
Key Usage	Key Encipherment	NO
Extended Key Usage	emailProtection (1.3.6.1.5.5.7.3.4)	NO

3. ORGANIZATION SEALING CERTIFICATE (MANAGED)

3.1 ORGANIZATION SEALING CERTIFICATE POLICY

S. No.	Attribute	Organization Sealing Certificate
1	Policy Name	Organization Sealing Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.3.1.2.1.1.3.1
3	Subject	"CN = <Full Organization and Department Name, suffixed with one or more of the below: - Role, - Designation, - Location, - Application Name***>, OU=<optional searchbase(s)>, C = SA" *** Identifier rules: - Use of only organization name in the CN is not permitted - Some examples of CN are 'CN=Ministry of Communications and IT – HR Department' OR 'CN=Ministry of Communications and IT – Finance – Riyadh – ERP1' OR 'CN=Ministry of Communications and IT – Payroll'
4	Certificate Profile	See below after the table.
5	Application Usage	**If subscriber wants to engage in legal signing he/she is advised to use Signing certificates/keys. Digital Signatures made using this certificate type should be considered compliant to chapter four of the Saudi e-Transactions Law (Royal Decree No. (M/8), and thus considered valid in the court of law.** Every Participant acknowledges and agrees, to the extent permitted by applicable law, that where a transaction is required to be in writing, a message or other record bearing a digital signature verifiable with reference to an Government- CA 2 issued Signing Certificate is valid, effective, and enforceable to an extent no less than had the same message or record been written and signed on paper. Government- CA 2 issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA 2 issued Signing Certificate should honour Key Usage. Following are some of the common usage of the certificate • Inter Government correspondence; • Public Information Posting by Authorized Government Personnel; • Departmental Forms Submission; • Sealing electronic document; • PKI enabled Application work-flow; and • E Tendering The Signing 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 as per the Government- CA 2 practices, Subscribers agreement and not otherwise prohibited by the law of Saudi Arabia. Certificate(s) issued under this type shall not be used for any form of data encryption.
6	Verification Process	**1.** Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents.

S. No.	Attribute	Organization Sealing Certificate
		2. If subscriber representing organisation changes for any reason the Verification Process for the new subscriber taking over the responsibility is to be done without fail. **3.** The following will be considered valid identity documents: **a.** National ID / passport for citizens. **b.** Residence permit / passport for residents. **4.** Validation of Identifier rules as stated in point 3 of this table. *** **5.** It is mandatory to obtain specific approval letter for such representation from the Minister, Governor, or equivalent authority applicable to the organization, government agency, government body, government program, government department, government department head or associated role. In case of commercial organizations/entities, such approval letter should be approved by the authorized signatories along with a valid Chamber of Commerce attestation. Such letter must include authorization of issuance mentioning the exact certificate subject name, and must also identify the subscriber's name along with his National ID number or Passport Number. **6.** During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types.
7	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys, subscriber shall use FIPS 140-2 Level 3 or higher certified Hardware Security Module for key generation and storage. **Signing certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA 2 CP.** The Private key corresponding to the signing certificate must be generated and stored on FIPS 140-2 Level 3 or higher certified Hardware Security Module, and the RA shall not retain any copy of the subscriber Private Key. In addition, the Subscriber shall acknowledge receipt of the private key.
8	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber will be present at the RA for face-to-face identity verification • The RA will validate the documents submitted by the subscriber • The RA will complete the registration and issue the sealing certificate • The RA will hand the certificate to the certificate owner (subscriber) • The certificate owner (subscriber) will install the certificate on the sealing client application

S. No.	Attribute	Organization Sealing Certificate
9	Key Usage	Signing certificate and associated keys can be used for legal-signing, data integrity, and client-authentication based on the identifier/attribute to which the certificate was issued.
10	Private Key Protection	Subscribers shall protect their private key(s) in a FIPS 140-2 Level 3 or higher certified Hardware Security Module. Subscriber is obligated to secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware module, or other activation data that is used to control access to the Subscriber's private key. Generation and/or Storage of signing private keys shall only be done in FIPS 140-2 Level 3 or higher certified Hardware Security Module.
11	Certificate Life Time	36 months
12	Key Backup	The DTSP or CA shall not take any backup of the private keys of this certificate type.
13	Asymmetric Key Length	Minimum 2048 bits RSA
14	Certificate Re-key	Certificate re-key shall take place after a certificate is revoked and the subscriber information is still accountable or if a certificate has expired or is nearing expiry. In case of certificate's revocation and/or after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall be required to physically attend to the RA for identity validation and submission of supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed automatically by a supported client without revocation of the existing certificate. The certificate re-key can be done transparently when the subscriber logs in to the client software using his Digital ID.
15	Assurance Level	High

3.2 ORGANIZATION SEALING CERTIFICATE PROFILE

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = < Full Organization and Department Name, suffixed with one or more of the below: - Role, - Designation, - Location, Application Name***> OU=<optional searchbase(s)> C = SA (Encoding should be in UTF8 only)	V1 Field

Field / x.509 extension	Value or Value Constant	Critical
	*** Please refer to the Identifier Rules in point 3 of the preceding table.	
Serial Number	Unique serial number generated by the CMS	NO
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://web.ncdc.gov.sa/gca2/crl/gca2part<n>.crl Directory Address=(DN of the CRL entry in LDAP) [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://web.ncdc.gov.sa/gca2/policies	NO
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Issuing CA (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.2.1.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa/gca2/policies [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA 2 Certification Policy and associated documentation available at http://web.ncdc.gov.sa/gca2/policies is	NO

Field / x.509 extension	Value or Value Constant	Critical
	hereby incorporated into your use or reliance on this Certificate.	
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ncdc.gov.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://web.ncdc.gov.sa/certs/gca2.crt	NO
Key Usage	Digital Signature	YES
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2)	NO

4. EMPLOYEE SIGNING CERTIFICATE (MANAGED)

4.1 Employee Signing Certificate Policy

S. No.	Attribute	Employee Signing Certificate
1	Policy Name	Employee Signing Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.3.1.2.1.1.4.1
3	Subject	"CN = <English FirstName> <English SecondName> <English ThirdName> <English LastName>/ <Arabic LastName> <Arabic ThirdName> <Arabic SecondName> <Arabic FirstName> - < Role of the Employee> *** O= Organization Name of Employee Applying for Certificate OU=<optional searchbase(s)>, C = SA" *** Identifier rules: - Full Name of the Employee either in English or Arabic - Full Name either in English or Arabic, suffixed with Employee Role - Email ID of the Employee - Organization Name of Employee
4	Certificate Profile	See below after the table.
5	Application Usage	**If subscriber wants to engage in legal signing he/she is advised to use Signing certificates/keys. Digital Signatures made using this certificate type should be considered compliant to chapter four of the Saudi e-Transactions Law (Royal Decree No. (M/8), and thus considered valid in the court of law.** Every Participant acknowledges and agrees, to the extent permitted by applicable law, that where a transaction is required to be in writing, a message or other record bearing a digital signature verifiable with reference to an Government- CA 2 issued Signing Certificate is valid, effective, and enforceable

S. No.	Attribute	Employee Signing Certificate
		to an extent no less than had the same message or record been written and signed on paper. Government- CA 2 issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA 2 issued Signing Certificate should honour Key Usage. Following are some of the common usage of the certificate • Inter Government correspondence; • Public Information Posting by Authorized Government Personnel; • Departmental Forms Submission; • Sealing electronic document; • PKI enabled Application work-flow; and • E Tendering The Signing 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 as per the Government- CA 2 practices, Subscribers agreement and not otherwise prohibited by the law of Saudi Arabia. Certificate(s) issued under this type shall not be used for any form of data encryption.
6	Verification Process	**1.** Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents. **2.** If subscriber representing organisation for Employee Certificate changes for any reason the Verification Process for the new subscriber taking over the responsibility is to be done without fail. **3.** The following will be considered valid identity documents: **a.** National ID / passport for citizens. **b.** Residence permit / passport for residents. **c. Employment ID / Employment Certificate** **4.** Validation of Identifier rules as stated in point 3 of this table. *** **5.** It is mandatory to obtain specific approval letter for such representation from the Minister, Governor, or equivalent authority applicable to the organization, government agency, government body, government program, government department, government department head or associated role. In case of commercial organizations/entities, such approval letter should be approved by the authorized signatories along with a valid Chamber of Commerce attestation. Such letter must include authorization of issuance mentioning the exact certificate subject name, and must also identify the subscriber's name along with his National ID number or Passport Number. **6.** During the request submission, the identity of the subscriber will be validated by ensuring the authenticity of the subscriber's identity documentation and matching it with his / her characteristics Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the Subscriber/approver may use a digital signature performed using the existing certificate to waive another face-to-face verification, and for verifying the

S. No.	Attribute	Employee Signing Certificate
		attribute/identifier to which such certificate was issued. Such digital signature shall be accepted only if performed by one of NIC-approved signing certificate types.
7	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys, subscriber shall use Hardware Security device like smart card / tokens for key generation and storage. **Employee Certificate MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA 2 CP.** The Employee Signing Private keys must be generated and stored on FIPS 140-2 Level 2 or higher certified hardware token or smart card, and the RA shall not retain any copy of the subscriber Private Keys. In addition, the Subscriber shall acknowledge receipt of the private key(s).
8	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber will be present at the RA for face-to-face identity verification • The RA will validate the documents submitted by the subscriber • The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner. • The subscriber will go to the RA customization center • The Subscriber will plug his smart card / USB token into the customization device. • The Subscriber will enter the PIN of the smart card / USB token • The Subscriber will enter reference number and an authorization code to generate keys and download certificates. • The Client Software will generate the Subscriber's keys securely on his smart card / USB token. • The CA will authenticate the Subscriber using the reference number and authorization code and receive the certificate signing request using a secure protocol such as PKIX-CMP. Upon successful authentication, the CA shall create the Subscribers certificates and transport them securely onto the Subscriber's smart cards / USB tokens.
9	Key Usage	Employee certificate and keys can be used for legal-signing, data integrity, and non-repudiation based on the identifier/attribute to which the certificate was issued, within the bounds of the specified Key Usage.
10	Private Key Protection	Subscribers shall protect their private keys in a FIPS 140-2 Level 2 or higher certified smart card or other hardware token/module. Subscriber is obligated to secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key. Generation and/or Storage of name signing private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.
11	Certificate Life Time	36 months
12	Key Backup	The DTSP or CA shall not take any backup of the private keys of this certificate type.
13	Asymmetric Key Length	Minimum 2048 bits RSA

S. No.	Attribute	Employee Signing Certificate
14	Certificate Re-key	Certificate re-key shall take place after a certificate is revoked and the subscriber information is still accountable or if a certificate has expired or is nearing expiry. In case of certificate's revocation and/or after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall be required to physically attend to the RA for identity validation and submission of supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed automatically by a supported client without revocation of the existing certificate. The certificate re-key can be done transparently when the subscriber logs in to the client software using his Digital ID.
15	Assurance Level	High

4.2 EMPLOYEE SIGNING CERTIFICATE PROFILE

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = <English FirstName> <English SecondName> <English ThirdName> <English LastName> **/** <Arabic LastName> <Arabic ThirdName> <Arabic SecondName> <Arabic FirstName> **-** < Role of the Employee> O= <Organization Name of Employee Applying for Certificate> OU=<optional searchbase(s)> C = SA (Encoding should be in UTF8 only)	V1 Field
Subject Alternative Name	RFC822 Name=<end-entity's verified email address> (should be verified to be the same as written in the subject) Note: Subject Alternative Names other than the RFC822 Name (email address) are not permitted to be included here.	NO
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://web.ncdc.gov.sa/gca2/crl/gca2part<n>.crl Directory Address=(DN of the CRL entry in LDAP) [2]CRL Distribution Point Distribution Point Name: Full Name:	NO

Field / x.509 extension	Value or Value Constant	Critical
	URL=http://web.ncdc.gov.sa/gca2/crl/gca2comb.crl	
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Issuing CA (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.2.1.1.4.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa/gca2/policies [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA 2 Certification Policy and associated documentation available at http://web.ncdc.gov.sa/gca2/policies is hereby incorporated into your use or reliance on this Certificate.	NO
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ncdc.gov.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://web.ncdc.gov.sa/certs/gca2.crt	NO
Key Usage	Digital Signature, Non Repudiation	NO
Extended Key Usage	Email Protection	YES

5. EMPLOYEE REMOTE SIGNING CERTIFICATE (MANAGED)

5.1 EMPLOYEE REMOTE SIGNING CERTIFICATE POLICY

S. No.	Attribute	Employee Remote Signing Certificate
1	Policy Name	Employee Remote Signing Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.3.1.2.1.1.5.1
3	Subject	"CN = <English FirstName> <English SecondName> <English ThirdName> <English LastName>/ <Arabic LastName> <Arabic ThirdName> <Arabic SecondName> <Arabic FirstName> - < Job Title> *** E= email ID of the employee O= Organization Name of Employee Applying for Certificate OU=<optional searchbase(s)>, C = SA" *** Identifier rules: - Full Name of the Employee either in English or Arabic - Full Name either in English or Arabic, suffixed with Job Title - Email ID of the Employee - Organization Name of Employee
4	Certificate Profile	See below after the table.
5	Application Usage	**If subscriber wants to engage in legal signing he/she is advised to use Signing certificates/keys. Digital Signatures made using this certificate type should be considered compliant to chapter four of the Saudi e-Transactions Law (Royal Decree No. (M/8), and thus considered valid in the court of law.** Every Participant acknowledges and agrees, to the extent permitted by applicable law, that where a transaction is required to be in writing, a message or other record bearing a digital signature verifiable with reference to an Government- CA 2 issued Signing Certificate is valid, effective, and enforceable to an extent no less than had the same message or record been written and signed on paper. Government- CA 2 issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA 2 issued Signing Certificate should honour Key Usage. Following are some of the common usage of the certificate • Inter Government correspondence; • Public Information Posting by Authorized Government Personnel; • Departmental Forms Submission; and • PKI enabled Application work-flow. The Signing 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 as per the Government- CA 2 practices, Subscribers agreement and not otherwise prohibited by the law of Saudi Arabia. Certificate(s) issued under this type shall not be used for any form of data encryption. The Employee Remote Signing Certificate issued to Partner employee shall be used within the Government agency processes and communication which is requesting for Partner employee certificate from NIC DTSP.

S. No.	Attribute	Employee Remote Signing Certificate
		The Employee Remote Signing Certificate is issued to Partner employee on special request from Government agency. The usage of this certificate is limited within requesting Government agency. Partner employee shall be liable for any use of such certificate outside the requesting Government agency.
6	Verification Process	1. After successful completion of the employee hiring process employee information is populated in the trusted database of the organization. This trusted information source is used for the Employee Remote Signing Certificate for the employees. 2. Some of the attributes can be used from this trusted database for the Employee Remote Signing Certificate and serve as indirect pre-verified information of the employees. 3. The following information is considered duly verified (equivalent of high assurance) regarding employee from the trusted database of the organization: a. Name b. Job Title c. Organization Name d. Department e. Email Address f. Mobile Number g. Employment ID 4. Validation of Identifier rules as stated in point 3 of this table. *** 5. Employee interested in Remote Signing Certificate requests through h. Face to face registration with reporting manager approval or i. Other equivalent method. 6. If DTSP decides to follow Face to Face method for Remote Signing Certificate, the RA shall collect relevant employee identity data required for identity proofing and verification. 7. RA verifies Employee information before approval. Process for Partner employee working or having business relationship with Government Agency: 1. Government Agency communicates with NIC for the Partner certificates with business justification as to why it is important to provide Employee Remote Signing Certificate for particular Partner employees. 2. After looking at business justification given by Government Agency , CA PA may give approval for Employee Remote Signing Certificates to Partner employees. 3. Approval of Employee Remote Signing Certificate to Partner employee is at sole discretion of CA PA. 4. Once approved, Government Agency will be initiating the Employee Remote Signing Certificate registration process on behalf the Partner employee.

S. No.	Attribute	Employee Remote Signing Certificate
		5. NIC DTSP will be providing registration process along with Identity Proofing requirements to Government Agency through mail or other means. 6. Partner employee completes application form and submits required information to Government Agency. 7. Government Agency is responsible for providing accurate information along with supportive documents to NIC DTSP as part of registration process. 8. Government Agency is responsible to verify the Partner employee information and identity according to verification process defined by the NIC DTSP.. 9. Government Agency shall be sending verified Partner employee information to NIC through the agreed channel. 10. Once complete verified information along with application form is received by NIC DTSP, RA will be initiating certificate issuance process.
7	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys, subscriber shall use Hardware Security device for key generation and storage. Employee Remote Signing keys are generated and stored using FIPS 140-2 Level 3 or higher certified hardware security module. The signing keys are under the control of employee and used through key activation data provided by employee during every transaction.
8	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom belongs to the organization as per following or similar other process defined by the DTSP: • Upon successful verification, RA approves the employee certificate request. • Mail is sent to employee with specific links in order to activate his/her account. • By clicking the link; employee is asked to setup Signing Platform password and security question. Employee is to accept the Terms of Service and Privacy Policy to move forward the activation steps. • Employee can download Signing Platform mobile application from Apple or Google Play Store. • After installing the application employee logs in to Signing Platform using his/her credentials. • Next smart phone will ask for the fingerprint/face recognition registration. • OTPs are sent to email and mobile number of the employee.

S. No.	Attribute	Employee Remote Signing Certificate
		• To setup the smart phone for remote authorization employee types the OTPs received on email and mobile. • Employee is required to sign a document in order to initiate the key generation process. • Employee clicks on the sign button which in turn will ask for the password (i.e. Signing Platform login password). • It will ask employee to remote authorize using smart phone with fingerprint/face recognition. For Partner employee working or having business relationship with Government Agency: NIC DTSP will initiate the certificate issuance process as mentioned above, subject to: • Government Agency communicates partner certificates request with business justification to NIC, • CA PA gives approval, • Government Agency completes registration process, • Government Agency performs verification process as per NIC DTSP requirements, and • Government Agency submits verified Partner employee information to NIC DTSP.
9	Key Usage	Employee certificate and keys can be used for legal-signing, data integrity, and non-repudiation based on the identifier/attribute to which the certificate was issued.
10	Private Key Protection	Employee is obligated to secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key. Employee Remote Signing keys are protected using the FIPS 140-2 Level 3 or higher certified hardware security module. The signing keys are under the control of employee and used through key activation data provided by employee during every transaction.
11	Certificate Life Time	36 months
12	Key Backup	The DTSP or CA requires backup of employee remote signing private keys to facilitate disaster recovery. The backed up keys are protected using FIPS 140-2 Level 3 or higher certified hardware security module under multi-person control.
13	Asymmetric Key Length	Minimum 2048 bits RSA
14	Certificate Re-key	Certificate re-key shall take place after a certificate is revoked and the employee information is still accountable or if a certificate has expired or is nearing expiry. In case of certificate's revocation and/or after expiry, Employee request submission through the ERP system using employee credentials and mail is to be sent to the reporting manager for the re-key of a Subscriber's certificate. Certificate re-key for Partner Employee Remote Signing Certificate shall be as defined by the NIC DTSP. In case of certificate nearing expiry (as set in the CA policies for managed certificate), the re-key process may be performed automatically by a supported

S. No.	Attribute	Employee Remote Signing Certificate
		client without revocation of the existing certificate. The certificate re-key can be done transparently when the employee logs in to the client software using his Digital ID.
15	Certificate Revocation	If the employee quits/terminated in organisation, mail is to be sent from trusted database of the organization to RA or using other method to intimate RA for revocation of the certificate. Employee can request revocation of his Employee Remote Signing Certificate through mail. At any point, request for revocation of Partner Employee Remote Signing Certificate can be requested by- • Government agency which has requested for certificate or • Partner employee apart from law enforcing agencies and NIC.
16	Assurance Level	High

5.2 EMPLOYEE REMOTE SIGNING CERTIFICATE PROFILE

Field / x.509 extension	Value or Value Constant	Critical
Subject	CN = <English FirstName> <English SecondName> <English ThirdName> <English LastName> **/** <Arabic LastName> <Arabic ThirdName> <Arabic SecondName> <Arabic FirstName> - < Job Title> E=<Email ID of the Employee> O= <Organization Name of Employee Applying for Certificate> OU=<optional searchbase(s)> C = SA (Encoding should be in UTF8 only)	V1 Field
Subject Alternative Name	RFC822 Name=<end-entity's verified email address> (should be verified to be the same as written in the subject) Note: Subject Alternative Names other than the RFC822 Name (email address) are not permitted to be included here.	NO
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://web.ncdc.gov.sa/gca2/crl/gca2part<n>.crl Directory Address=(DN of the CRL entry in LDAP) [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://web.ncdc.gov.sa/gca2/crl/gca2comb.crl	NO

Field / x.509 extension	Value or Value Constant	Critical
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Issuing CA (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=End Entity Path Length Constraint=None	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.2.1.1.5.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa/gca2/policies [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA 2 Certification Policy and associated documentation available at http://web.ncdc.gov.sa/gca2/policies is hereby incorporated into your use or reliance on this Certificate.	NO
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.ncdc.gov.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://web.ncdc.gov.sa/certs/gca2.crt	NO
Key Usage	Digital Signature, Non Repudiation	NO
Extended Key Usage	Email Protection	NO