



# **NCDC GOVERNMENT-CA CERTIFICATE POLICY**

***Document Classification:***

***Public***

***Version Number: 2.4***

***Issue Date: April 15, 2012***

## Document Reference

<b>Item</b>	<b>Description</b>
<b>Document Title:</b>	NCDC Government-CA Certificate Policy
<b>Version Number:</b>	2.4
<b>Document Status:</b>	Approved

## Document Control

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

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

## Table of Contents

<b>1. INTRODUCTION.....</b>	<b>9</b>
1.1 Overview.....	9
1.1.1 <i>CERTIFICATE POLICY</i> .....	10
1.1.2 <i>RELATIONSHIP BETWEEN THE CP AND THE CPS</i> .....	10
1.1.3 <i>INTERACTION WITH OTHER PKIS</i> .....	10
1.1.4 <i>SCOPE</i> .....	10
1.2 Document Name and Identification .....	11
1.3 PKI Participants .....	11
1.3.1 <i>GOVERNMENT-CA POLICY AUTHORITY (GOVERNMENT-CA PA)</i> .....	11
1.3.2 <i>GOVERNMENT CERTIFICATION AUTHORITY (GOVERNMENT-CA)</i> .....	11
1.3.3 <i>CERTIFICATION SERVICE PROVIDER (CSP)</i> .....	12
1.3.4 <i>TRUSTED AGENT</i> .....	13
1.3.5 <i>SUBSCRIBERS</i> .....	13
1.3.6 <i>RELYING PARTIES</i> .....	13
1.3.7 <i>DEVICE SPONSOR</i> .....	13
1.3.8 <i>ONLINE CERTIFICATE STATUS PROTOCOL RESPONDER</i> .....	13
1.4 Certificate Usage .....	14
1.4.1 <i>APPROPRIATE CERTIFICATE USES</i> .....	14
1.4.2 <i>PROHIBITED CERTIFICATE USES</i> .....	15
1.5 Policy Administration .....	15
1.5.1 <i>ADMINISTRATION ORGANIZATION</i> .....	15
1.5.2 <i>CONTACT PERSON</i> .....	15
1.5.3 <i>PERSON DETERMINING CPS SUITABILITY FOR THE POLICY</i> .....	15
1.5.4 <i>CPS APPROVAL</i> .....	15
1.6 Definitions and Acronyms .....	15
<b>2. PUBLICATION AND REPOSITORY RESPONSIBILITIES.....</b>	<b>16</b>
2.1 Repositories .....	16
2.1.1 <i>REPOSITORY OBLIGATIONS</i> .....	16
2.2 Publication of Certification Information .....	16
2.2.1 <i>PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS</i> .....	16
2.2.2 <i>PUBLICATION OF CA INFORMATION</i> .....	16
2.2.3 <i>INTEROPERABILITY</i> .....	17
2.3 Time or Frequency of Publication .....	17
2.4 Access Controls on Repositories .....	17
<b>3. IDENTIFICATION AND AUTHENTICATION .....</b>	<b>18</b>
3.1 Naming.....	18
3.1.1 <i>TYPES OF NAMES</i> .....	18
3.1.2 <i>NEED FOR NAMES TO BE MEANINGFUL</i> .....	18
3.1.3 <i>ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS</i> .....	18
3.1.4 <i>RULES FOR INTERPRETING VARIOUS NAME FORMS</i> .....	18
3.1.5 <i>UNIQUENESS OF NAMES</i> .....	18
3.1.6 <i>RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS</i> .....	19
3.2 Initial Identity Validation.....	19
3.2.1 <i>METHOD TO PROVE POSSESSION OF PRIVATE KEY</i> .....	19
3.2.2 <i>AUTHENTICATION OF ISSUER IDENTITY</i> .....	19
3.2.3 <i>IDENTITY-PROOFING OF INDIVIDUAL IDENTITY</i> .....	19
3.2.4 <i>NON-VERIFIED SUBSCRIBER INFORMATION</i> .....	20
3.2.5 <i>CRITERIA OF INTEROPERATION</i> .....	20
3.3 Identification and Authentication for Re-key Requests.....	20
3.3.1 <i>IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY</i> .....	20
3.3.2 <i>IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION</i> .....	20

3.4 Identification and Authentication for Revocation Requests ..... 21

**4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS ..... 22**

4.1 Certificate Application ..... 22

    4.1.1 *SUBMISSION OF CERTIFICATE APPLICATION* ..... 22

    4.1.2 *ENROLLMENT PROCESS AND RESPONSIBILITIES* ..... 22

4.2 Certificate Application Processing ..... 22

    4.2.1 *PERFORMING IDENTITY-PROOFING FUNCTIONS* ..... 22

    4.2.2 *APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS* ..... 23

    4.2.3 *TIME TO PROCESS CERTIFICATE APPLICATIONS* ..... 23

4.3 Certificate Issuance ..... 23

    4.3.1 *CA ACTIONS DURING CERTIFICATE ISSUANCE* ..... 23

    4.3.2 *NOTIFICATION TO SUBSCRIBER OF CERTIFICATE ISSUANCE* ..... 23

4.4 Certificate Acceptance ..... 24

    4.4.1 *CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE* ..... 24

    4.4.2 *PUBLICATION OF THE CERTIFICATE BY THE CA* ..... 24

    4.4.3 *NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES* ..... 24

4.5 Key Pair and Certificate Usage ..... 24

    4.5.1 *SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE* ..... 24

    4.5.2 *RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE* ..... 24

4.6 Certificate Renewal ..... 24

4.7 Certificate Re-Key ..... 25

    4.7.1 *CIRCUMSTANCES FOR CERTIFICATE RE-KEY* ..... 25

    4.7.2 *WHO CAN REQUEST A CERTIFICATE RE-KEY* ..... 25

    4.7.3 *PROCESSING CERTIFICATE RE-KEYING REQUESTS* ..... 25

    4.7.4 *NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER* ..... 25

    4.7.5 *CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE* ..... 25

    4.7.6 *PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA* ..... 25

    4.7.7 *NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES* ..... 25

4.8 Certificate Modification ..... 26

4.9 Certificate Revocation and Suspension ..... 26

    4.9.1 *CIRCUMSTANCE FOR REVOCATION OF A CERTIFICATE* ..... 26

    4.9.2 *WHO CAN REQUEST REVOCATION OF A CERTIFICATE* ..... 27

    4.9.3 *PROCEDURE FOR REVOCATION REQUEST* ..... 27

    4.9.4 *REVOCATION REQUEST GRACE PERIOD* ..... 28

    4.9.5 *TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST* ..... 28

    4.9.6 *REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES* ..... 28

    4.9.7 *CRL ISSUANCE FREQUENCY* ..... 28

    4.9.8 *MAXIMUM LATENCY OF CRLS* ..... 28

    4.9.9 *ONLINE REVOCATION CHECKING AVAILABILITY* ..... 28

    4.9.10 *ONLINE REVOCATION CHECKING REQUIREMENTS* ..... 28

    4.9.11 *OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE* ..... 28

    4.9.12 *SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE* ..... 28

    4.9.13 *CIRCUMSTANCES FOR SUBSCRIBER CERTIFICATE SUSPENSION* ..... 29

    4.9.14 *WHO CAN REQUEST SUSPENSION* ..... 29

    4.9.15 *PROCEDURE FOR SUSPENSION REQUEST* ..... 29

    4.9.16 *LIMITS ON SUSPENSION PERIOD* ..... 29

    4.9.17 *CIRCUMSTANCES FOR TERMINATING SUSPENDED CERTIFICATES* ..... 29

    4.9.18 *PROCEDURE FOR TERMINATING THE SUSPENSION OF A CERTIFICATE* ..... 30

4.10 Certificate Status Services ..... 30

4.11 End of Subscription ..... 30

4.12 Key Escrow and Recovery ..... 30

    4.12.1 *KEY ESCROW POLICY AND PRACTICES* ..... 30

    4.12.2 *SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES* ..... 30

**5. FACILITY MANAGEMENT AND OPERATIONAL CONTROLS ..... 31**

5.1 Physical Security Controls ..... 31

- 5.1.1 *SITE LOCATION AND CONSTRUCTION*..... 31
- 5.1.2 *PHYSICAL ACCESS*..... 31
- 5.1.3 *POWER AND AIR CONDITIONING*..... 32
- 5.1.4 *WATER EXPOSURE*..... 32
- 5.1.5 *FIRE PREVENTION AND PROTECTION*..... 32
- 5.1.6 *MEDIA STORAGE*..... 32
- 5.1.7 *WASTE DISPOSAL*..... 33
- 5.1.8 *OFF-SITE BACKUP*..... 33
- 5.2 *Procedural Controls* ..... 33
  - 5.2.1 *TRUSTED ROLES*..... 33
  - 5.2.2 *NUMBER OF PERSONS REQUIRED PER TASK*..... 33
  - 5.2.3 *IDENTITY-PROOFING FOR EACH ROLE*..... 33
  - 5.2.4 *SEPARATION OF ROLES*..... 33
- 5.3 *Personnel Controls*..... 34
  - 5.3.1 *BACKGROUND, QUALIFICATIONS, EXPERIENCE AND SECURITY CLEARANCE REQUIREMENTS*.. 34
  - 5.3.2 *BACKGROUND CHECK PROCEDURES*..... 34
  - 5.3.3 *TRAINING REQUIREMENTS*..... 34
  - 5.3.4 *RETRAINING FREQUENCY AND REQUIREMENTS* ..... 34
  - 5.3.5 *JOB ROTATION FREQUENCY AND SEQUENCE*..... 34
  - 5.3.6 *SANCTIONS FOR UNAUTHORIZED ACTIONS*..... 34
  - 5.3.7 *CONTRACTING PERSONNEL REQUIREMENTS*..... 34
  - 5.3.8 *DOCUMENTATION SUPPLIED TO PERSONNEL* ..... 35
- 5.4 *Audit Logging Procedures*..... 35
  - 5.4.1 *TYPES OF EVENTS RECORDED*..... 35
  - 5.4.2 *FREQUENCY OF PROCESSING DATA* ..... 36
  - 5.4.3 *RETENTION PERIOD FOR SECURITY AUDIT DATA*..... 36
  - 5.4.4 *PROTECTION OF SECURITY AUDIT DATA*..... 36
  - 5.4.5 *SECURITY AUDIT DATA BACKUP PROCEDURES*..... 36
  - 5.4.6 *SECURITY AUDIT COLLECTION SYSTEM (INTERNAL OR EXTERNAL)*..... 36
  - 5.4.7 *NOTIFICATION TO EVENT-CAUSING SUBJECT*..... 36
  - 5.4.8 *VULNERABILITY ASSESSMENTS*..... 37
- 5.5 *Records Archival* ..... 37
  - 5.5.1 *TYPES OF EVENTS ARCHIVED* ..... 37
  - 5.5.2 *RETENTION PERIOD FOR ARCHIVE*..... 37
  - 5.5.3 *PROTECTION OF ARCHIVE* ..... 37
  - 5.5.4 *ARCHIVE BACKUP PROCEDURES*..... 37
  - 5.5.5 *REQUIREMENTS FOR TIME-STAMPING OF RECORDS*..... 38
  - 5.5.6 *ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)* ..... 38
  - 5.5.7 *PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION*..... 38
- 5.6 *Key Changeover*..... 38
- 5.7 *Compromise and Disaster Recovery*..... 38
  - 5.7.1 *INCIDENT AND COMPROMISE HANDLING PROCEDURES*..... 38
  - 5.7.2 *COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED*..... 38
  - 5.7.3 *CA PRIVATE KEY COMPROMISE RECOVERY PROCEDURES*..... 38
  - 5.7.4 *BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER*..... 38
- 5.8 *CA or RA Termination* ..... 39
  - 5.8.1 *CA TERMINATION*..... 39
  - 5.8.2 *RA TERMINATION*..... 40
- 6. TECHNICAL SECURITY CONTROLS ..... 41**
  - 6.1 *Key Pair Generation and Installation*..... 41
    - 6.1.1 *KEY PAIR GENERATION* ..... 41
    - 6.1.2 *PRIVATE KEY DELIVERY TO SUBSCRIBER*..... 41
    - 6.1.3 *PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER*..... 41
    - 6.1.4 *CA PUBLIC KEY DELIVERY TO SUBSCRIBERS AND RELYING PARTIES*..... 42
    - 6.1.5 *KEY SIZES*..... 42
    - 6.1.6 *PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING* ..... 42

- 6.1.7 *KEY USAGE PURPOSES*.....42
- 6.2 Private Key Protection and Crypto-Module Engineering Controls .....43
  - 6.2.1 *CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS* .....43
  - 6.2.2 *CA PRIVATE KEY MULTI-PERSON CONTROL*.....43
  - 6.2.3 *PRIVATE KEY ESCROW*.....43
  - 6.2.4 *PRIVATE KEY BACKUP*.....43
  - 6.2.5 *PRIVATE KEY ARCHIVAL* .....43
  - 6.2.6 *PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE*.....43
  - 6.2.7 *PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE*.....44
  - 6.2.8 *METHOD OF ACTIVATING PRIVATE KEYS* .....44
  - 6.2.9 *METHODS OF DEACTIVATING PRIVATE KEYS*.....44
  - 6.2.10 *METHODS OF DESTROYING PRIVATE KEYS*.....44
  - 6.2.11 *CRYPTOGRAPHIC MODULE RATING*.....44
- 6.3 Other Aspects of Key Pair Management .....44
  - 6.3.1 *PUBLIC KEY ARCHIVE* .....44
  - 6.3.2 *CERTIFICATE OPERATIONAL PERIODS AND KEY USAGE PERIODS*.....45
- 6.4 Activation Data.....45
  - 6.4.1 *ACTIVATION DATA GENERATION AND INSTALLATION* .....45
  - 6.4.2 *ACTIVATION DATA PROTECTION*.....45
  - 6.4.3 *OTHER ASPECTS OF ACTIVATION DATA*.....45
- 6.5 Computer Security Controls.....45
  - 6.5.1 *SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS*.....45
  - 6.5.2 *COMPUTER SECURITY RATING*.....46
- 6.6 Life-Cycle Security Controls .....46
  - 6.6.1 *SYSTEM DEVELOPMENT CONTROLS* .....46
  - 6.6.2 *SECURITY MANAGEMENT CONTROLS*.....46
  - 6.6.3 *LIFE CYCLE SECURITY RATINGS* .....46
- 6.7 Network Security Controls .....46
- 6.8 Time Stamping.....46
- 7. CERTIFICATE, CRL AND OCSP PROFILES..... 47**
  - 7.1 Certificate Profile .....47
    - 7.1.1 *VERSION NUMBERS* .....47
    - 7.1.2 *CERTIFICATE EXTENSIONS*.....47
    - 7.1.3 *ALGORITHM OBJECT IDENTIFIERS* .....47
    - 7.1.4 *NAME FORMS*.....47
    - 7.1.5 *NAME CONSTRAINTS*.....47
    - 7.1.6 *CERTIFICATE POLICY OBJECT IDENTIFIER* .....47
    - 7.1.7 *USAGE OF POLICY CONSTRAINTS EXTENSION*.....47
    - 7.1.8 *POLICY QUALIFIERS SYNTAX AND SEMANTICS* .....48
    - 7.1.9 *PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION*.....48
  - 7.2 CRL Profile .....48
    - 7.2.1 *VERSION NUMBERS* .....48
    - 7.2.2 *CRL AND CRL ENTRY EXTENSIONS*.....48
  - 7.3 OCSP Profile.....48
    - 7.3.1 *VERSION NUMBER* .....48
    - 7.3.2 *OCSP EXTENSIONS* .....48
- 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS ..... 49**
  - 8.1 Frequency of Audit or Assessments.....49
  - 8.2 Identity and Qualifications of Assessor .....49
  - 8.3 Assessor’s Relationship to Assessed Entity .....49
  - 8.4 Topics Covered By Assessment .....49
  - 8.5 Actions Taken As A Result of Deficiency .....50
  - 8.6 Communication of Results .....50
- 9. OTHER BUSINESS AND LEGAL MATTERS..... 51**

- 9.1 Fees ..... 51
  - 9.1.1 CERTIFICATE ISSUANCE/RENEWAL FEE..... 51
  - 9.1.2 CERTIFICATE ACCESS FEES..... 51
  - 9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEE..... 51
  - 9.1.4 FEES FOR OTHER SERVICES..... 51
  - 9.1.5 REFUND POLICY..... 51
- 9.2 Financial Responsibility..... 51
  - 9.2.1 INSURANCE COVERAGE..... 51
  - 9.2.2 OTHER ASSETS..... 51
  - 9.2.3 INSURANCE/WARRANTY COVERAGE FOR END-ENTITIES..... 51
- 9.3 Confidentiality of Business Information..... 52
  - 9.3.1 SCOPE OF CONFIDENTIAL INFORMATION..... 52
  - 9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION..... 52
  - 9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION..... 52
- 9.4 Privacy of Personal Information ..... 52
  - 9.4.1 PRIVACY PLAN ..... 52
  - 9.4.2 INFORMATION TREATED AS PRIVATE..... 52
  - 9.4.3 INFORMATION NOT DEEMED PRIVATE ..... 52
  - 9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION..... 52
  - 9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION..... 53
  - 9.4.6 DISCLOSURE PURSUANT TO JUDICIAL/ADMINISTRATIVE PROCESS..... 53
  - 9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES ..... 53
- 9.5 Intellectual Property Rights ..... 53
- 9.6 Representations and Warranties ..... 53
  - 9.6.1 GOVERNMENT-CA’S REPRESENTATIONS AND WARRANTIES ..... 53
  - 9.6.2 RA REPRESENTATIONS AND WARRANTIES..... 54
  - 9.6.3 RELYING PARTIES REPRESENTATIONS AND WARRANTIES..... 54
  - 9.6.4 SUBSCRIBER REPRESENTATIONS AND WARRANTIES ..... 54
- 9.7 Disclaimers of Warranties ..... 55
- 9.8 Limitations of Liability..... 56
- 9.9 Indemnities ..... 56
- 9.10 Term and Termination ..... 57
  - 9.10.1 TERM ..... 57
  - 9.10.2 TERMINATION ..... 57
  - 9.10.3 EFFECT OF TERMINATION AND SURVIVAL..... 57
- 9.11 Individual Notices and Communications with Participants..... 57
- 9.12 Amendments ..... 57
  - 9.12.1 PROCEDURE FOR AMENDMENT ..... 57
  - 9.12.2 NOTIFICATION MECHANISM AND PERIOD..... 58
  - 9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED..... 58
- 9.13 Dispute Resolution Procedures..... 58
- 9.14 Governing Law..... 58
- 9.15 Compliance with Applicable Law ..... 58
- 9.16 Miscellaneous Provisions..... 58
  - 9.16.1 ENTIRE AGREEMENT..... 58
  - 9.16.2 ASSIGNMENT ..... 58
  - 9.16.3 SEVERABILITY..... 58
  - 9.16.4 ENFORCEMENT (ATTORNEY FEES/WAIVER OF RIGHTS)..... 59
  - 9.16.5 FORCE MAJEURE ..... 59
- 9.17 Other Provisions ..... 59
  - 9.17.1 FIDUCIARY RELATIONSHIPS ..... 59
  - 9.17.2 ADMINISTRATIVE PROCESSES ..... 59
- APPENDIX- A: CERTIFICATE TYPES ..... 60**
  - 1. NAME ID (MANAGED) ..... 61**
    - 1.1 Name Signing (Non-Repudiation) Certificate..... 61

1.1.1 NAME SIGNING (NON-REPUDIATION) CERTIFICATE POLICY..... 61

1.1.2 NAME SIGNING (NON-REPUDIATION) CERTIFICATE PROFILE ..... 63

1.2 Name Authentication Certificate ..... 65

1.2.1 NAME AUTHENTICATION CERTIFICATE POLICY..... 65

1.2.2 NAME AUTHENTICATION CERTIFICATE PROFILE ..... 67

1.3 Name Encryption Certificate Profile ..... 69

1.3.1 NAME ENCRYPTION CERTIFICATE POLICY..... 69

1.3.2 NAME ENCRYPTION CERTIFICATE PROFILE ..... 71

**2. EMAIL ID (MANAGED) ..... 73**

2.1 Email Signing (Non-Repudiation) Certificate ..... 73

2.1.1 EMAIL SIGNING (NON-REPUDIATION) CERTIFICATE POLICY..... 73

2.1.2 EMAIL SIGNING (NON-REPUDIATION) CERTIFICATE PROFILE ..... 75

2.2 Email Authentication Certificate..... 78

2.2.1 EMAIL AUTHENTICATION CERTIFICATE POLICY..... 78

2.2.2 EMAIL AUTHENTICATION CERTIFICATE PROFILE ..... 80

2.3 Email Encryption Certificate ..... 82

2.3.1 EMAIL ENCRYPTION CERTIFICATE POLICY..... 82

2.3.2 EMAIL ENCRYPTION CERTIFICATE PROFILE ..... 84

**3. SECURE SITE CERTIFICATE (UNMANAGED) ..... 86**

3.1 Secure Site Certificate Policy ..... 86

3.2 Secure Site Certificate Profile ..... 88

**4. ORGANIZATION SIGNING CERTIFICATE (UNMANAGED) ..... 91**

4.1 Organization Signing Certificate Policy ..... 91

4.2 Organization Signing Certificate Profile ..... 93

**5. YESSER GSN CLIENT AUTHENTICATION CERTIFICATE (UNMANAGED) ..... 96**

5.1 Yesser GSN Client Authentication Certificate Policy (For use by Yesser Only) ..... 96

5.2 Yesser GSN Client Authentication Certificate Profile..... 98

**6. YESSER GSN INTERNAL SECURE SITE CERTIFICATE (UNMANAGED) ..... 100**

6.1 Yesser GSN Internal Secure Site Certificate Policy (For use by Yesser Only) ..... 100

6.2 Yesser GSN Internal Secure Site Certificate Profile..... 102

## 1. INTRODUCTION

The Government of Saudi Arabia has embarked on an ambitious e-transaction program, recognizing 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. Named the National Center for Digital Certification (NCDC), NCDC is created by an act of law and its mandate is stipulated in the Saudi e-Transactions Act and its bylaws.

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

- Government
- Citizens
- Businesses

Government Certification Authority (henceforth referred as Government-CA) is owned by the Ministry of Communication and Information Technology (MCIT). Government-CA 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. The Government-CA is responsible for issuing and managing Digital Certificates to Government employees, entities, non-human subscribers (like Servers and Network Devices) within the Government domain, through Certificate Service Providers (CSPs) within the framework.

The Government-CA is hosted in the National Center for Digital Certification - Shared Services Center (NCDC-SSC) which is responsible for managing Government-CA operations as per the agreed service levels.

This CP shall define the policies by which the Government-CA 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 NCDC Glossary section which can be found at <http://www.ncdc.gov.sa>.

### 1.1 OVERVIEW

This CP defines a high level of trust and assurance for use by all Government-CA PKI participants.

Assurance level is defined as 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,
- Security provided by the PKI itself.

The certificate types supported by Government-CA 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 advice to subscriber and any Relying Party.

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

Any use of or reference to this CP outside the context of the Government-CA 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 CPS and NCDC Operations Policies and Procedures.

As described in this CP, the Government-CA 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. Any application for Digital Certificates or reliance on validation services of the Government-CA 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 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 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 CP states what assurance can be placed in a certificate issued by Government-CA to subscriber participating in the Saudi National PKI. The Certificate Practice Statement (CPS) states how Government-CA 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 as governed by this CP and related documents which describe NCDC requirements and use of Certificates.

### **1.1.3 INTERACTION WITH OTHER PKIS**

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

### **1.1.4 SCOPE**

This CP applies to all certificates issued by the Government-CA. The Government-CA is a subordinate CA in the Saudi National PKI hierarchy, maintained and operated by NCDC in an online environment for issuance and management of Subscriber certificates and revocation lists. More specifically, the Government-CA issues Subscriber (human, device or entity) certificates and certificates for its CSPs.

## 1.2 DOCUMENT NAME AND IDENTIFICATION

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

OID: 2.16.682.1.101.5000.1.3.1.1.1

Please refer to the latest OID Allocation document available on <http://www.ncdc.gov.sa>.

## 1.3 PKI PARTICIPANTS

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

### 1.3.1 GOVERNMENT-CA POLICY AUTHORITY (GOVERNMENT-CA PA)

Government CA Policy Authority (Government-CA PA) is responsible for the governance of the Government-CA. Its members are appointed by NCDC and shall include NCDC representatives and a subset of policy administrators from various Government CSPs. Its tasks include:

- Ensuring the operation of the Government-CA comply with the requirements of the Government-CA CP, PDS, CPS and NCDC Operations Policies and Procedures.
- Review and approve the Subscriber Agreement, Relying Party Agreement and other related Agreements based on the Government-CA'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.
- Act as liaison with NCDC.

### 1.3.2 GOVERNMENT CERTIFICATION AUTHORITY (GOVERNMENT-CA)

The term CA refers to any entity approved by NCDC to join the Saudi National PKI, directly under the Saudi National Root-CA and issue certificates and map to one of the policy OIDs listed in NCDC OID Allocation table, which can be found at <http://www.ncdc.gov.sa>. CAs will issue subscriber certificates, OSCP responder certificates and other certificates required by PKI components. CAs, acting on behalf of CSPs, will issue certificates to Subscribers in accordance with their CSP 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 type they will issue and determine the level of warranties and liabilities.

A Government-CA is responsible for:

- Control over the designation of RAs.
- Control over the designation of CSPs.
- 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 CSPs.
- Assist in audits conducted by or on behalf of NCDC.
- Performance of all aspects of the services, operations and infrastructure related to Government-CA.

### **1.3.3 CERTIFICATION SERVICE PROVIDER (CSP)**

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

The CSP comprise of Policy Administrator (PA) and Registration Authority (RA).

#### **1.3.3.1 Policy Administrator (CSP PA)**

Policy Administrator (PA) is responsible for the governance of the CSP. These Policy Administrators are located at various Government CSPs.

#### **1.3.3.2 Registration Authority (RA)**

Government-CA, subject to the approval of NCDC, shall designate specific CSPs 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 CSP 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 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 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 CP and CPS including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements,
- Follow NCDC Privacy policy in accordance with Government-CA CP and CPS and applicable RA Agreement.

### **1.3.4 TRUSTED AGENT**

Trusted Agents (TAs) can perform the identity proofing duties of an RA when authorised to do so by a PA.

TAs are obligated to operate in accordance with the TA Agreement, Government-CA CP, CPS and NCDC Operations Policies and Procedures.

### **1.3.5 SUBSCRIBERS**

Subscribers are individuals (end users), entities (organizations) or devices 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 CP.

### **1.3.6 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. 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 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 CP if:

- The certificate has been used for the purpose for which it has been issued, as described in the Government-CA 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;
- 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.

### **1.3.7 DEVICE SPONSOR**

The Device Sponsor shall serve as the representative of a Device to a CSP in order to register the device as a Subscriber with the Government-CA. The requirements for device Sponsors in the Government-CA are set forth under [3.2.3.2](#).

### **1.3.8 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 may make their Certificate status information available through an OCSP responder in addition to any other mechanisms they wish to employ. The Government-CA 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

Government-CA 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),
- Authentication certificates, where certificates are used to identify/authenticate the subscriber to services and applications.

Government-CA 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 CSP.

#### 1.4.1.1 Certificate Issued to Employees

Certificates issued from Government-CA to the 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 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

A Server certificate is issued to a Government organization whose existence is recognized by the laws of Saudi Arabia (the "Subscriber Organization"); and that wishes to have a certificate issued in a server name owned by that organization.

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 [3.2.3.2](#).

These certificates are generally used for secure SSL/TLS sessions.

#### **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 shall not be liable for any claims arising from such use.

### **1.5 POLICY ADMINISTRATION**

#### **1.5.1 ADMINISTRATION ORGANIZATION**

This CP is administered by Government-CA PA (see section [1.3.1](#)).

#### **1.5.2 CONTACT PERSON**

Queries regarding Government-CA CP shall be directed at:

Email: [info@ncdc.gov.sa](mailto:info@ncdc.gov.sa)

Telephone: +966 1 4522197

Fax: +966 1 4522034

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

#### **1.5.4 CPS APPROVAL**

Changes or updates to the Government-CA 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 Policy Authority approval. Procedure for CPS approval and amendments are covered under section [9.12.1](#) of the Government-CA CPS document.

### **1.6 DEFINITIONS AND ACRONYMS**

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

## **2. PUBLICATION AND REPOSITORY RESPONSIBILITIES**

### **2.1 REPOSITORIES**

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

NCDC-SSC operates repositories to support operations on a 24x7 basis and replicates Government-CA issued certificates, CRLs and Authority Revocation List's (ARL's) to additional 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.
- The availability of the information as required by the certificate information posting and retrieval stipulations of this CP and Government-CA CPS.
- 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 shall publish in the appropriate repository: CA Certificates, subscriber Encryption Certificates, and CRLs as described in the same section in the CPS.

Government-CA 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 PKI Participants at NCDC website <http://www.ncdc.gov.sa>. This web site is the only source for up-to-date documentation and Government-CA reserves the right to publish newer versions of the documentation without prior notice.

Additionally, Government-CA will publish an approved, current and digitally signed version of the Government-CA CP and its PDS.

NCDC Public LDAP directory and NCDC website (<http://www.ncdc.gov.sa>) are the only authoritative sources for:

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

### **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 are published promptly following their generation and issue. 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 PA and NCDC.

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

### **2.4 ACCESS CONTROLS ON REPOSITORIES**

Certificates and certificate status information in the repository shall be made available to Saudi National PKI Participants and other parties on a 24X7 basis as determined by the applicable agreements and NCDC Privacy Policy, and subject to routine maintenance.

The Government-CA will 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.

The controls employed by NCDC-SSC shall prevent unauthorized persons from adding, deleting or modifying repository entries. Access restrictions shall be implemented on directory search to prevent misuse and unauthorized harvesting of 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 Government-CA is approved by the Saudi National Root-CA, while Government-CA approves RAs and CSPs. The subscriber's name is approved by CSPs.

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

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

The certificate types supported by Government-CA are covered in Certificate Types under [Appendix-A](#).

Pilot/Test CSPs are identified by including the word "TEST" in the CSP name which is included in the subject DN as an Organizational Unit. Thus Certificates issued by Pilot/Test CSPs 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**

Government-CA may issue anonymous or pseudonymous certificates pursuant to the approval of NCDC.

##### **3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS**

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

##### **3.1.5 UNIQUENESS OF NAMES**

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

### **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, CSPs, 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 shall be resolved as per NCDC Dispute Resolution Policy. The Government-CA PA is responsible for ensuring name uniqueness through its CSPs.

The Government-CA shall have the right to revoke a Certificate upon receipt of a properly authenticated order from NCDC, a CSP, 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.

Government-CA may carry out the central key generation service on behalf of the Subscriber. The Government-CA will generate the keys in a trustworthy system and environment and ensure that the Private Key is not tampered with. The Private Key together with the certificate are delivered to the applicant in a secure manner after identity verification.

### **3.2.2 AUTHENTICATION OF ISSUER IDENTITY**

Entities wishing to join Saudi National PKI hierarchy or cross certify with the Saudi National Root-CA shall be authenticated in accordance with NCDC specifications and requirements. In all cases, NCDC 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 IDENTITY-PROOFING OF INDIVIDUAL IDENTITY**

#### **3.2.3.1 Identity-Proofing of End User Subscribers**

The CSP will ensure that the Applicant's identity information is verified. Minimal procedures for RA authentication of Subscribers are described further in the Government-CA CPS and respective verification process applicable to specific certificate types is provided in [Appendix-A](#) of this document, which is mandated.

#### **3.2.3.2 Identity-Proofing of Device Subscribers**

If the Certificate subject is a device, then the device shall have a sponsor authorized by the device owner to apply for a certificate. The Government-CA will authenticate, through an approved CSP, the identity of the sponsor applying for the device Certificate. Respective verification process applicable to specific certificate types is provided in [Appendix -A](#) of this document, which is mandated.

### **3.2.3.3 Identity-Proofing of Organizational Entities**

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

For RA certificate under CSP the request will contain the following information as a minimum:

- RA Details (Full Name, ID details, email address, phone)
- Requester Organization Information and address
- Subject of RA (DN) (optional)
- CSP Approval

The request will be supported with an Identity Proof.

NCDC 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, unless specifically mentioned in the Certificate Types section in [Appendix-A](#).

### **3.2.5 CRITERIA OF 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 using their current Authentication Keys.

For routine re-key of RA Certificate refer to NCDC Level One CA Operations Policies and Associated Procedures section 8.

For re-key of a Government-CA, a representative shall provide proper information to authorise the request.

### **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 described in section [3.2.3](#) to obtain a new certificate.

If Government-CA certificate is revoked for any reason, a representative of the Government-CA shall provide sufficient information to proof his authorization for re-key and NCDC shall

re-assess, whether the requirements listed in section [3.2.2](#) are still valid, before a re-keying is initiated.

### **3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS**

Prior to the revocation of a Certificate, a Government-CA 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. The CSP 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.
- Transmit to the Government-CA a confirmation that the Applicant has met the authentication requirements and the information which is to appear in the Certificate.

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

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

#### **4.1.1 SUBMISSION OF CERTIFICATE APPLICATION**

Subscriber certificate applicants, including those applying for a device or entity certificate, will follow the application process specified in section [3.2.3](#) and the Subscriber Agreement.

#### **4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES**

##### **4.1.2.1 Subscribers**

Subscribers follow the procedures published by the CSPs for certificate application.

##### **4.1.2.2 CSP Certificates**

An entity wishing to become CSP under the Government-CA shall agree to the terms of the CSP Agreement as part of the application process. The CSP 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 Agreement, Relying Party or RA/LRA/TA Agreement.

### **4.2 CERTIFICATE APPLICATION PROCESSING**

#### **4.2.1 PERFORMING IDENTITY-PROOFING FUNCTIONS**

CSPs shall perform identification and authentication of all required Subscriber information as described in section [3.2](#) of this CP.

#### **4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS**

The CSP 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 the Subscribers Agreement and outlined in section [3.2](#).

The CSP will reject a certificate application if:

- Identification and authentication of all required Subscriber information as described in the Subscribers Agreement cannot be completed.
- The Subscriber fails to furnish supporting documentation upon request.
- The Subscriber fails to respond to notices within a specified time.
- The CSP believes that issuing a certificate to the Subscriber may bring the Government-CA 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 CSP, the CSP shall ensure that its RA which is applying for certification meets the entitlement requirements for RA certification. Detailed procedure is described in NCDC Level One CA Operations Policies and Associated Procedures section 7.

The application process for CSPs under Government-CA would be as per the Government CSP Joining Process and NCDC shall decide on the acceptance or rejection of the CSP application request based on fulfillment of requirements.

#### **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 CSPs receive a request for a Certificate, Certificate is not issued before the applicant accepts the terms of a Subscriber Agreement, successfully completes the application form and gets approval from the Government-CA.

Following successfully completion of the registration process, the Government-CA will 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 OF CERTIFICATE ISSUANCE**

The Government-CA shall notify Subscribers, either directly or through the CSP that they have created the Subscribers Certificate and provide Subscribers with access to the Certificates by notifying them, using a secure method, that their Certificates are available.

## **4.4 CERTIFICATE ACCEPTANCE**

### **4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE**

Certificate acceptance is governed by the agreements set out between the CSP and Applicants, any requirements imposed by Government-CA 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**

NCDC shall be notified upon the issuance of Government-CA 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, Government-CA CPS and applicable laws. Subscribers shall protect their Private Keys from access by any other party and shall notify the CSP 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 the RP relies on information provided by the Government-CA 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, the Government-CA CP and CPS. The RP is solely responsible for deciding whether or not to rely on the information in a certificate provided by Government-CA. 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 issued certificates.

## **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 CAN REQUEST A CERTIFICATE RE-KEY**

In accordance with the conditions specified in section [4.7.1](#), Certificate re-key may be requested by:

- the Government-CA 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**

See section [3.3.1](#).

### **4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER**

Notification of issuance of a re-keyed certificate to the Subscriber is in accordance with section [4.3.2](#).

### **4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE**

See section [4.4.1](#).

### **4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA**

See section [4.4.2](#).

### **4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES**

See section [4.4.3](#).

## 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 CP does not support other forms of Certificate modification.

## 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 CSP 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 NCDC to the subscriber's registered email address.),
- 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 OF A CERTIFICATE

A Certificate Authority shall revoke Certificates 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;
- NCDC suspects or determines that revocation of a Certificate is in the best interest of the integrity of NCDC;
- The Government-CA 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 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.
- If Subscribers, Relying Parties and other third parties suspect Secure Site Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA shall do the appropriate investigation before taking any action on the request through respective CSP.
- Subscriber or other authorized agent asks for his/her Certificate to be revoked.

- CSP to revoke the certificate of the subscriber, if he/she is no longer part of the organisation.
- The CSP's Agreement or the Registration Authority's Agreement has been terminated.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on a CRL and/or specified as revoked by an OCSP Responder.

Government-CA shall publicly disclose the instructions through a readily accessible online means regarding Secure Site Certificate problem reporting.

#### **4.9.2 WHO CAN REQUEST REVOCATION OF A CERTIFICATE**

The following entities can request revocation of a certificate:

- NCDC can request the revocation of any certificates issued by any CA participating in the Saudi National PKI,
- The Government-CA PA can request the revocation of any certificates issued under its authority,
- The Government-CA can request the revocation of any RA or LRA certificates,
- A CSP, 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.
- A legal, judicial or regulatory agency in Saudi Arabia, can request certificate revocation, within applicable laws and in coordination with NCDC.

Government-CA shall begin investigation of a Secure Site Certificate Problem Report within twenty-four hours of receipt, and decide whether revocation or other appropriate action is warranted based on the nature of the problem reported.

Government-CA shall maintain a continuous 24x7 ability to respond internally to a high-priority Secure Site Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

If any request for revocation cannot be resolved, the request is subject to the Dispute Resolution process described in NCDC 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 NCDC Level One CA Operations Policies and Associated Procedures section 9.

The CSPs issuing Secure Site Certificate shall maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries and provide a process for Subscribers to request revocation of their own Certificates.

#### **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***

Government-CA 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 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 OF 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 CHECKING AVAILABILITY***

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

#### **4.9.10   *ONLINE REVOCATION CHECKING REQUIREMENTS***

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

#### **4.9.11   *OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE***

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

#### **4.9.12   *SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE***

Government-CA will seek to inform subscribers and any relevant relying parties of any potential or actual CA key compromises using any means of communications deemed appropriate.

#### **4.9.13 CIRCUMSTANCES FOR SUBSCRIBER CERTIFICATE SUSPENSION**

The Government-CA 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:

- NCDC 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 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.
- 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 NCDC Level One CA Operations Policies and Associated Procedures section 10.

#### **4.9.16 LIMITS ON SUSPENSION PERIOD**

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

#### **4.9.17 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.

#### **4.9.18**    *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 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**

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

#### **4.11**    **END OF SUBSCRIPTION**

No stipulation.

#### **4.12**    **KEY ESCROW AND RECOVERY**

When data-encryption is supported, the Government-CA must maintain a backup of the private decryption keys to support accessing data encrypted with an unavailable Key. Additionally, in this case, key escrow functionality must be available to provide authorized third parties with the capability to decrypt data encrypted by a certain key. Access to the Key Escrow shall be subject to proper authorization.

##### **4.12.1**    *KEY ESCROW POLICY AND PRACTICES*

The policies and practices for key escrow and recovery will be defined by the issuing CA, applicable Agreements and NCDC Key Escrow Policy.

Digital Signature private keys and authentication private keys shall not be escrowed.

##### **4.12.2**    *SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES*

Subscriber authentication private keys shall not be escrowed.

## **5. FACILITY MANAGEMENT AND OPERATIONAL CONTROLS**

### **5.1 PHYSICAL SECURITY CONTROLS**

NCDC operates the Saudi National Root-CA and other approved CAs, Repositories and OCSP Responder at NCDC-SSC, with appropriate physical and procedural access controls for all hardware and software sub-systems used in the issuance and revocation of certificates. NCDC limits access to functions critical to registration and certificate to personnel in Trusted Roles (see section [5.2.1](#) of this CP).

The Government-CA is collocated in NCDC-SSC and follows the physical security requirements specified as below:

- 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,
- Maintain and periodically inspect access logs.

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

A security check of the facility housing the CAs equipment shall occur on a regular basis. NCDC-SSC facility shall never leave unattended.

#### **5.1.1 SITE LOCATION AND CONSTRUCTION**

The location and construction of the facility housing the Saudi National Root-CA and other approved CAs, NCDC-SSC, equipment is 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, provides robust protection against unauthorized access to the CA equipment and records.

#### **5.1.2 PHYSICAL ACCESS**

NCDC-SSC systems are protected by seven tiers of physical security, with access to the lower tier required before gaining access to the higher tier. Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of two factor biometric authentication. Unescorted personnel, including un-trusted employees or visitors, are not allowed into such secured areas.

NCDC has implemented policies and procedures to ensure that the physical environments in which the Government-CA systems are installed maintain a high level of security:

- NCDC-SSC systems are installed in a secure facility that is isolated from outside networks, with all access controlled;
- NCDC-SSC is separated into a series of progressively secure areas; and

- The entrances and exits from the secure areas are under constant video surveillance and all systems that provide authentication, as well as those that record entry, exit and network activity, are in secured areas.

The security techniques employed are designed to resist a large number and combination of different forms of attack. The mechanisms NCDC-SSC uses include:

- Perimeter alarms
- Closed circuit television
- Two-factor authentication using Biometrics and dual mechanical rotary locks
- Mantraps
- Radio frequency attenuation shielding and reinforced walls
- Motion detectors
- Human guards
- All the Networking and systems components including the certification components are installed in secure Data cabinets with pin locks from both sides.

To prevent tampering, cryptographic hardware is stored in a most secure area of NCDC-SSC, with access limited to authorized personnel.

NCDC uses human guards to continually monitor the facility housing the CA equipment on a 7x24x365 basis. NCDC-SSC facility is never left unattended.

The security mechanisms employed are commensurate with the level of threat in the equipment environment.

### **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 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 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 NCDC 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. The following are the trusted roles for Government-CA:

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

### **5.2.2 NUMBER OF PERSONS REQUIRED PER TASK**

NCDC 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 section [5.2.1](#). 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 of the CA certificate signing Private Key shall require actions by at least two individuals.

### **5.2.3 IDENTITY-PROOFING 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 SEPARATION OF ROLES**

Individual CA personnel are specifically designated to the five roles defined in section [5.2.1](#) of this CP. The Government-CA will ensure that no individual shall be assigned more than one Trusted Role.

## **5.3 PERSONNEL CONTROLS**

### **5.3.1 BACKGROUND, QUALIFICATIONS, EXPERIENCE AND SECURITY CLEARANCE REQUIREMENTS**

All persons filling trusted roles are selected on the basis of skills, loyalty, trustworthiness, and integrity and holder of CA Master trusted roles must be 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 Government-CA CPS. While performing any critical operation one of the trusted roles should be held by the Saudi citizen.

### **5.3.2 BACKGROUND CHECK PROCEDURES**

Background check procedures are described in the CPS and demonstrate that requirements set forth in section [5.3.1](#) are met.

### **5.3.3 TRAINING REQUIREMENTS**

The Government-CA 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 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 are 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 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**

NCDC 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 CONTRACTING PERSONNEL REQUIREMENTS**

Contractor personnel employed to perform functions pertaining to the CA shall be under adequate supervision and perform only assigned tasks.

### **5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL**

Government-CA will 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, and other associated components. The security audit logs for each auditable event defined in this section are maintained in accordance with Retention period for archive, section [5.5.2](#).

### **5.4.1 TYPES OF EVENTS RECORDED**

The Government-CA PA shall ensure recording in audit log files all events relating to the security of the CA system hosted in NCDC-SSC. 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 are required to be processed in accordance with NCDC Audit Policy.

#### **5.4.3     *RETENTION PERIOD FOR SECURITY AUDIT DATA***

The Government-CA 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 SECURITY AUDIT DATA***

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

#### **5.4.5     *SECURITY AUDIT DATA BACKUP PROCEDURES***

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

#### **5.4.6     *SECURITY AUDIT COLLECTION SYSTEM (INTERNAL OR EXTERNAL)***

The audit collection system is detailed in NCDC Audit 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 for its CA, RA and other systems hosted in NCDC-SSC.

Government-CA 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 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 EVENTS 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 are established in accordance with applicable regulatory guidance, laws, Agreements, and as specified by the Government-CA PA. NCDC's minimum retention period for archive data is established at 10 years.

The Government-CA shall ensure that CSPs 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 NCDC, Government-CA 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 NCDC Operations Policies and procedures.

### **5.5.7     *PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION***

As specified in NCDC Operations Policies and Procedures.

## **5.6     KEY CHANGEOVER**

The CA system utilized by the Government-CA supports key rollover, allowing CA keys to be changed periodically as required to minimize risk to the integrity of the Government-CA. Once changed the new key is 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***

If the Government-CA 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 NCDC Operations Policies and Procedures 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 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     *CA PRIVATE KEY COMPROMISE RECOVERY PROCEDURES***

As specified in NCDC Operations Policies and Procedures.

### **5.7.4     *BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER***

NCDC has developed robust Business Continuity Management System for critical PKI services to provide the minimum acceptable level of assurance to its subscriber for service availability.

All NCDC critical infrastructure equipment at the primary site (NCDC-SSC) have built-in hardware fault-tolerance, and configured to be highly available with auto-failover switching.

NCDC currently maintains copies of backup media and infrastructure system software, which include but are not limited to: PKI services related critical data; database records for all certificates issued and audit related data, at its offsite business continuity and disaster recovery storage facilities.

NCDC Business Continuity Management System (BCMS) demonstrates the capability to restore or recover critical PKI services at the primary site within twenty four (24) hours in the event of service(s) non-availability.

Business Continuity Management components at NCDC are being regularly tested, verified, and updated to be operational to address crisis situation in the event of a disruption. For security reasons details of these plans are not publicly available.

NCDC business continuity plan includes:

- Conditions for activating the plan;
- Emergency procedures;
- Fall-back procedures;
- Resumption procedures;
- A maintenance schedule for the plan;
- Awareness and education requirements;
- The responsibilities of the individuals;
- Recovery time objective (RTO);
- Regular testing of contingency plans;
- The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
- Acceptable system outage and recovery time;
- Procedure/frequently of backup copies for essential business information and software are taken; and
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

NCDC has developed recovery plans to mitigate the effects of any kind of natural, man-made or equipment failure related disaster.

NCDC is in the process of implementing an alternate recovery site as per industry standards to provide full recovery of critical PKI services within one week following a disaster at the primary site. NCDC Business Continuity Policy contains further details.

## **5.8 CA OR RA TERMINATION**

### **5.8.1 CA TERMINATION**

No stipulation.

### **5.8.2 RA TERMINATION**

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

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 CSP.

NCDC 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.

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 unauthorised 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.

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

Government-CA 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 key pair is generated in pre-planned Key Generation Ceremony in accordance with the requirements of NCDC. 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 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).

#### **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 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 SUBSCRIBERS AND RELYING PARTIES**

The Government-CA will 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. All FIPS-approved signature algorithms shall be considered acceptable. If NCDC 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 key lengths as per NCDC standard for minimum key sizes are;

- Government-CA 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. The use of a specific key is determined by the key usage extension in the X.509 certificate. Government-CA 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 NCDC shall comply with FIPS-PUB 140-2 "Security Requirements for Cryptographic Modules".

### **6.2.2 CA PRIVATE KEY MULTI-PERSON CONTROL**

Using of any CA Private signing keys shall require action by multiple persons. Government-CA keys can only be accessed on the physical and logical level by adhering to '2 out of 5' control, meaning that 2 of the 5 persons shall present.

### **6.2.3 PRIVATE KEY ESCROW**

Subscriber decryption keys may be escrowed by the issuing CA. Policies and practices for the subscriber decryption private key escrow and recovery are described in NCDC Key Escrow.

### **6.2.4 PRIVATE KEY BACKUP**

#### **6.2.4.1 Backup of CA Signing Private Key**

Government-CA 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 signing Private Key backup shall be detailed in NCDC Operations Policies and Procedures.

#### **6.2.4.2 Backup of Subscriber Private Keys**

Subscriber's Decryption Keys shall be backed up. Subscriber's signing Private Keys and authentication Private keys shall not be backed up.

### **6.2.5 PRIVATE KEY ARCHIVAL**

Government-CA 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 detailed policies and practices governing key backup, archiving and escrow and recovery are detailed in NCDC Key Escrow Policy.

### **6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE**

The cryptographic modules implemented by NCDC are validated to FIPS 140-2 Level 3 ensuring that the CA keys cannot be exported to less secure media.

The Government-CA 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.

### **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 section [6.2.2](#), 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 authorised personnel, as defined in section [6.2.2](#) 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**

CA keys shall be destroyed as per the NCDC CA's Cryptographic Devices and Key Destruction Policy and Associated Procedures.

Private decryption keys must be escrowed in accordance with section [6.2.3](#).

### **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:

<b>Key/Certificate</b>	<b>Key Length in Bits</b>	<b>Maximum Validity Period</b>
Government CA signing key and certificate	2048	120 months
End Entity signing and non-repudiation key and Certificate	2048	36 months
End Entity Encryption Certificate	2048	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 will be secured at the level of the data that the associated cryptographic module is used to protect, and will 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 NCDC-SSC 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

- 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 SECURITY CONTROLS**

### **6.6.1**     **SYSTEM DEVELOPMENT CONTROLS**

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

### **6.6.2**     **SECURITY MANAGEMENT CONTROLS**

The configuration of the Government-CA 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 RATINGS**

No stipulation.

## **6.7**     **NETWORK SECURITY CONTROLS**

The Government-CA 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. The Certificate profile for the Government-CA is described in the Saudi National Root-CA CP.

#### **7.1.1 VERSION NUMBERS**

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

#### **7.1.2 CERTIFICATE EXTENSIONS**

NCDC 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 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 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 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 CRL Profile is as below:

Field	Content	Comment
Version	1	
Algorithm	SHA256withRSA	
Issuer	OU=Government CA O=National Center for Digital Certification C=SA	
This update	<issue date>	
Next update	<issue date + 24 hours>	
AuthorityKeyIdentifier	Issuing CA's Subject Key Identifier	
CRL number	<number>	

**7.2.1 VERSION NUMBERS**

The Government-CA 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 2560.

**7.3.1 VERSION NUMBER**

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 PA shall be responsible for overseeing compliance of the Government-CA, CSPs, Government-CA CP and CPS. NCDC-SSC and Government-CA PA shall ensure that the requirements of the Government-CA CP and CPS and the provisions of applicable Agreements with NCDC are implemented and enforced.

### **8.1 FREQUENCY OF AUDIT OR ASSESSMENTS**

The Government-CA 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. NCDC also performing internal audit at least a quarterly basis against a randomly selected sample for monitor adherence and service quality. Moreover, NCDC may require ad-hoc compliance audits of any CSP's operation to validate that it is operating in accordance with the applicable CP, PDS, CPS Audit Policy and NCDC Operations Policies and Procedures. Similarly, the Government-CA PA has the right to require periodic inspections of its CSPs to validate that the CSPs are operating in accordance with the Government-CA CP and/or CSP agreement. The Government-CA shall internally audit each delegated third party's (CSP, RA & TA) compliance against defined requirements on an annual basis.

### **8.2 IDENTITY AND 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;

NCDC will appoint Qualified Auditor who shall 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 will 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),
- software and information.

The auditor shall provide the Government-CA PA and/or NCDC 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 NCDC or Government-CA PA, as determined by NCDC, 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 NCDC as appropriate.

Where an audited party fails to take remedial action in response to the identified deficiencies, NCDC 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 PA and/or NCDC as applicable.

The Government-CA 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/RENEWAL FEE**

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

#### **9.1.2 CERTIFICATE ACCESS FEES**

Government-CA 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**

Government-CA may charge for other services depending on business needs and subject to NCDC 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 disclaims all liability implicit or explicit due to the use of any certificates issued by the Government-CA which certify public keys of subscribers.

#### **9.2.1 INSURANCE COVERAGE**

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

#### **9.2.2 OTHER ASSETS**

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

#### **9.2.3 INSURANCE/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 NCDC or Government-CA PA. Specific confidentiality requirements for business information are defined in NCDC Privacy Policy and the applicable Agreements.

#### **9.3.1 SCOPE OF CONFIDENTIAL INFORMATION**

Any corporate or personal information held by NCDC, Government-CA, CSPs related to the application and issuance of Certificates is considered confidential and will not be released without the prior consent of the relevant holder, unless required otherwise by law or to fulfill the requirements of this CP, and in accordance with NCDC Privacy policy. NCDC Document Control Policy specifies which documents are considered to be confidential.

#### **9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION**

Such information as specified by the Government-CA PA, NCDC Privacy Policy, NCDC Document Control Policy, NCDC 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 NCDC Privacy Policy and applicable laws and Agreements.

### **9.4 PRIVACY OF PERSONAL INFORMATION**

Any personal identifying information collected by a Government CSPs shall be protected in accordance with NCDC Privacy Policy. The CSPs 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 NCDC 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 is treated as private.

#### **9.4.3 INFORMATION NOT DEEMED PRIVATE**

Information appearing in Subscriber Certificates such as the name, organization affiliation and public key will not be deemed private.

#### **9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION**

Access to Government-CA 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 are defined in the respective Agreements and NCDC Privacy Policy.

#### **9.4.6 DISCLOSURE PURSUANT TO JUDICIAL/ADMINISTRATIVE PROCESS**

Any disclosure shall be handled in accordance with NCDC Privacy Policy.

#### **9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES**

Any disclosure shall be handled in accordance with NCDC Privacy Policy.

### **9.5 INTELLECTUAL PROPERTY RIGHTS**

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

### **9.6 REPRESENTATIONS AND WARRANTIES**

#### **9.6.1 GOVERNMENT-CA'S REPRESENTATIONS AND WARRANTIES**

Government-CA 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 NCDC Operations Policies and Procedures
  - Within applicable agreements, Saudi Law and regulations
- At the time of Certificate issuance; Government-CA implemented procedure for verifying accuracy of the information contained within it before installation and first use;
- Implemented a procedure for reducing the likelihood that the information contained in the Certificate is not misleading.
- Implemented procedures for verifying Device Sponsor requesting the Secure Site Certificate on behalf of the Device as authorized representative and to verify that the applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension.
- Maintaining 24 x 7 publicly-accessible repositories with current information and replicates Government-CA 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 unauthorised use of the private key CA private key is generated using multi-person control "m-of-n" split key knowledge scheme;

- Backing up of the CA signing Private Key is under the same multi-person control as the original Signing Key;
- Keep confidential, any passwords, PINs or other personal secrets used in obtaining authenticated access to PKI facilities and maintain proper control procedures for all such personal secrets;
- 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 NCDC 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 CPS and the RA Agreement.

### **9.6.3 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.
- Determining that such Certificate provides adequate assurances for its intended use.

### **9.6.4 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 CSP, both in the certificate request and verification process defined by the CSP for specific Certificate type to be supplied by the Government-CA;
  - 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 CSPs
  - Notify the CSP in the event of any information in the Certificate is, or becomes, incorrect or inaccurate;
  - Notify the CSP 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 CSP 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 CSP or otherwise inconsistent with the terms of this Subscriber Agreement or the Government-CA 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 CSP 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 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.

## 9.7 DISCLAIMERS OF WARRANTIES

NCDC, 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 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 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 NCDC. The Government-CA 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 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 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 from and against any such liability and costs and claims arising there from.
- The Government-CA will not be liable to any party whatsoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services.
- End-Users and CSPs are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been verified by CSPs or Government-CA.
- 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.
- Certificate Service Providers (CSPs) shall bear the consequences of their failure to perform the Registration Authorities obligations described in the CSP agreement.
- Government-CA 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 CSPs shall indemnify, defend and hold harmless the following parties:

- NCDC, its directors, officers, employees, agents, consultants, and subsidiaries from any and all claims, damages, costs (including, without limitation, attorney's fees), judgments, awards or liability;

- the CSP's own employees, arising from any of the CSP's operations and activities as a CSP, of any entity or services subordinated or outsourced by the CSP;
- any parties relying on the CSP'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 NCDC. 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 CP can be found at: <http://www.ncdc.gov.sa>.

### **9.10.3 EFFECT OF TERMINATION AND SURVIVAL**

Upon termination of this CP, all Government-CA 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 NCDC, PA, Saudi National Root-CA, CSPs, 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 the this CP Certificate assurance level.

## **9.12 AMENDMENTS**

### **9.12.1 PROCEDURE FOR AMENDMENT**

The Government-CA 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 PA and/or NCDC. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change as per NCDC Change Management Policy.

Subject to the approval of NCDC, the Government-CA PA reserves the right to change this CP from time to time. The Government-CA 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 Participants within two weeks of approval. The Government-CA 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 PA shall provide their comments to the Government-CA PA in accordance with NCDC rules. The Government-CA 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 PA and shall only change pursuant to a decision from NCDC.

## **9.13 DISPUTE RESOLUTION PROCEDURES**

The use of certificates issued by the Government-CA is governed by contracts, agreements, and standards set forth by NCDC. 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 NCDC 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 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/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 will be treated according to laws of Kingdom of Saudi Arabia.

#### **9.16.5 FORCE MAJEURE**

The Government-CA 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, or any of its subcontractors, agents, officers, suppliers, employees, partners, principals, or directors to be a partner, Affiliate, trustee, of any Relying Party or any third party, or to create any fiduciary relationship between the Government-CA 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.

#### **9.17.2 ADMINISTRATIVE PROCESSES**

As specified in NCDC Operations Policies and applicable Agreements.

## **APPENDIX- A: CERTIFICATE TYPES**

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

For issuance of a particular certificate type, CSP shall submit request to NCDC. Based on NCDC approval a CSP 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 CSP by NCDC.

## 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	2.16.682.1.101.5000.1.3.1.1.1.1.1
3	Subject	<p>"cn=&lt;English-Firstname&gt; &lt;English-Secondname&gt; &lt;English-Thirdname&gt; &lt;English-Lastname&gt; &lt;Arabic-Lastname&gt; &lt;Arabic-Thirdname&gt; &lt;Arabic-SecondName&gt; &lt;Arabic-FirstName&gt; *, OU=&lt;optional searchbase(s)&gt;,OU = Government CA,O = National Center for Digital Certification, C = SA"</p> <p>* Optional unverified nickname may be added at the end of the CN to achieve uniqueness of the subject.</p>
4	Certificate Profile	See below after the table.
5	Application Usage	<p><b>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.</b></p> <p>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 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.</p> <p>Government- CA issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA issued Name Certificate should honour Key Usage.</p> <p>Following are some of the common usage of the certificate</p> <ul style="list-style-type: none"> <li>• Inter Government correspondence;</li> <li>• Public Information Posting by Authorised Government Personnel;</li> <li>• Departmental Forms Submission;</li> <li>• PKI enabled Application work-flow; and</li> <li>• E Tendering</li> </ul> <p>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 practices, Subscribers agreement and not otherwise prohibited by the law of Saudi Arabia.</p>
6	Verification Process	<ol style="list-style-type: none"> <li>1. Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents.</li> <li>2. The following will be considered valid identity documents: <ul style="list-style-type: none"> <li>• National ID / passport for citizens.</li> <li>• Residence permit / passport for residents.</li> </ul> </li> </ol>

S. No.	Attribute	Name Signing (Non-Repudiation) Certificate
		<p>3. Letter from an authorized party (as prescribed by the CSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process</p> <p>4. 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.</p> <p>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 NCDC-approved <u>signing</u> certificate types.</p>
7	Key Pair Generation and Installation	<p>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.</p> <p><b>All Name ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA CP.</b></p> <p>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).</p>
8	Certificate Issuance Process	<p>Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following:</p> <ul style="list-style-type: none"> <li>• The Subscriber will be present at the RA for face-to-face identity verification</li> <li>• The RA will validate the documents submitted by the subscriber</li> <li>• The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner.</li> <li>• The subscriber will go to the RA customization center</li> <li>• The Subscriber will plug his smart card / USB token into the customization device.</li> <li>• The Subscriber will enter the PIN of the smart card / USB token</li> <li>• The Subscriber will enter reference number and an authorization code to generate keys and download certificates.</li> <li>• The Client Software will generate the Subscriber’s keys securely on his smart card / USB token.</li> <li>• 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.</li> </ul>
9	Key Usage	<p>Name Signing certificate and keys can be used for data integrity, and non-repudiation based on name only.</p>

S. No.	Attribute	Name Signing (Non-Repudiation) Certificate
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	Up to 36months(3years)
12	Key Backup	The CSP 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.

**1.1.2 NAME SIGNING (NON-REPUDIATION) CERTIFICATE PROFILE**

Field / x.509 extension	Value or Value Constant	Critical
<b>Subject</b>	CN = <English FirstName> <English SecondName> <English ThirdName> <English LastName> <Arabic LastName> <Arabic ThirdName> <Arabic SecondName> <Arabic FirstName> * OU=<optional searchbase(s)> OU = Government CA O = National Center for Digital Certification 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
<b>CRL Distribution</b>	e.g. [1]CRL Distribution Point	NO

Field / x.509 extension	Value or Value Constant	Critical
<b>Points</b>	Distribution Point Name: Full Name:  URL=http://web.ncdc.gov.sa/crl/gcapart<n>.crl Directory Address: CN=CRL1 OU=Government CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name:  URL=http://web.ncdc.gov.sa/crl/gcacomb<n>.crl	
<b>Authority Key Identifier</b>	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 (excluding the tag, length, and number of unused bits).	NO
<b>Subject Key Identifier</b>	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
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None	NO
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.1.1.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA Certification Policy and associated documentation available at http://web.ncdc.gov.sa/ is hereby incorporated into your use or reliance on this Certificate.	NO
<b>Authority Information Access</b>	[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	NO

Field / x.509 extension	Value or Value Constant	Critical
	Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name:  URL=http://web.ncdc.gov.sa/certs/gca.crt	
<b>Key Usage</b>	Non Repudiation	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	2.16.682.1.101.5000.1.3.1.1.1.1.2
3	Subject	“cn=<English-Firstname> <English-Secondname> <English-Thirdname> <English-Lastname> <Arabic-Lastname> <Arabic-Thirdname> <Arabic-SecondName> <Arabic-FirstName> * , OU=<optional searchbase(s)>,OU = Government CA,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	<p>Government- CA issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA issued Name Certificate should honour Key Usage.</p> <p>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.</p> <p>Following are some of the common usage of the certificate</p> <ul style="list-style-type: none"> <li>• Inter Government correspondence;</li> <li>• Public Information Posting by Authorized Government Personnel;</li> <li>• Departmental Forms Submission;</li> <li>• PKI enabled Application work-flow; and</li> <li>• E Tendering</li> </ul> <p>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 practices, Subscribers agreement and not otherwise prohibited by law of Saudi Arabia.</p>
6	Verification Process	<ol style="list-style-type: none"> <li>1. Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents.</li> <li>2. The following will be considered valid identity documents:                             <ul style="list-style-type: none"> <li>• National ID / passport for citizens.</li> <li>• Residence permit / passport for residents.</li> </ul> </li> <li>3. Letter from an authorized party (as prescribed by the CSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process</li> <li>4. During the request submission, the identity of the subscriber will be</li> </ol>

S. No.	Attribute	Name Authentication Certificate
		<p>validated by ensuring the authenticity of the subscriber’s identity documentation and matching it with his / her characteristics</p> <p>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 NCDC-approved <u>signing</u> certificate types.</p>
7	Key Pair Generation and Installation	<p>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.</p> <p><b>All Name ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA CP.</b></p> <p>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).</p>
8	Certificate Issuance Process	<p>Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following:</p> <ul style="list-style-type: none"> <li>• The Subscriber will be present at the RA for face-to-face identity verification</li> <li>• The RA will validate the documents submitted by the subscriber</li> <li>• The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner.</li> <li>• The subscriber will go to the RA customization center</li> <li>• The Subscriber will plug his smart card / USB token into the customization device.</li> <li>• The Subscriber will enter the PIN of the smart card / USB token</li> <li>• The Subscriber will enter reference number and an authorization code to generate keys and download certificates.</li> <li>• The Client Software will generate the Subscriber’s keys securely on his smart card / USB token.</li> <li>• 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.</li> </ul>
9	Key Usage	<p>Name Authentication certificate and keys shall be used for authentication of/by name only.</p>
10	Private Key Protection	<p>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.</p> <p>Generation and/or Storage of name authentication private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.</p>

S. No.	Attribute	Name Authentication Certificate
11	Certificate Life Time	Up to 36months(3years)
12	Key Backup	The CSP 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	<p>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.</p> <p>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.</p> <p>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.</p>

**1.2.2 NAME AUTHENTICATION CERTIFICATE PROFILE**

Field / x.509 extension	Value or Value Constant	Critical
<b>Subject</b>	<p>CN = &lt;English FirstName&gt; &lt;English SecondName&gt; &lt;English ThirdName&gt; &lt;English LastName&gt; &lt;Arabic LastName&gt; &lt;Arabic ThirdName&gt; &lt;Arabic SecondName&gt; &lt;Arabic FirstName&gt; *</p> <p>OU=&lt;optional searchbase(s)&gt;</p> <p>OU = Government CA</p> <p>O = National Center for Digital Certification</p> <p>C = SA</p> <p>(Encoding should be in UTF8 only)</p> <p>* Optional unverified nickname may be added at the end of the CN to achieve uniqueness of the subject.</p>	V1 Field
<b>CRL Distribution Points</b>	<p>e.g.</p> <p>[1]CRL Distribution Point                      Distribution Point Name:                      Full Name:                      URL=http://web.ncdc.gov.sa/crl/gcapart&lt;n&gt;.crl                      Directory Address:                      CN=CRL1                      OU=Government CA                      O=National Center for</p>	NO

Field / x.509 extension	Value or Value Constant	Critical
	Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcacomb<n>.crl	
<b>Authority Key Identifier</b>	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 (excluding the tag, length, and number of unused bits).	NO
<b>Subject Key Identifier</b>	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
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None	NO
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.1.1.1.1.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Government CA Certification Policy and associated documentation available at http://web.ncdc.gov.sa/ is hereby incorporated into your use or reliance on this Certificate.	NO
<b>Authority Information Access</b>	[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/gca.crt	NO
<b>Key Usage</b>	Digital Signature	NO
<b>Extended Key Usage</b>	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	2.16.682.1.101.5000.1.3.1.1.1.1.3
3	Subject	<p>"cn=&lt;English-Firstname&gt; &lt;English-Secondname&gt; &lt;English-Thirdname&gt; &lt;English-Lastname&gt; &lt;Arabic-Lastname&gt; &lt;Arabic-Thirdname&gt; &lt;Arabic-SecondName&gt; &lt;Arabic-FirstName&gt; * , OU=&lt;optional searchbase(s)&gt;,OU = Government CA,O = National Center for Digital Certification, C = SA"</p> <p>* Optional unverified nickname may be added at the end of the CN to achieve uniqueness of the subject.</p>
4	Certificate Profile	See below after the table.
5	Application Usage	<p>Government- CA issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA issued Name Certificate should honour Key Usage.</p> <p>The Name Encryption certificate should be used for data encryption.</p> <p>Following are some of the common usage of the certificate</p> <ul style="list-style-type: none"> <li>• Inter Government correspondence;</li> <li>• Public Information Posting by Authorised Government Personnel;</li> <li>• Departmental Forms Submission;</li> <li>• PKI enabled Application work-flow; and</li> <li>• E Tendering</li> </ul> <p>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 practices, Subscribers agreement and not otherwise prohibited by law of Saudi Arabia.</p>
6	Verification Process	<ol style="list-style-type: none"> <li>1. Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents.</li> <li>2. The following will be considered valid identity documents:                             <ul style="list-style-type: none"> <li>• National ID / passport for citizens.</li> <li>• Residence permit / passport for residents.</li> </ul> </li> <li>3. Letter from an authorized party (as prescribed by the CSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process</li> <li>4. 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</li> </ol> <p>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 NCDC-approved <u>signing</u> certificate types.</p>
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.

S. No.	Attribute	Name Encryption Certificate
		<p><b>All Name ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA CP.</b></p> <p>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).</p>
8	Certificate Issuance Process	<p>Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following:</p> <ul style="list-style-type: none"> <li>• The Subscriber will be present at the RA for face-to-face identity verification</li> <li>• The RA will validate the documents submitted by the subscriber</li> <li>• The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner.</li> <li>• The subscriber will go to the RA customization center</li> <li>• The Subscriber will plug his smart card / USB token into the customization device.</li> <li>• The Subscriber will enter the PIN of the smart card / USB token</li> <li>• The Subscriber will enter reference number and an authorization code to generate keys and download certificates.</li> <li>• 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.</li> </ul>
9	Key Usage	Name Encryption certificate and keys shall be used for data encryption.
10	Private Key Protection	<p>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.</p> <p>Storage of name encryption private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.</p>
11	Certificate Life Time	Up to 36months(3years)
12	Key Backup	Only Private Decryption keys are backed up by the Government-CA. 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	<p>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.</p> <p>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.</p>

S. No.	Attribute	Name Encryption Certificate
		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.

**1.3.2 NAME ENCRYPTION CERTIFICATE PROFILE**

Field / x.509 extension	Value or Value Constant	Critical
<b>Subject</b>	CN = <English FirstName> <English SecondName> <English ThirdName> <English LastName> <Arabic LastName> <Arabic ThirdName> <Arabic SecondName> <Arabic FirstName> * OU=<optional searchbase(s)> OU = Government CA O = National Center for Digital Certification 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
<b>CRL Distribution Points</b>	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcapart<n>.crl Directory Address: CN=CRL1 OU=Government CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcacombo<n>.crl	NO
<b>Authority Key Identifier</b>	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
<b>Subject Key Identifier</b>	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

Field / x.509 extension	Value or Value Constant	Critical
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None	NO
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.1.1.1.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA Certification Policy and associated documentation available at http://web.ncdc.gov.sa/ is hereby incorporated into your use or reliance on this Certificate.	NO
<b>Authority Information Access</b>	[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/gca.crt	NO
<b>Key Usage</b>	Key Encipherment	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	2.16.682.1.101.5000.1.3.1.1.1.2.1
3	Subject	<p>“CN = &lt;end-entity’s verified email address&gt;, OU=&lt;optional searchbase(s)&gt;, OU = Government CA, O = National Center for Digital Certification, C = SA”</p> <p><b>Email ID certificates should only be issued to email addresses with domains which are verified to be owned by the respective CSP Organization.</b></p>
4	Certificate Profile	See below after the table.
5	Application Usage	<p><b>If subscriber wants to engage in legal signing he/she is advised to use Email <u>Signing</u> 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.</b></p> <p>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 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.</p> <p>Government- CA issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA issued Email Certificate should honour Key Usage.</p> <p>Following are some of the common usage of the certificate</p> <ul style="list-style-type: none"> <li>• Inter Government correspondence;</li> <li>• Public Information Posting by Authorised Government Personnel;</li> <li>• Departmental Forms Submission;</li> <li>• PKI enabled Application work-flow; and</li> <li>• E Tendering</li> </ul> <p>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 practices, Subscribers agreement and not otherwise prohibited by the law of Saudi Arabia.</p>
6	Verification Process	<ol style="list-style-type: none"> <li>1. Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents.</li> <li>2. The following will be considered valid identity documents:</li> </ol>

S. No.	Attribute	Email Signing (Non-Repudiation) Certificate
		<ul style="list-style-type: none"> <li>• National ID / passport for citizens.</li> <li>• Residence permit / passport for residents.</li> </ul> <ol style="list-style-type: none"> <li>3. Letter from an authorized party (as prescribed by the CSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process</li> <li>4. The domain name for the email address requested on the certificate should be verified to be owned by the issuing CSP organization.</li> <li>5. Email address shall be verified by sending the authorization code on subscriber’s email address; or verified against a CSP-trusted database.</li> <li>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</li> </ol> <p>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 NCDC-approved <u>signing</u> certificate types.</p>
7	Key Pair Generation and Installation	<p>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.</p> <p><b>All Email ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA CP.</b></p> <p>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).</p>
8	Certificate Issuance Process	<p>Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following:</p> <ul style="list-style-type: none"> <li>• The Subscriber will be present at the RA for face-to-face identity verification</li> <li>• The RA will validate the documents submitted by the subscriber</li> <li>• The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner.</li> <li>• The subscriber will go to the RA customization center</li> <li>• The Subscriber will plug his smart card / USB token into the customization device.</li> <li>• The Subscriber will enter the PIN of the smart card / USB token</li> <li>• The Subscriber will enter reference number and an authorization code to generate keys and download certificates.</li> <li>• The Client Software will generate the Subscriber’s keys securely on his smart card / USB token.</li> <li>• The CA will authenticate the Subscriber using the reference number and authorization code and receive the certificate</li> </ul>

S. No.	Attribute	Email Signing (Non-Repudiation) 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 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	Up to 36months(3years)
12	Key Backup	The CSP 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.

**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)> OU = Government CA O = National Center for Digital Certification C = SA (Encoding should be in UTF8 only)	V1 Field

Field / x.509 extension	Value or Value Constant	Critical
<b>Subject Alternative Name</b>	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
<b>CRL Distribution Points</b>	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcapart<n>.crl Directory Address: CN=CRL1 OU=Government CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcacomb<n>.crl	NO
<b>Authority Key Identifier</b>	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
<b>Subject Key Identifier</b>	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
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None	NO
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.1.1.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA Certification Policy and associated documentation available at http://web.ncdc.gov.sa/ is hereby incorporated into your use or reliance on this Certificate.	NO
<b>Authority</b>	[1]Authority Info Access	NO

Field / x.509 extension	Value or Value Constant	Critical
<b>Information Access</b>	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/gca.crt	
<b>Key Usage</b>	Non Repudiation	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	2.16.682.1.101.5000.1.3.1.1.1.2.2
3	Subject	<p>“CN = &lt;end-entity’s verified email address&gt;, OU=&lt;optional searchbase(s)&gt;, OU = Government CA, O = National Center for Digital Certification, C = SA”</p> <p><b>Email ID certificates should only be issued to email addresses with domains which are verified to be owned by the respective CSP Organization.</b></p>
4	Certificate Profile	See below after the table.
5	Application Usage	<p>Government- CA issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA issued Email Certificate should honour Key Usage.</p> <p>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.</p> <p>Following are some of the common usage of the certificate</p> <ul style="list-style-type: none"> <li>• Inter Government correspondence;</li> <li>• Public Information Posting by Authorised Government Personnel;</li> <li>• Departmental Forms Submission;</li> <li>• PKI enabled Application work-flow; and</li> <li>• E Tendering</li> </ul> <p>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 practices, Subscribers agreement and not otherwise prohibited by law of Saudi Arabia.</p>
6	Verification Process	<ol style="list-style-type: none"> <li>1. Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents.</li> <li>2. The following will be considered valid identity documents: <ul style="list-style-type: none"> <li>• National ID / passport for citizens.</li> <li>• Residence permit / passport for residents.</li> </ul> </li> <li>3. Letter from an authorized party (as prescribed by the CSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process</li> <li>4. The domain name for the email address requested on the certificate should be verified to be owned by the issuing CSP organization.</li> <li>5. Email address shall be verified by sending the authorization code on subscriber’s email address; or verified against a CSP-trusted database.</li> <li>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</li> </ol>

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 NCDC-approved <u>signing</u> 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. <b>All Email ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA CP.</b> 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: <ul style="list-style-type: none"><li>• The Subscriber will be present at the RA for face-to-face identity verification</li><li>• The RA will validate the documents submitted by the subscriber</li><li>• The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner.</li><li>• The subscriber will go to the RA customization center</li><li>• The Subscriber will plug his smart card / USB token into the customization device.</li><li>• The Subscriber will enter the PIN of the smart card / USB token</li><li>• The Subscriber will enter reference number and an authorization code to generate keys and download certificates.</li><li>• The Client Software will generate the Subscriber’s keys securely on his smart card / USB token.</li><li>• 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.</li></ul>
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	Up to 36months(3years)

S. No.	Attribute	Email Authentication Certificate
12	Key Backup	The CSP 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	<p>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.</p> <p>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.</p> <p>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.</p>

**2.2.2 EMAIL AUTHENTICATION CERTIFICATE PROFILE**

Field / x.509 extension	Value or Value Constant	Critical
<b>Subject</b>	CN = <end-entity’s verified email address> OU=<optional searchbase(s)> OU = Government CA O = National Center for Digital Certification C = SA (Encoding should be in UTF8 only)	V1 Field
<b>Subject Alternative Name</b>	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
<b>CRL Distribution Points</b>	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcapart<n>.crl Directory Address: CN=CRL1 OU=Government CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point	NO

Field / x.509 extension	Value or Value Constant	Critical
	Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcacomb<n>.crl	
<b>Authority Key Identifier</b>	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
<b>Subject Key Identifier</b>	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
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None	NO
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.1.1.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA Certification Policy and associated documentation available at http://web.ncdc.gov.sa/ is hereby incorporated into your use or reliance on this Certificate.	NO
<b>Authority Information Access</b>	[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/gca.crt	NO
<b>Key Usage</b>	Digital Signature	NO
<b>Extended Key Usage</b>	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	2.16.682.1.101.5000.1.3.1.1.1.2.3
3	Subject	<p>“CN = &lt;end-entity’s verified email address&gt;, OU=&lt;optional searchbase(s)&gt;, OU = Government CA, O = National Center for Digital Certification, C = SA”</p> <p><b>Email ID certificates should only be issued to email addresses with domains which are verified to be owned by the respective CSP Organization.</b></p>
4	Certificate Profile	See below after the table.
5	Application Usage	<p>Government- CA issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA issued Email Certificate should honour Key Usage.</p> <p>The Email Encryption certificate should be used for data encryption.</p> <p>Following are some of the common usage of the certificate</p> <ul style="list-style-type: none"> <li>• Inter Government correspondence;</li> <li>• Public Information Posting by Authorised Government Personnel;</li> <li>• Departmental Forms Submission;</li> <li>• PKI enabled Application work-flow; and</li> <li>• E Tendering</li> </ul> <p>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 practices, Subscribers agreement and not otherwise prohibited by law of Saudi Arabia.</p>
6	Verification Process	<ol style="list-style-type: none"> <li>1. Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents.</li> <li>2. The following will be considered valid identity documents: <ul style="list-style-type: none"> <li>• National ID / passport for citizens.</li> <li>• Residence permit / passport for residents.</li> </ul> </li> <li>3. Letter from an authorized party (as prescribed by the CSP PA) that the Subscriber has been permitted to obtain the Certificate, apart from the face-to-face verification process</li> <li>4. The domain name for the email address requested on the certificate should be verified to be owned by the issuing CSP organization.</li> <li>5. Email address shall be verified by sending the authorization code on subscriber’s email address; or verified against a CSP-trusted database.</li> <li>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</li> </ol> <p>Where a Subscriber/approver have already undergone face-to-face identity and authentication process by an RA to receive a certificate, the</p>

S. No.	Attribute	Email Encryption Certificate
		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 NCDC-approved <u>signing</u> certificate types.
7	Key Pair Generation and Installation	<p>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.</p> <p><b>All Email ID certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA CP.</b></p> <p>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).</p>
8	Certificate Issuance Process	<p>Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following:</p> <ul style="list-style-type: none"> <li>• The Subscriber will be present at the RA for face-to-face identity verification</li> <li>• The RA will validate the documents submitted by the subscriber</li> <li>• The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner.</li> <li>• The subscriber will go to the RA customization center</li> <li>• The Subscriber will plug his smart card / USB token into the customization device.</li> <li>• The Subscriber will enter the PIN of the smart card / USB token</li> <li>• The Subscriber will enter reference number and an authorization code to generate keys and download certificates.</li> <li>• 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.</li> </ul>
9	Key Usage	Email Encryption certificate and keys shall be used for data encryption.
10	Private Key Protection	<p>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.</p> <p>Storage of email encryption private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.</p>
11	Certificate Life Time	Up to 36months(3years)
12	Key Backup	<p>Only Private Decryption keys are backed up by the Government-CA. 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.</p>
13	Asymmetric Key Length	Minimum 2048 bits RSA

S. No.	Attribute	Email Encryption Certificate
14	Certificate Re-key	<p>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.</p> <p>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.</p> <p>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.</p>

**2.3.2 EMAIL ENCRYPTION CERTIFICATE PROFILE**

Field / x.509 extension	Value or Value Constant	Critical
<b>Subject</b>	CN = <end-entity’s verified email address> OU=<optional searchbase(s)> OU = Government CA O = National Center for Digital Certification C = SA (Encoding should be in UTF8 only)	V1 Field
<b>Subject Alternative Name</b>	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
<b>CRL Distribution Points</b>	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcapart<n>.crl Directory Address: CN=CRL1 OU=Government CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcacomb<n>.crl	NO

Field / x.509 extension	Value or Value Constant	Critical
<b>Authority Key Identifier</b>	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
<b>Subject Key Identifier</b>	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
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None	NO
<b>Certificate Policies</b>	<pre>[1]Certificate Policy:     Policy     Identifier=2.16.682.1.101.5000.1.3.1.1.1.1.2.3     [1,1]Policy Qualifier Info:         Policy Qualifier Id=CPS         Qualifier:             http://web.ncdc.gov.sa     [1,2]Policy Qualifier Info:         Policy Qualifier Id=User Notice         Qualifier:             Notice Text= Government CA Certification Policy and associated documentation available at http://web.ncdc.gov.sa/ is hereby incorporated into your use or reliance on this Certificate.</pre>	NO
<b>Authority Information Access</b>	<pre>[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/gca.crt</pre>	NO
<b>Key Usage</b>	Key Encipherment	NO

### 3. SECURE SITE CERTIFICATE (UNMANAGED)

#### 3.1 SECURE SITE CERTIFICATE POLICY

S. No.	Attribute	Secure Site Certificate
1	Policy Name	Secure Site Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.3.1.1.1.1.3.1
3	Subject	<p>“CN = &lt;FQDN for Server or Device&gt;, OU=&lt;optional searchbase(s)&gt;, OU = Government CA, O = National Center for Digital Certification, C = SA”</p> <p><b>** See notes in point 6 of this table.</b></p>
4	Certificate Profile	See below after the table.
5	Application Usage	<p>Secure Site certificates are only issued to servers, such as applications or web servers within the Kingdom of Saudi Arabia. Appropriate use of such certificate(s) is for server authentication and session encryption, and where another web site or device requires high-assurance proof of server/device identity.</p> <p>Certificate(s) issued under this type must not be used for any form of data encryption, except SSL/TLS session encryption.</p>
6	Verification Process	<ol style="list-style-type: none"> <li>1. The Device Sponsor shall serve as the representative of the Device to an RA in order to register the device as a Subscriber with the Saudi PKI</li> <li>2. Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents.</li> <li>3. The following will be considered valid identity documentation: <ul style="list-style-type: none"> <li>• National ID / passport for citizens.</li> <li>• Residence permit / passport for residents.</li> </ul> </li> <li>4. The below should be verified for secure site certificates <ul style="list-style-type: none"> <li>• Letter from the official domain names registrar (CITC) that the Subscriber owns the domain for which the certificate is being requested and has been permitted to obtain the Secure Site Certificate, apart from the face-to-face verification process</li> <li>• Verifying fully qualified domain name or IP address</li> </ul> </li> </ol> <p>Only publicly verifiable Fully Qualified Domain Name (FQDN) or IP Address shall be included in the subject of the certificate.</p> <p><b>** Subject Alternative Names may optionally be added to the certificate. The following rules should be applied for the Subject and the Subject Alternative Name:</b></p> <ul style="list-style-type: none"> <li>- The subject alternative name extension may include ‘Publicly Verifiable Alternative FQDN’ or ‘Public IP Address’ for Server or Device</li> <li>- The subject alternative name extension may include privately-addressable pseudo-domains and hostnames</li> <li>- This CP does not allow to add non-verified details in the Subject Field of the Secure Site certificate</li> <li>- wildcard host or domain names such as ‘*.ncdc.gov.sa’ are not allowed</li> <li>- Private IP addresses as mentioned in RFC 1918 are not allowed to be included in Secure Site Certificates</li> <li>- All public FQDNs inserted in the Subject Alternative Name field should be considered at par with the Subject and should be individually verified</li> </ul>

S. No.	Attribute	Secure Site Certificate
		<ul style="list-style-type: none"> <li>- The Subject Alternative Names field allows the addition of privately-addressable pseudo-domains and hostnames, which can only be used internally within the organization (e.g. webmail.ncdc.local, autodiscover.local, autodiscover, etc.). Government CA or applicable CSP/RA does not confirm privately-addressable pseudo-domains and hostnames and provides no assurances other than that the information was officially submitted by the subscriber or sponsor of the certificate.</li> <li>- Secure Site Certificates including Subject Alternative Names should not be used on servers/devices other than those assigned to the Subject Name.</li> <li>- If the subjectAltName extension is present, its value MUST contain at least one entry and should not be left empty.</li> <li>- If the subjectAltName extension is present, the subject must not be left empty.</li> </ul>
7	Key Pair Generation and Installation	<p>Key Pair generation must be performed using trustworthy systems / devices where the Secure Site Certificate is required, and follow processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized usage. The Secure Site Private keys are generated by the subscriber on the respective device. The CA will deliver the Secure Site Certificate by secure email / secured web session / physical delivery of secure media to authorized person.</p> <p>It is highly recommended to use secure hardware meeting the minimum requirements as mentioned in the Government-CA CP for Key generation and storage.</p>
8	Certificate Issuance Process	<p>Certificates shall only be issued to fully qualified domain name or valid IP address which are publicly registered and publicly verifiable, after the applicant has successfully completed the registration process. Please see additional verification rules in point 6 of this table **.</p> <ul style="list-style-type: none"> <li>• The Subscriber (device sponsor) will be present at the RA for face-to-face identity verification</li> <li>• The RA will validate the documents submitted by the subscriber, as requested in the subscriber form.</li> <li>• Verify against official Registrar.</li> <li>• The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner.</li> <li>• The subscriber will generate the keys in the device/machine and a corresponding PKCS#10 certificate signing request (CSR)</li> <li>• The Subscriber will enter his reference number, authorization code and paste the CSR on a NCDC designated secure site to download the Secure Site Certificate.</li> <li>• The Subscriber will install and use the Secure Site Certificate on the authorized device/machine only.</li> </ul>

S. No.	Attribute	Secure Site Certificate
9	Key Usage	Secure Site keys shall be used for strongly authenticating Servers/Devices, and for encrypting SSL/TLS sessions. This CP prohibits the use of Secure Site Certificates for Data-Encryption.
10	Private Key Protection	Private keys shall be protected using a Trustworthy System and private key holders shall take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with <a href="#">section 6.2</a> of the Government-CA CP document. Private keys may be stored in software and shall be protected with strong passwords as a minimum. Generation and Storage in appropriate FIPS 140-2 Level 2 or higher certified cryptographic hardware is recommended. Device Sponsor may keep a backup of the private key and such backups should also be protected with strong passwords as a minimum
11	Certificate Life Time	Up to 36months(3years)
12	Key Backup	No Key Backups shall be taken by the CA for Secure Site Certificates.
13	Asymmetric Key Length	Minimum 2048 bits RSA
14	Certificate Re-key	Not applicable

### 3.2 SECURE SITE CERTIFICATE PROFILE

Field / x.509 extension	Value or Value Constant	Critical
<b>Subject</b>	CN = <FQDN for Server or Device **> OU=<optional searchbase(s)> OU = Government CA O = National Center for Digital Certification C = SA (Encoding should be in UTF8 only) ** Please refer to point 6 of the preceding table for applicable rules	V1 Field
<b>Subject Alternative Name</b>	** dNSName=<Publicly Verifiable Alternative FQDN or IP Address for Server or Device> OR <privately-addressable pseudo-domains and hostnames> Note: Subject Alternative Names other than the dNSName are not permitted to be included here. ** Please refer to point 6 of the preceding table for applicable rules	NO
<b>CRL Distribution Points</b>	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcapart<n>.crl Directory Address: CN=CRL1 OU=Government CA O=National Center for Digital Certification	NO

Field / x.509 extension	Value or Value Constant	Critical
	C=SA [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcacomb<n>.crl	
<b>Authority Key Identifier</b>	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
<b>Subject Key Identifier</b>	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
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None	NO
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.1.1.1.3.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA Certification Policy and associated documentation available at http://web.ncdc.gov.sa/ is hereby incorporated into your use or reliance on this Certificate.	NO
<b>Authority Information Access</b>	[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/gca.crt	NO
<b>Key Usage</b>	Digital Signature; Key Encipherment	NO
<b>Extended Key Usage</b>	Server Authentication (1.3.6.1.5.5.7.3.1)	NO



## 4. ORGANIZATION SIGNING CERTIFICATE (UNMANAGED)

### 4.1 ORGANIZATION SIGNING CERTIFICATE POLICY

S. No.	Attribute	Organization Signing Certificate (UnManaged)
1	Policy Name	Organization Signing Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.3.1.1.1.1.4.1
3	Subject	<p>“CN = &lt;Full Organization Name, suffixed with one or more of the below:</p> <ul style="list-style-type: none"> <li>- Role,</li> <li>- Designation,</li> <li>- Location,</li> <li>- Application Name***&gt;,”</li> </ul> <p>OU=&lt;optional searchbase(s)&gt;, OU = Government CA, O = National Center for Digital Certification, C = SA”</p> <p>*** Identifier rules:</p> <ul style="list-style-type: none"> <li>- Use of only organization name in the CN is not permitted</li> <li>- 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’</li> </ul>
4	Certificate Profile	See below after the table.
5	Application Usage	<p><b>If subscriber wants to engage in legal signing he/she is advised to use <u>Signing</u> 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.</b></p> <p>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 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.</p> <p>Government- CA issued Certificates are general-purpose Certificates and are not tied to any specific application or function. The applications using the Government- CA issued Signing Certificate should honour Key Usage.</p> <p>Following are some of the common usage of the certificate</p> <ul style="list-style-type: none"> <li>• Inter Government correspondence;</li> <li>• Public Information Posting by Authorised Government Personnel;</li> <li>• Departmental Forms Submission;</li> <li>• PKI enabled Application work-flow; and</li> <li>• E Tendering</li> </ul> <p>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 practices, Subscribers agreement and not otherwise prohibited by the law of Saudi Arabia.</p> <p>Certificate(s) issued under this type shall not be used for any form of data encryption.</p>
6	Verification Process	<p><b>1.</b> Subscriber shall be required to attend to the RA for face-to-face</p>

S. No.	Attribute	Organization Signing Certificate (UnManaged)
		<p>identity validation and submission of supporting documents.</p> <ol style="list-style-type: none"> <li>2. The following will be considered valid identity documents:                             <ol style="list-style-type: none"> <li>a. National ID / passport for citizens.</li> <li>b. Residence permit / passport for residents.</li> </ol> </li> <li>3. Validation of Identifier rules as stated in point 3 of this table. ***</li> <li>4. 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.</li> <li>5. 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</li> </ol> <p>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 NCDC-approved <u>signing</u> certificate types.</p>
7	Key Pair Generation and Installation	<p>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.</p> <p><b>Signing certificates MUST be stored on the secured hardware meeting the minimum requirements as mentioned in the Government-CA CP.</b></p> <p>The Private key corresponding to the signing certificate 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 Key. In addition, the Subscriber shall acknowledge receipt of the private key.</p>
8	Certificate Issuance Process	<p>Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following:</p> <ul style="list-style-type: none"> <li>• The Subscriber will be present at the RA for face-to-face identity verification</li> <li>• The RA will validate the documents submitted by the subscriber</li> <li>• The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner.</li> <li>• NCDC prescribed web-site along with client-side Software will generate the Subscriber’s keys securely on his smart card / USB token/Software.</li> <li>• The CA will authenticate the Subscriber using the reference</li> </ul>

S. No.	Attribute	Organization Signing Certificate (UnManaged)
		number and authorization code. Upon successful authentication, the CA shall create the Subscribers certificates and transport them securely onto the Subscriber’s smart cards / USB tokens, or provide for download.
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 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 signing private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.
11	Certificate Life Time	Up to 36months (3 years)
12	Key Backup	The CSP 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	Not applicable for UnManaged Signing Certificate.

#### 4.2 ORGANIZATION SIGNING CERTIFICATE PROFILE

Field / x.509 extension	Value or Value Constant	Critical
<b>Subject</b>	CN = < Full Organization Name, suffixed with one or more of the below: - Role, - Designation, - Location, Application Name***> OU=<optional searchbase(s)> OU = Government CA O = National Center for Digital Certification C = SA (Encoding should be in UTF8 only) *** Please refer to the Identifier Rules in point 3 of the preceding table.	V1 Field
<b>CRL Distribution Points</b>	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcapart<n>.crl Directory Address: CN=CRL1	NO

Field / x.509 extension	Value or Value Constant	Critical
	OU=Government CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name:  URL=http://web.ncdc.gov.sa/crl/gcacombo1.crl	
<b>Authority Key Identifier</b>	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
<b>Subject Key Identifier</b>	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
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None	NO
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.3.1.1.1.1.4.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA Certification Policy and associated documentation available at http://web.ncdc.gov.sa/ is hereby incorporated into your use or reliance on this Certificate.	NO
<b>Authority Information Access</b>	[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/gca.crt	NO

Field / x.509 extension	Value or Value Constant	Critical
<b>Key Usage</b>	Non-Repudiation; Digital Signature	NO
<b>Extended Key Usage</b>	Client Authentication (1.3.6.1.5.5.7.3.2)	NO

## 5. YESSER GSN CLIENT AUTHENTICATION CERTIFICATE (UNMANAGED)

### 5.1 YESSER GSN CLIENT AUTHENTICATION CERTIFICATE POLICY (FOR USE BY YESSER ONLY)

S. No.	Attribute	Yesser GSN Client Authentication Certificate (UnManaged)
1	Policy Name	Yesser GSN Client Authentication Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.5.2.3
3	Subject	“CN = <Yesser GSN DNS Registered domain name>, OU=<optional searchbase(s)>, OU = Government CA, O = National Center for Digital Certification, C = SA”
4	Certificate Profile	See below after the table.
5	Application Usage	<p>These certificate types are consumed by Yesser Government Service Network (GSN) and/or Yesser Government Service Bus (GSB) programs. The applications using this type of Certificate should honour Key Usage.</p> <p>This certificate should be used for client authentication and may also be used to verify data integrity. For Legal-Signing, it is required to use a NCDC Signing Certificate type.</p> <p>The Yesser GSN Client Authentication 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 practices, Subscribers agreement and not otherwise prohibited by the law of Saudi Arabia.</p> <p>Certificate(s) issued under this type must not be used for any form of data encryption.</p>
6	Verification Process	<ol style="list-style-type: none"> <li>1. Subscriber shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents.</li> <li>2. The following will be considered valid identity documents: <ol style="list-style-type: none"> <li>a. National ID / passport for citizens.</li> <li>b. Residence permit / passport for residents.</li> <li>c. Yesser or Ministry of Communications and IT employee ID card</li> </ol> </li> <li>3. Validation of requested Common Name against the Yesser GSN DNS.</li> <li>4. 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</li> </ol> <p>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 NCDC-approved <u>signing</u> certificate types.</p>
7	Key Pair Generation	Key Pair generation must be performed using trustworthy systems /

S. No.	Attribute	Yesser GSN Client Authentication Certificate (UnManaged)
	and Installation	<p>devices where the Yesser GSN Client Authentication Certificate is required and follow processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized usage. The Yesser GSN Client Authentication Private keys are generated by the subscriber on the respective device. The CA will deliver the Secure Site Certificate by secure email / secured web session / physical delivery of secure media to authorized person.</p> <p>It is highly recommended to use secure hardware meeting the minimum requirements as mentioned in the Government-CA CP for Key generation and storage.</p>
8	Certificate Issuance Process	<p>Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following:</p> <ul style="list-style-type: none"> <li>• The Subscriber (Device Sponsor) will be present at the RA for face-to-face identity verification</li> <li>• The RA will validate the documents submitted by the subscriber, as requested in the subscriber form.</li> <li>• Verify against Yesser GSN DNS.</li> <li>• The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner.</li> <li>• The subscriber will go to the RA customization center</li> <li>• The Subscriber will plug his smart card / USB token into the customization device.</li> <li>• The Subscriber will enter the PIN of the smart card / USB token</li> <li>• The Subscriber will enter reference number and an authorization code to generate keys and download certificates.</li> <li>• The web-site along with client-side Software will generate the Subscriber’s keys securely on his smart card / USB token.</li> <li>• The CA will authenticate the Subscriber using the reference number and authorization code. Upon successful authentication, the CA shall create the Subscribers certificates and transport them securely onto the Subscriber’s smart cards / USB tokens.</li> </ul>
9	Key Usage	<p>Authentication certificate and associated keys can be used for data integrity and client-authentication based on the identifier/attribute to which the certificate was issued.</p>
10	Private Key Protection	<p>Private keys shall be protected using a Trustworthy System and private key holders shall take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with <a href="#">section 6.2</a> of the Government-CA CP document. Private keys may be stored in software and shall be protected with strong passwords as a minimum. Generation and Storage in appropriate FIPS 140-2 Level 2 or higher certified cryptographic hardware is recommended. Device Sponsor may keep a backup of the private key and such backups should also be protected with strong passwords as a minimum</p>

S. No.	Attribute	Yesser GSN Client Authentication Certificate (UnManaged)
11	Certificate Life Time	Up to 36months (3 years)
12	Key Backup	The CSP 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	Not applicable

## 5.2 YESSER GSN CLIENT AUTHENTICATION CERTIFICATE PROFILE

Field / x.509 extension	Value or Value Constant	Critical
<b>Subject</b>	CN = < Yesser GSN DNS Registered domain name> OU=<optional searchbase(s)> OU = Government CA O = National Center for Digital Certification C = SA (Encoding should be in UTF8 only)	V1 Field
<b>CRL Distribution Points</b>	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcapart<n>.crl Directory Address: CN=CRL1 OU=Government CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://web.ncdc.gov.sa/crl/gcacom<n>.crl	NO
<b>Authority Key Identifier</b>	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
<b>Subject Key Identifier</b>	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
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None	NO

Field / x.509 extension	Value or Value Constant	Critical
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.5.2.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA Certification Policy and associated documentation available at http://web.ncdc.gov.sa/ is hereby incorporated into your use or reliance on this Certificate.	NO
<b>Authority Information Access</b>	[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/gca.crt	NO
<b>Key Usage</b>	Digital Signature	NO
<b>Extended Key Usage</b>	Client Authentication (1.3.6.1.5.5.7.3.2)	NO

## 6. YESSER GSN INTERNAL SECURE SITE CERTIFICATE (UNMANAGED)

### 6.1 YESSER GSN INTERNAL SECURE SITE CERTIFICATE POLICY (FOR USE BY YESSER ONLY)

S. No.	Attribute	Yesser GSN Internal Secure Site Certificate
1	Policy Name	Yesser GSN Internal Secure Site Certificate Policy
2	Policy OID	2.16.682.1.101.5000.1.5.2.2
3	Subject	<p>“CN = &lt; Yesser GSN DNS Registered domain name *&gt;, OU=&lt;optional searchbase(s)&gt;, OU = Government CA, O = National Center for Digital Certification, C = SA”</p> <p>*Publicly verifiable domain names or IP address should not be included in the certificate for this certificate type. For such requirements, issue a ‘Secure Site Certificate’ only.</p>
4	Certificate Profile	See below after the table.
5	Application Usage	<p>Yesser GSN Internal Secure Site certificates are only issued to servers/devices, such as applications or web servers within the Kingdom of Saudi Arabia. Appropriate use of such certificate(s) is for server authentication and session encryption, and where another web site or device requires high-assurance proof of server/device identity.</p> <p>These certificate(s) shall only be issued to server/device full names (such as host.domain.egov), verifiable against the Yesser GSN DNS.</p> <p>Such certificate(s) may also be used for client authentication, provided the subscriber/device sponsor is the same and control of keys remain with the same subscriber/device sponsor.</p> <p>Certificate(s) issued under this type shall not be used for any form of data encryption, except SSL/TLS session encryption.</p>
6	Verification Process	<ol style="list-style-type: none"> <li>1. Subscriber (Device Sponsor) shall be required to attend to the RA for face-to-face identity validation and submission of supporting documents.</li> <li>2. The following will be considered valid identity documents:                             <ol style="list-style-type: none"> <li>a. National ID / passport for citizens.</li> <li>b. Residence permit / passport for residents.</li> <li>c. Yesser or Ministry of Communications and IT employee ID card</li> </ol> </li> <li>3. Validation of requested Common Name against the Yesser GSN DNS.</li> <li>4. 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</li> </ol> <p>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 NCDC-approved <u>signing</u> certificate types.</p>
7	Key Pair Generation	Key Pair generation must be performed using trustworthy systems /

S. No.	Attribute	Yesser GSN Internal Secure Site Certificate
	and Installation	<p>devices where the Yesser GSN Internal Secure Site Certificate is required and follow processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized usage. The Yesser GSN Internal Secure Site Private keys are generated by the subscriber on the respective device. The CA will deliver the Secure Site Certificate by secure email / secured web session / physical delivery of secure media to authorized person.</p> <p>It is highly recommended to use secure hardware meeting the minimum requirements as mentioned in the Government-CA CP for Key generation and storage.</p>
8	Certificate Issuance Process	<p>Certificates shall only be issued to Yesser GSN DNS domain names, after the applicant has successfully completed the registration process.</p> <ul style="list-style-type: none"> <li>• The Subscriber (device sponsor) will present the required forms and documentation to the RA</li> <li>• The RA will validate the documents submitted by the subscriber</li> <li>• The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner.</li> <li>• The subscriber will generate the keys in the device/machine and a corresponding PKCS#10 certificate signing request (CSR)</li> <li>• The Subscriber will enter his reference number, authorization code and paste the CSR on a NCDC designated secure site to download the Yesser GSN Internal Secure Site Certificate.</li> <li>• The Subscriber will install and use the Yesser GSN Internal Secure Site Certificate on the authorized device/machine only.</li> </ul>
9	Key Usage	<p>Yesser GSN Internal Secure Site keys shall be used for authenticating Servers/Devices /Clients, and for encrypting SSL/TLS sessions. Certificate(s) issued under this type shall not be used for any form of data encryption, except SSL/TLS session encryption.</p>
10	Private Key Protection	<p>Private keys shall be protected using a Trustworthy System and private key holders shall take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with <a href="#">section 6.2</a> of the Government-CA CP document.</p> <p>Private keys may be stored in software and shall be protected with strong passwords as a minimum. Generation and Storage in appropriate FIPS 140-2 Level 2 or higher certified cryptographic hardware is recommended. Device Sponsor may keep a backup of the private key and such backups should also be protected with strong passwords as a minimum</p>
11	Certificate Life Time	Up to 36 months (3 years)
12	Key Backup	No Key Backups shall be taken by the CA for Internal Secure Site Certificates.
13	Asymmetric Key Length	Minimum 2048 bits RSA
14	Certificate Re-key	Not applicable

## 6.2 YESSER GSN INTERNAL SECURE SITE CERTIFICATE PROFILE

Field / x.509 extension	Value or Value Constant	Critical
<b>Subject</b>	CN = < Yesser GSN DNS Registered domain name *> OU=<optional searchbase(s)> OU = Government CA O = National Center for Digital Certification C = SA (Encoding should be in UTF8 only) *Publicly verifiable domain names or IP address should not be included in the certificate for this certificate type. For such requirements, issue a 'Secure Site Certificate' only.	V1 Field
<b>CRL Distribution Points</b>	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name:  URL=http://web.ncdc.gov.sa/crl/gcapart<n>.crl Directory Address: CN=CRL1 OU=Government CA O=National Center for Digital Certification C=SA [2]CRL Distribution Point Distribution Point Name: Full Name:  URL=http://web.ncdc.gov.sa/crl/gcacombo<n>.crl	NO
<b>Authority Key Identifier</b>	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
<b>Subject Key Identifier</b>	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
<b>Basic Constraints</b>	Subject Type=End Entity Path Length Constraint=None	NO
<b>Certificate Policies</b>	[1]Certificate Policy: Policy Identifier=2.16.682.1.101.5000.1.5.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://web.ncdc.gov.sa	NO

Field / x.509 extension	Value or Value Constant	Critical
	[1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= Government CA Certification Policy and associated documentation available at <a href="http://web.ncdc.gov.sa/">http://web.ncdc.gov.sa/</a> is hereby incorporated into your use or reliance on this Certificate.	
<b>Authority Information Access</b>	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= <a href="http://ocsp.ncdc.gov.sa">http://ocsp.ncdc.gov.sa</a> [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= <a href="http://web.ncdc.gov.sa/certs/gca.crt">http://web.ncdc.gov.sa/certs/gca.crt</a>	NO
<b>Key Usage</b>	Digital Signature; Key Encipherment	NO
<b>Extended Key Usage</b>	Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2)	NO