Certificate Policy and Practice Statement (CP/CPS)

for High Assurance Certification Services and Timestamping

Document Control

☐ Draft ☐ Final ☐ New Version ☒ Approved

Version	Action	Reviewer	Date	Notes
0.1	Initial Draft Version	Ascertia	12-Feb-2026	
0.2	Updated version after internal review	Ascertia	15-Feb-2026	
0.3	Amended based on CROWE's Auditors review & feedback	Ascertia	20-Feb-2026	
0.4	Amended based on additional CROWE's Auditors feedback	Ascertia	10-Apr-2026	
0.5	Amended based on: • NIC feedback • Signit feedback regarding CA naming, OIDs and URLs	Ascertia	24-Apr-2026	
0.6	Based on NIC/Signit feedback: • Remove the National ID number as a possible value for the "SERIALNUMBER" field in 7.1.10.3.2	Ascertia	07-May-2026	
0.7	Amendment based on Signit feedback related to possible value for the "SERIALNUMBER" field in 7.1.10.3.2	Signit	13-May-2026	
0.8	Amended based on additional CROWE's Auditors review & feedback	Signit	22-May-2026	
0.9	Updating cryptographic algorithms across the PKI hierarchy to support ECC	Signit	09-Jun-2026	
1.0	Approved by the Signit PKI Governance Board	Signit	18-Jun-26	
1.1	• Recognized Reliable KYC Providers as entities that may perform defined registration activities for Natural Person short-term certificates, extended their responsibilities, and identified the categories of organization eligible to act in that role. • Introduced the applicant-generated key-pair model for eSeal certificates, allocated a separate certificate policy object identifier to it, and defined the requirements for Signit approval of the applicant's cryptographic module. • Added an object identifier table in Section 1.2 and clarified the certificate policy identifiers in Section 7.1.6. • Updated key protection requirements to Common Criteria certification for cryptographic modules operated by Signit. • Added Subscriber representations and warranties in Section 9.6.3.	Ascertia	22-Sep-2026	

	• Added verification requirements for organizations that cannot be verified through the Saudi commercial registry and introduced a twelve-month reliance period for verified organization information. • Removed the requirement for personnel holding Trusted Roles to be Saudi citizens. • Revised the Natural Person Certificate Subject DN, amended the wording of Section 4.10.2 for clarity, improved wording and corrected typographical errors throughout			

Sign off

Role: PKI Director

Name: Mohamed El Abbouri

Date: 29/09/2026

Signature: 

Table Of Contents

DOCUMENT CONTROL 2

1. INTRODUCTION 10

1.1. OVERVIEW 10
1.1.1. SIGNIT GOVERNANCE BOARD (SIGNIT GB) 11
1.2. DOCUMENT NAME AND IDENTIFICATION 12
1.3. PKI PARTICIPANTS 13
1.3.1. CERTIFICATION AUTHORITIES 13
1.3.2. REGISTRATION AUTHORITIES 13
1.3.3. SUBSCRIBERS 14
1.3.4. PKI SERVICE COMPONENTS OPERATED BY SIGNIT 14
1.3.5. RELYING PARTIES 15
1.3.6. OTHER PARTICIPANTS 15
1.4. CERTIFICATE USAGE 16
1.4.1. APPROPRIATE CERTIFICATE USES 16
1.4.2. PROHIBITED CERTIFICATE USES 17
1.5. POLICY ADMINISTRATION 17
1.5.1. ORGANIZATION ADMINISTERING THE DOCUMENT 17
1.5.2. CONTACT PERSON 17
1.5.3. PERSON DETERMINING CP/CPS SUITABILITY FOR THE POLICY 18
1.5.4. CP/CPS APPROVAL PROCEDURES 18
1.6. DEFINITIONS AND ACRONYMS 18
1.6.1. DEFINITIONS 18
1.6.2. ACRONYMS 23
1.6.3. REFERENCES 25

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 26

2.1. REPOSITORY 26
2.2. PUBLICATION OF CERTIFICATION INFORMATION 26
2.3. TIME OR FREQUENCY OF PUBLICATION 26
2.3.1. CA CERTIFICATES 26
2.3.2. CERTIFICATE REVOCATION LISTS 27
2.4. ACCESS CONTROLS ON REPOSITORIES 27

3. IDENTIFICATION AND AUTHENTICATION 28

3.1. NAMING 28
3.1.1. TYPES OF NAMES 28
3.1.2. NEED FOR NAMES TO BE MEANINGFUL 28
3.1.3. ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS 28
3.1.4. RULES FOR INTERPRETING VARIOUS NAME FORMS 28
3.1.5. UNIQUENESS OF NAMES 28
3.1.6. RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS 29
3.2. INITIAL IDENTITY VALIDATION 29
3.2.1. METHOD TO PROVE POSSESSION OF PRIVATE KEY 29
3.2.2. AUTHENTICATION OF ORGANIZATION IDENTITY 29
3.2.3. AUTHENTICATION OF INDIVIDUAL IDENTITY 30

3.2.4. Non-verified Subscriber Information 30
3.2.5. Validation of Authority 30
3.2.6. Criteria for Interoperation 31
3.3. Identification and Authentication for Re-key Requests 31
3.3.1. Identification and Authentication for Routine Re-key 31
3.3.2. Identification and Authentication for Re-key after Revocation 32
3.4. Identification and Authentication for Revocation Request 32

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 34

4.1. Certificate Application 34
4.1.1. Who Can Submit a Certificate Application 34
4.1.2. Enrollment Process and Responsibilities 35
4.2. Certificate Application Processing 37
4.2.1. Performing Identification and Authentication Functions 37
4.2.2. Approval or Rejection of Certificate Applications 39
4.2.3. Time to Process Certificate Applications 40
4.3. Certificate Issuance 40
4.3.1. CA Actions During Certificate Issuance 40
4.3.2. Notification to Subscriber by the CA of Issuance of Certificate 41
4.4. Certificate Acceptance 41
4.4.1. Conduct Constituting Certificate Acceptance 41
4.4.2. Publication of the Certificate by the CA 42
4.4.3. Notification of Certificate Issuance by the CA to Other Entities 42
4.5. Key Pair and Certificate Usage 42
4.5.1. Subscriber Private Key and Certificate Usage 42
4.5.2. Relying Party Public Key and Certificate Usage 42
4.6. Certificate Renewal 43
4.6.1. Circumstance for Certificate Renewal 43
4.6.2. Who May Request Renewal 43
4.6.3. Processing Certificate Renewal Requests 43
4.6.4. Notification of New Certificate Issuance to Subscriber 43
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate 43
4.6.6. Publication of the Renewal Certificate by the CA 43
4.6.7. Notification of Certificate Issuance by the CA to Other Entities 43
4.7. Certificate Re-Key 43
4.7.1. Circumstance for Certificate Re-Key 44
4.7.2. Who May Request Certification of a New Public Key 44
4.7.3. Processing Certificate Re-Keying Requests 44
4.7.4. Notification of New Certificate Issuance to Subscriber 44
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate 44
4.7.6. Publication of the Re-Keyed Certificate by the CA 44
4.7.7. Notification of Certificate Issuance by the CA to Other Entities 44
4.8. Certificate Modification 44
4.8.1. Circumstance for Certificate Modification 44
4.8.2. Who May Request Certificate Modification 44
4.8.3. Processing Certificate Modification Requests 45
4.8.4. Notification of New Certificate Issuance to Subscriber 45
4.8.5. Conduct Constituting Acceptance of Modified Certificate 45
4.8.6. Publication of the Modified Certificate by the CA 45
4.8.7. Notification of Certificate Issuance by the CA to Other Entities 45
4.9. Certificate Revocation and Suspension 45
4.9.1. Circumstances for Revocation 45
4.9.2. Who Can Request Revocation 47

4.9.3. Procedure for Revocation Request 48
4.9.4. Revocation Request Grace Period 49
4.9.5. Time Within Which CA Must Process the Revocation Request 50
4.9.6. Revocation Checking Requirement for Relying Parties 50
4.9.7. CRL Issuance Frequency 50
4.9.8. Maximum Latency for CRLs 51
4.9.9. On-Line Revocation/Status Checking Availability 51
4.9.10. On-Line Revocation Checking Requirements 51
4.9.11. Other Forms of Revocation Advertisements Available 52
4.9.12. Special Requirements Related to Key Compromise 52
4.9.13. Circumstances for Suspension 52
4.9.14. Who Can Request Suspension 52
4.9.15. Procedure for Suspension Request 52
4.9.16. Limits on Suspension Period 53
4.10. Certificate Status Services 53
4.10.1. Operational Characteristics 53
4.10.2. Service Availability 53
4.10.3. Optional Features 54
4.11. End of Subscription 54
4.12. Key Escrow and Recovery 54
4.12.1. Key Escrow and Recovery Policy and Practices 54
4.12.2. Session Key Encapsulation and Recovery Policy and Practices 54

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 55

5.1. Physical Security Controls 55
5.1.1. Site Location and Construction 55
5.1.2. Physical Access 56
5.1.3. Power and Air Conditioning 56
5.1.4. Water Exposures 56
5.1.5. Fire Prevention and Protection 57
5.1.6. Media Storage 57
5.1.7. Waste Disposal 57
5.1.8. Off-Site Backup 58
5.2. Procedural Controls 58
5.2.1. Trusted Roles 58
5.2.2. Number of Persons Required per Task 59
5.2.3. Identification and Authentication for each Role 59
5.2.4. Roles Requiring Separation of Duties 59
5.3. Personnel Controls 60
5.3.1. Qualifications, Experience, and Clearance Requirements 60
5.3.2. Background Check Procedures 60
5.3.3. Training Requirements 60
5.3.4. Retraining Frequency and Requirements 61
5.3.5. Job Rotation Frequency and Sequence 61
5.3.6. Sanctions for Unauthorized Actions 61
5.3.7. Independent Contractor Requirements 61
5.3.8. Documentation Supplied to Personnel 61
5.4. Audit Logging Procedures 62
5.4.1. Types of Events Recorded 62
5.4.2. Frequency of Processing Log 63
5.4.3. Retention Period for Audit Log 64
5.4.4. Protection Of Audit Log 64
5.4.5. Audit Log Backup Procedures 64

5.4.6. Audit Collection System (Internal vs. External) 64
5.4.7. Notification to Event-Causing Subject 65
5.4.8. Vulnerability Assessments 65
5.5. Records Archival 66
5.5.1. Types of Records Archived 66
5.5.2. Retention Period for Archive 66
5.5.3. Protection of Archive 66
5.5.4. Archive Backup Procedures 66
5.5.5. Requirements for Timestamping of Records 67
5.5.6. Archive Collection System (Internal or External) 67
5.5.7. Procedures to Obtain and Verify Archive Information 67
5.6. Key Changeover 67
5.7. Compromise and Disaster Recovery 68
5.7.1. Incident and Compromise Handling Procedures 68
5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data are Corrupted 68
5.7.3. Recovery procedures after key compromise 68
5.7.4. Business Continuity Capabilities after a Disaster 69
5.8. CA or RA Termination 69

6. TECHNICAL SECURITY CONTROLS 71

6.1. Key Pair Generation and Installation 71
6.1.1. Key Pair Generation 71
6.1.2. Private Key Delivery to Subscriber 72
6.1.3. Public Key Delivery to Certificate Issuer 72
6.1.4. CA Public Key Delivery to Relying Parties 72
6.1.5. Key Sizes 72
6.1.6. Public Key Parameters Generation and Quality Checking 72
6.1.7. Key Usage Purposes (as per X.509 v3 key usage field) 72
6.2. Private Key Protection and Cryptographic Module Engineering Controls 73
6.2.1. Cryptographic Module Standards and Controls 73
6.2.2. Private Key (m out of n) Multi-person Control 73
6.2.3. Private Key Escrow 73
6.2.4. Private Key Backup 74
6.2.5. Private Key Archival 74
6.2.6. Private Key Transfer into or from a Cryptographic Module 74
6.2.7. Private key Storage on Cryptographic Module 75
6.2.8. Method of Activating Private Key 75
6.2.9. Method of Deactivating Private Key 75
6.2.10. Method of Destroying Private Key 76
6.2.11. Cryptographic Module Rating 77
6.3. Other Aspects of Key Pair Management 77
6.3.1. Public Key Archival 77
6.3.2. Certificate Operational Periods and Key Pair Usage Periods 77
6.4. Activation Data 78
6.4.1. Activation Data Generation and Installation 78
6.4.2. Activation Data Protection 78
6.4.3. Other Aspects of Activation Data 78
6.5. Computer Security Controls 79
6.5.1. Specific Computer Security Technical Requirements 79
6.5.2. Computer Security Rating 79
6.6. Life Cycle Technical Controls 79
6.6.1. System Development Controls 79
6.6.2. Security Management Controls 80

6.6.3. Life Cycle Security Controls 80
6.7. Network Security Controls 81
6.8. Timestamping 81

7. CERTIFICATE, CRL, OCSP, AND TSA PROFILES 82

7.1. Certificate Profile 82
7.1.1. Certificate Extensions 82
7.1.2. Version Number(s) 82
7.1.3. Algorithm Object Identifiers 82
7.1.4. Name Forms 82
7.1.5. Name Constraints 82
7.1.6. Certificate Policy Object Identifier 82
7.1.7. Usage of Policy Constraints Extension 83
7.1.8. Policy Qualifiers Syntax and Semantics 83
7.1.9. Processing Semantics for the Critical Certificate Policies Extension 83
7.1.10. Signit Certificate Profiles 83
7.2. CRL & CARL Profiles 102
7.2.1. Signit Licensed CA CARL Profile 103
7.2.2. Subordinate CAs CRL Profiles 104
7.2.3. Version Number(s) 107
7.2.4. CRL and CRL Entry Extensions 107
7.3. OCSP Profile 107
7.3.1. Signit Intermediate OCSP Responder Certificate 107
7.3.2. Subordinate CAs OCSP Responder Certificate 108
7.4. OCSP Request and Response Formats 113
7.4.1. OCSP Request Format 113
7.4.2. OCSP Response Format 113
7.5. Timestamp Request and Response Formats 114
7.5.1. TSA Request Format 114
7.5.2. TSA Response Format 115

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 116

8.1. Frequency or Circumstances of Assessment 116
8.2. Identity/Qualifications of Assessor 116
8.3. Assessor's Relationship to Assessed Entity 116
8.4. Topics Covered by Assessment 117
8.5. Actions Taken as a Result of Deficiency 117
8.6. Communication of Results 117

9. OTHER BUSINESS AND LEGAL MATTERS 118

9.1. Fees 118
9.1.1. Certificate Issuance or Renewal Fees 118
9.1.2. Certificate Access Fees 118
9.1.3. Revocation Or Status Information Access Fees 118
9.1.4. Fees for Other Services 118
9.1.5. Refund Policy 118
9.2. Financial Responsibility 118
9.2.1. Insurance Coverage 118
9.2.2. Other Assets 118

9.2.3. Insurance or Warranty Coverage for End-Entities 118
9.3. Confidentiality of Business Information 118
9.3.1. Scope of Confidential Information 118
9.3.2. Information Not within the Scope of Confidential Information 119
9.3.3. Responsibility to Protect Confidential Information 119
9.4. Privacy of Personal Information 119
9.4.1. Privacy Plan 119
9.4.2. Information Treated as Private 119
9.4.3. Information Not Deemed Private 119
9.4.4. Responsibility to Protect Private Information 120
9.4.5. Notice and Consent to Use Private Information 120
9.4.6. Disclosure Pursuant to Judicial or Administrative Process 120
9.4.7. Other Information Disclosure Circumstances 120
9.5. Intellectual Property Rights 120
9.6. Representations and Warranties 120
9.6.1. CA Representations and Warranties 120
9.6.2. RA Representations and Warranties 121
9.6.3. Subscriber Representations and Warranties 121
9.6.4. Relying Party Representations and Warranties 122
9.6.5. Representations and Warranties of Other Participants 122
9.7. Disclaimers Of Warranties 122
9.8. Limitations of Liability 123
9.9. Indemnities 123
9.10. Term And Termination 123
9.10.1. Term 123
9.10.2. Termination 123
9.10.3. Effect of Termination and Survival 123
9.11. Individual Notices and Communications with Participants 123
9.12. Amendments 124
9.12.1. Procedure for Amendment 124
9.12.2. Notification Mechanism and Period 124
9.12.3. Circumstances under which OID Must Be Changed 124
9.13. Dispute Resolution Provisions 124
9.14. Governing Law 124
9.15. Compliance with Applicable Law 124
9.16. Miscellaneous Provisions 124
9.16.1. Entire Agreement 124
9.16.2. Assignment 125
9.16.3. Severability 125
9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights) 125
9.16.5. Force Majeure 125
9.17. Other Provisions 125

1.Introduction

This Certificate Policy and Certification Practice Statement (CP/CPS) defines the policies, governance framework, and operational practices implemented by Signit for the issuance and lifecycle management of digital certificates within its Public Key Infrastructure (PKI). The purpose of this document is to provide transparency regarding the rules and procedures governing certificate approval, issuance, management, revocation, and status validation.

Signit is a Saudi technology company established in 2021 that provides digital trust capabilities supporting secure electronic transactions. As part of these capabilities, Signit operates certification services that enable electronic signatures, electronic seals, verification services, and the issuance of certificates used by Timestamping Units (TSU).

This CP/CPS applies to all certificates issued under Signit PKI. It describes the roles and responsibilities of Signit, PKI participants, subscribers, and relying parties, and outlines the technical and organizational controls applied to maintain trust in issued certificates.

Certificates issued under this CP/CPS support a high level of assurance, reflecting the strength of identity verification and issuance controls applied by Signit.

Operational practices related to the provision of timestamping services, including time source management and time-stamp token generation, are defined separately in Signit Timestamping Policy and Practice Statement. Within this CP/CPS, references to timestamping are limited strictly to the issuance and lifecycle management of certificates used by Timestamping Units.

The structure and content of this CP/CPS follow the framework defined in RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework: https://datatracker.ietf.org/doc/html/rfc3647

In addition, this CP/CPS is intended to operate in accordance with the Saudi National Root CA Certificate Policy and the Saudi Electronic Transactions Law, and aligns with relevant technical standards applicable to certificates used by timestamping units.

Where applicable, Signit aligns its certification practices with recognized audit frameworks, including the WebTrust Principles and Criteria for Certification Authorities (https://www.cpacanada.ca), to support independent assurance of its certification services

Further information with regard to this CP/CPS can be obtained from Signit, using contact information provided in clause 1.5.

1.1. Overview

Signit provides certification capabilities intended to support secure electronic transactions for individuals and organizations operating within Saudi Arabia. Through its PKI, Signit enables the issuance and lifecycle management of digital certificates used for electronic signatures, electronic seals, validation-related services, and Timestamping Unit (TSU) signing functions.

To maintain strong security controls while ensuring operational scalability and resilience, Signit operates its PKI applications, systems and supporting components with cryptographic key protection provided through Signit-controlled HSMs within secure infrastructures and facilities

located in the Kingdom of Saudi Arabia and managed by approved infrastructure and facilities service providers.

The approved infrastructure and facilities services providers supplies, respectively, the hosting environment for the PKI application layer, and the physical facilities housing the HSMs and associated key-management equipment. Signit retains exclusive logical and cryptographic control of the HSMs, CA private keys, activation data and key-ceremony material.

Within this framework, Signit operates a structured Certification Authority (CA) hierarchy designed to separate Certification Authorities responsible for managing CA certificates from those used for issuing certificates to subscribers and system components. The PKI hierarchy consists of:

(i) **Level 1:** Signit Licensed CA (intermediate CA) at this level serves as the top CA within Signit PKI hierarchy. It operates as a single, offline CA that is certified by the publicly trusted Saudi National Root CA, which is managed by the National Information Center (NIC). This Signit Licensed CA is responsible for issuing certificates to subordinate Certification Authorities within the next layer of Signit PKI hierarchy.

(ii) **Level 2:** This level consists of Signit's Subordinate CAs, which are dedicated to serving their Subscribers. Each Subordinate CA is certified by the Top CA (Signit Licensed CA) at Level 1 of the hierarchy, as illustrated in the figure below:

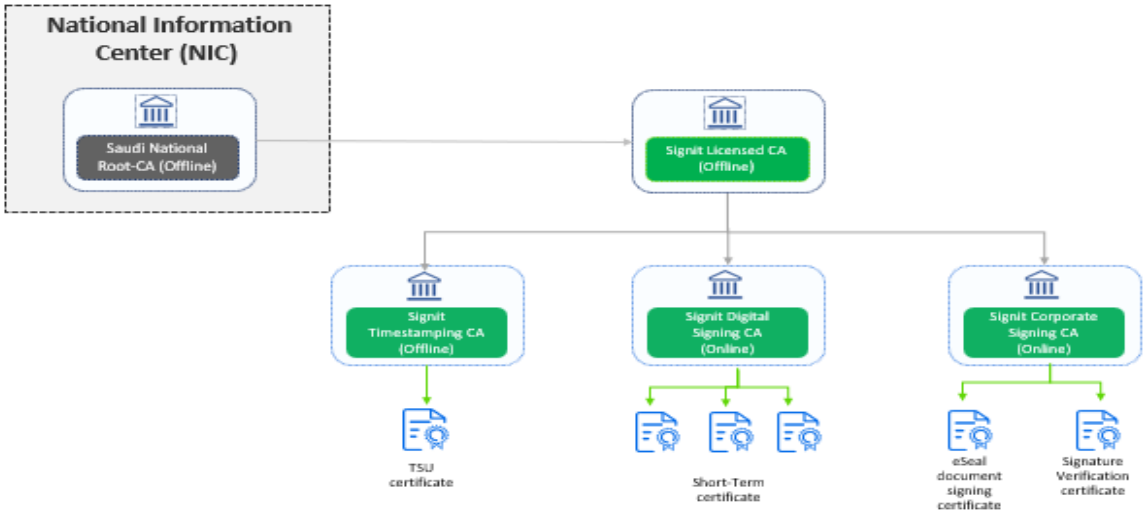


Figure 1 – Signit PKI hierarchy

1.1.1. Signit Governance Board (Signit GB)

Oversight of Signit PKI is performed by **Signit Governance Board (Signit GB)**. Signit GB includes representatives from key organizational functions such as policy, compliance, legal, information security, and technical architecture. Its role is to provide strategic direction and ensure continuous supervision of Signit operations activities.

Signit GB acts as the highest internal authority for certification services covered by this CP/CPS and holds overall responsibility for governance, risk management, and operational oversight. Signit GB is responsible for:

- Maintaining alignment with applicable legal, regulatory, and audit requirements;

- Defining and maintaining the strategy and service scope of Signit certification services;
- Approving and maintaining Signit policies, standards, and practices related to certification operations;
- Supervising the performance and compliance of PKI operational teams;
- Approving major architectural or infrastructure changes affecting certification services;
- Authorizing key ceremonies and overseeing internal and external audit activities;
- Making decisions regarding the response to significant security or operational incidents;
- Overseeing the resolution of disputes related to certification activities;
- Reviewing incidents involving non-compliance with security or operational procedures;
- Providing executive direction during disaster recovery events or other critical operational disruptions

1.2. Document Name and Identification

This document is the "Certificate Policy & Certification Practice Statement (CP/CPS) for High Assurance Certification Services and Timestamping", it's approved by Signit Governance Board (Signit GB) for the publication. This CP/CPS document is published under https://repository.pki.signit.sa/

Signit will use the OID 2.16.682.1.101.5000.1.4.1.4.1.1.1 to identify this document.

The following object identifiers are allocated under Signit arc within the Saudi National PKI OID schema:

Signit PKI OID subtree	
OID	**Description**
2.16.682.1.101.5000.1.4.1.4.1.1.1	This CP/CPS document
2.16.682.1.101.5000.1.4.1.4.1.1.2	Signit Timestamping Policy and Practice Statement
2.16.682.1.101.5000.1.4.1.4.1.2.1.1	Short-term certificates issued to natural persons
2.16.682.1.101.5000.1.4.1.4.1.2.2.1	Remote eSeal certificates, Signit-managed key-generation model
2.16.682.1.101.5000.1.4.1.4.1.2.2.2	Local eSeal certificates, applicant-generated key-pair model
2.16.682.1.101.5000.1.4.1.4.1.2.2.3	Signature validation certificates
2.16.682.1.101.5000.1.4.1.4.1.2.3.1	TSU certificates for the Signit Timestamping Service

The certificate policy object identifier applicable to a given certificate is included in that certificate, as specified in the certificate profiles in Section 7.1.10.

1.3. PKI Participants

PKI participants within the scope of this CP/CPS are the entities and roles that hold specific rights and obligations in relation to the issuance, management, and use of certificates under Signit certification infrastructure. These participants include Certification Authorities, Registration Authority functions, Subscribers, Relying Parties, and other supporting entities involved in governance or audit activities.

1.3.1. Certification Authorities

Signit operates a multi-tier Certification Authority (CA) hierarchy designed to separate CA certificate management functions from online certificate issuance activities.

1.3.1.1. Signit Licensed CA

The top-level Certification Authority (hereafter Signit Licensed CA) represents the upper tier of Signit PKI hierarchy. Signit Licensed CA public key certificate is digitally signed by the publicly trusted Saudi National Root CA, which is managed by the National Information Center (NIC) and which is distributed through common software trust stores. Signit Licensed CA operates under strict security controls and is used exclusively to issue certificates to subordinate CAs.

1.3.1.2. Signit Subordinate CAs

Subordinate CAs operate online and are responsible for issuing certificates to subscribers and system components in accordance with this CP/CPS. These authorities enforce certificate lifecycle controls, including issuance, renewal, revocation, and publication of certificate status information.

Signit Subordinate CAs may include:

- **Signit Digital Signing CA & Signit Corporate Signing CA**
  Responsible for issuing high-assurance certificates for natural persons and legal entities, as well as certificates used for validation-related services such as OCSP responder and Signature Validation. These Certification Authorities are collectively referred to as the **"Document Signing CAs".**
- **Timestamping Certification Authority (hereafter Signit Timestamping CA)**
  Responsible solely for issuing certificates used by Timestamping Units (TSU). This CA issues TSU signing certificates in addition to OCSP responder certificates.

1.3.2. Registration Authorities

1.3.2.1. Signit RA

The Registration Authority (RA) performs identification and authentication of certificate applicants and supports certificate lifecycle processes on behalf of the Certification Authorities.

Signit operates its Registration Authority function internally and may authorize Reliable KYC Providers to perform defined registration activities for Natural Person short-term certificates in accordance with this CP/CPS and the applicable agreement with Signit.

For Legal Person certificates, Signit RA performs the applicable registration and certificate request approval activities in accordance with this CP/CPS.

For Natural Person short-term certificates, identity proofing is performed using the SDAIA NAFATH national identity scheme. Identity proofing may be performed through Signit's own

integration with NAFATH or through an authorized Reliable KYC Provider that uses NAFATH and interacts directly with the Applicant during the registration process.
The Reliable KYC Provider is responsible for:

- Verifying and authenticating the Applicant using NAFATH;
- Verifying the NAFATH authentication response;
- Presenting the applicable Signit Subscriber Agreement to the Applicant and obtaining the Applicant's explicit acceptance of that agreement;
- Obtaining the Applicant's consent and completing the authentication required for the certificate and signing request;
- Creating a digitally signed assertion containing the verified subscriber information and the information required to process the request; and
- Securely submitting the signed assertion and the request information to Signit.

The Reliable KYC Provider shall ensure that its registration activities comply with this CP/CPS and its agreement with Signit.
Signit remains responsible for the certificate registration process and for ensuring that the identity information and other required conditions for certificate issuance have been successfully validated before the certificate is issued. This includes validating the authenticity, integrity and validity of the signed assertion and request information received from the Reliable KYC Provider.
Signit RA function is responsible, as applicable, for:

- verifying the identity of applicants using reliable data sources;
- reviewing and approving certificate issuance and revocation requests;
- submitting validated requests to the appropriate Certification Authority;
- ensuring that applicant information is processed and retained in accordance with this CP/CPS;
- supporting operational processes related to certificate lifecycle management

1.3.3. Subscribers

Subscribers are natural persons or legal entities to whom certificates are issued. Subscribers are responsible for complying with the obligations defined in this CP/CPS and any applicable Subscriber Agreement, including the protection of private keys and activation data under their control.
Certificates may be issued to:
a) **Natural Persons** — where the subscriber is the individual requesting the certificate and is directly accountable for its use.
b) **Legal Entities** — where the subscriber is an organization requesting certificates for electronic sealing purposes. eSeal certificates are issued under one of two key generation models, described in Section 6.1.1.2. Under the Signit-managed key-generation model, the key pair is generated and held within a cryptographic module operated by Signit. Under the applicant-generated key-pair model, the key pair is generated and held within a cryptographic module provided by the applicant and approved by Signit. Each model is identified by its own certificate policy object identifier, as set out in Section 1.2.

1.3.4. PKI service components operated by Signit

1.3.4.1. Timestamping Service:

The Timestamping Service is provided by Signit through the Time-Stamping Unit (TSU) component within Signit infrastructure. TSU is responsible for generating electronic timestamps and uses certificates issued by Signit Timestamping CA exclusively for timestamping operations. TSU certificates are issued to Signit for the operation of its timestamping service and shall not be used for any other purpose.

1.3.4.2. Signature Validation Service

Signature Validation Service is a PKI component operated by Signit to produce validation responses. Certificates issued for this service support the integrity and authenticity of validation responses. Signature validation certificates are issued to Signit for operation of this service.

1.3.5. Relying Parties

Relying Parties are natural persons or legal entities that rely on a Certificate and/or a digital signature, or electronic seal verified using the public key contained in that Certificate. Before relying on certificates or signatures issued under this CP/CPS, Relying Parties shall ensure:

- The validity of the certificate with regards to algorithms and procedures defined in RFC 5280.
- The validity of the certificate through the relevant CA Certificate Revocation Status Services (e.g., OCSP, CRL; see Chapter 7 for detailed information).
- The context in which the certificate is used against the OIDs of the certificates (See applicable Certificate Policy).

Relying Parties shall also comply with the Relying Parties obligations and liabilities as stated in the relevant sections of this CP/CPS.

1.3.6. Other Participants

Other Participants include:

- **Digital Government Authority (DGA)** - The Digital Government Authority (DGA) is the regulator of Digital Trust Services in the Kingdom of Saudi Arabia.
- **National Information Center (NIC)** - the entity responsible for the Saudi National Root CA.
- **Saudi Data & AI Authority (SDAIA)**: Operates the Saudi National Identity scheme (NAFATH) used to perform identity proofing of subscribers applying for natural person certificates.
- **Qualified independent WebTrust auditors** - Verifies the requirements set out in section 8.2
- **Reliable KYC Providers –** Organizations eligible under the applicable Saudi regulatory and National PKI requirements and authorized under an agreement with Signit to perform defined registration activities for Natural Person short-term certificates in accordance with this CP/CPS.
  A Reliable KYC Provider is responsible for:
  - Verifying and authenticating the Applicant using NAFATH;
  - Verifying the authentication response before using the resulting identity information;
  - Presenting the applicable Subscriber Agreement and obtain the Applicant's explicit acceptance of its terms and consent to certificate issuance and use;
  - Performing the authentication required for each certificate and signing request;
  - Creating a digitally signed assertion containing the verified subscriber information and the information required to process the request;
  - Securely submitting the signed assertion and request information to Signit; and
  - Performing its activities in accordance with this CP/CPS and its agreement with Signit.

Subject to the applicable Saudi regulatory and National PKI requirements, the following entities may be eligible to act as Reliable KYC Providers:

- The National Information Center and its authorized KYC service providers, partners or agencies;
- Organizations that verify their customers' identities through NAFATH, either directly or through a KYC service provider authorized by the National Information Center.
- Organizations that collect and verify the identity information of their own customers as part of a formal customer registration process carried out in accordance with applicable Saudi regulatory requirements, provided that the identity verification relied upon for certificate issuance is performed through NAFATH in accordance with Section 3.2.3.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

The certificates issued pursuant to this CP/CPS may be used for:

1) **Signit Licensed CA:**
   Signit Licensed CA shall be used exclusively for issuing and verifying certificates for Subordinate CAs and its designated OCSP responder, as well as for signing Certificate Authority Revocation Lists (CARLs) related to those Subordinate CAs. The designated OCSP responder signs the OCSP responses using its own private key. Signit Licensed CA does not issue end-entity certificates directly.
2) **Signit Subordinate CAs:**
   The Subordinate CAs (i.e., Signit Digital Signing CA, Signit Corporate Signing CA, and Signit Timestamping CA) certificates may be solely used for signing and verifying the certificates they issue, including their designated OCSP responder certificates, and the lists of the certificates revoked by the Subordinate CA (CRLs). The designated OCSP responders sign the OCSP responses using their own private keys.
3) **Certificate for Legal person:**
   eSeal certificates are used to create and verify high-assurance electronic seals on documents issued or attested by a legal entity. They may also be used to seal documents or transaction evidence associated with simple electronic signatures, providing assurance of the origin and integrity of the sealed evidence.
4) **Natural Person certificates:**
   Used to produce and verify high assurance digital signatures on documents/eTransactions.
5) **TSA service certificates**
   These certificates are issued by Signit Timestamping CA to create and verify electronic time stamps. TSU Certificates issued under this CP/CPS to Signit itself are used to provide the Time Stamping Service, in accordance with the Time Stamping Policy and Practice Statement, available under https://repository.pki.signit.sa/
6) **Signature Validation Certificates:**
   Certificates used by the signature validation service to digitally sign validation reports or responses resulting from the cryptographic and policy-based verification of electronic signatures and seals.
7) **OCSP Responder Certificates**
   Used to sign and verify the Online Certificate Status Protocol (OCSP) responses for certificates issued by the Issuing CA.

1.4.2. Prohibited Certificate Uses

Certificates issued under this CP/CPS shall be used only for the purposes specified in Section 1.4.1 and in accordance with the applicable certificate profile, Key Usage and Extended Key Usage extensions, Subscriber Agreement, and applicable legal and regulatory requirements.

Any unlawful, unauthorized or misleading use of a certificate, or any use inconsistent with this CP/CPS, is prohibited. Signit shall not be liable for claims arising from a certificate use that is not permitted under this CP/CPS.

1.5. Policy Administration

1.5.1. Organization Administering the Document

Signit GB holds overall responsibility for the development, maintenance, approval, and publication of this CP/CPS. Signit GB ensures that the document remains aligned with applicable legal, regulatory, and audit requirements and reflects the current operational practices of Signit certification infrastructure.

1.5.2. Contact Person

Requests for information, clarification, or comments related to this CP/CPS shall be directed to the designated Signit contact responsible for certification policy administration at:

Signit POLICY ADMINISTRATION
8479 Al Mashaf, Ar Rabie Dist, Riyadh 13316
Kingdom of Saudi Arabia
Email: cert.info@signit.sa

Signit accepts official correspondence related to this CP/CPS only through the designated contact channels.

Certificate Problem Report

Signit maintains a continuous 24/7 ability to internally respond to any high priority revocation requests and certificate problem reports provides instructions for certificate revocation and certificate problem reporting on a dedicated page in its public repository, accessible at https://repository.pki.signit.sa/certificate_problem_report. If Signit deems appropriate, it may forward the revocation reports to law enforcement authorities.

Subscribers, relying parties, application software suppliers, and other third parties can report suspected key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to any certificates issued by Signit by sending an email to **cert.problem@signit.sa** .

Signit GB will validate and investigate the request before taking an action in accordance with section 4.9.

1.5.3. Person Determining CP/CPS Suitability for the Policy

Signit GB is responsible for determining the suitability and continued applicability of this CP/CPS. This evaluation considers internal risk assessments, operational changes, and recommendations provided by independent auditors as described in Section 8

1.5.4. CP/CPS Approval Procedures

Signit Governance Board formally approves this CP/CPS and any subsequent revisions prior to publication in Signit public repository.

Proposed updates are reviewed by a specialist staff belonging to Signit GB to ensure consistency with The Saudi National Root CA CP, the applicable laws and regulations of the Kingdom of Saudi Arabia, industry best practices, applicable standards, and Signit operational environment. Revisions may be issued as updated versions of this document or through formal amendment notices. All changes are tracked through a document revision history.

Each updated version becomes effective upon publication in the repository and supersedes previous versions. Until publication, the previously approved version remains in force.

Once approved and published, Signit shall formally notify the NIC to enable timely updates to the Common CA Database (CCADB), in accordance with the applicable CCADB Policy requirements.

1.6. Definitions and Acronyms

1.6.1. Definitions

Applicant - A natural person or Legal Entity that requests the issuance or renewal of a Certificate. Once the Certificate is issued, the Applicant becomes the Subscriber.

Applicant Representative - A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA. In the context of this CP/CPS, the applicant representative is in charge of submitting certificate requests and certificate revocation requests on behalf of the applicant. The words Applicant representative and requester are used interchangeably.

Application Software Supplier - A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

Audit Period - In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA)

Audit Report - A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

Authorized Representative - A natural person authorized to act on behalf of a Legal Entity in relation to certificate requests and certificate lifecycle actions. The Authorized Representative is either the entity's Official Representative, being an individual who holds authority to represent the entity by virtue of their position, or a Delegated Representative acting under authority formally delegated by the Official Representative. The Authorized Representative approves the certificate request and accepts the applicable Subscriber Agreement on behalf of the entity. The Official Representative and Delegated Representative roles are described in the Signit RA Process Document.

Digital signature - data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

CA Key Pair - A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

Certificate - An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Data - Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process - Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy - A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements. In the context of this document, the Certificate Policy may be combined with the Certification Practice Statement (CP/CPS) to describe both the policy requirements and the operational practices implemented by Signit.

Certificate Problem Report -Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List - A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority Revocation List (CARL) - revocation list containing a list of CA-certificates issued to certification authorities that have been revoked by the certificate issuer.

Certification Authority - An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Signit Licensed CA and Subordinate CAs.

Certification Practice Statement - A document describing the practices and operational procedures implemented by Signit for the creation, issuance, management, revocation, and lifecycle control of Certificates. The CPS defines how the requirements set forth in the applicable Certificate Policy are implemented in practice. In this context, the CPS is combined with the Certificate Policy and published as a single CP/CPS document.

Certificate Profile - A set of documents or files that defines requirements for Certificate content and Certificate. Section 7 of this CP/CPS provides a list of the certificate profiles defined within it.

Control - The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management or legal nature

Country - Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

CSPRNG - A random number generator intended for use in cryptographic systems.

Delegated Third Party - A natural person or Legal Entity that is not Signit but that performs, under a written agreement with Signit, one or more functions or operational activities falling within the scope of this CP/CPS, including the performance of Trusted Roles. Signit remains responsible for the performance of any function delegated in this way.

Entity Authorization Letter - A document issued by a Legal Entity and signed by its Authorized Representative, confirming that a named individual is authorized to act on the entity's behalf in relation to certificate requests and certificate lifecycle actions. An equivalent corporate document serving the same purpose may be accepted.

Expiry Date - The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

High Assurance certificate - As defined in the Saudi National Root CA CP (https://sdaia.gov.sa/en/Sectors/Nic/ca/Pages/default.aspx) issued by SDAIA, a High Assurance certificate is a digital certificate issued under the High Assurance level applicable to Saudi National Root CA participants. This level includes a stringent identity proofing process performed by a Registration Authority prior to certificate issuance, and requires that digital certificates issued to Subscribers are held on hardware.

Issuing CA - In relation to a particular Certificate, the CA that issued the Certificate. This may include the issuance of Signit Licensed CA certificates, Subordinate CA certificates, TSU certificates, OCSP responder certificates, or end-entity certificates, as applicable under this CP/CPS.

Key Compromise - A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Generation Script - A documented plan of procedures for the generation of a CA Key Pair.

Key Pair - The Private Key and its associated Public Key.

Reliable KYC Provider – An organization eligible under the applicable Saudi regulatory and National PKI requirements and authorized under an agreement with Signit to perform defined registration activities for Natural Person short-term certificates in accordance with this CP/CPS.

Legal Entity - An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Multi-Factor Authentication - An authentication mechanism consisting of two or more of the following independent categories of credentials (i.e. factors) to verify the user's identity for a login or other transaction:

1. something the user knows (knowledge factor);
2. something the user has (possession factor); and
3. something the user is (inherence factor).

Each factor is independent of the other(s).

Object Identifier - A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder - An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol - An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

Private Key - The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key - The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure - A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly-Trusted Certificate - A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor - A natural person or Legal Entity that meets the requirements of Section 8.2.

Random Value - A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registration Authority (RA) - Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA. In the context of this CP/CPS, the RA function is operated by Signit. Under this CP/CPS, Signit operates the RA function and may use Reliable KYC Providers to perform the activities described in Sections 1.3.2 and 1.3.6.

Reliable Data Source - An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication - A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party - Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository - An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Request Token - A value, derived in a method specified by the CA which binds this demonstration of control to the certificate request. Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; or (ii) a hash of the Subject Public Key Info [X.509]; or (iii) a hash of a PKCS#10 CSR.

Root CA - The top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Signit Licensed CA Certificates. In the context of the present document, it refers to the Saudi National Root CA operated by NIC.

Root Certificate - The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to Signit. In the context of the present document, it refers to the Saudi National Root CA certificate operated by NIC.

short-term certificate: certificate whose validity period, i.e. the period of time from notBefore through notAfter, inclusive, is shorter than the maximum time to process a revocation request as specified in the present certificate practice statement. Due to its limited validity, a Short-Term Certificate may not require revocation mechanisms such as CRL or OCSP publication, provided that its expiration occurs before any potential revocation could be processed and propagated.

Subject -The natural person, Legal Entity, Certification Authority or service component identified in a Certificate and associated with the public key contained in that Certificate.

Subject Identity Information - Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA - A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA. In the context of the present document, Signit subordinate CA(s) are signed by Signit Licensed CA.

Subscriber - A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement - An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Terms of Use - Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the baseline requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Trusted Role - Those individuals who perform a security role that is critical to the operation or integrity of a PKI.

Trustworthy System - Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Timestamping Authority (TSA) - The Certification Authority (CA) of the Timestamping Services, which issues Time-Stamping Units (TSUs) and OCSP responder certificates. In the context of the present document, the Timestamping Authority is Signit Timestamping CA.

Time Stamp Token - Data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.

Timestamping Unit - Set of hardware and software which is managed as a unit and has a single Time Stamp Token signing key active at a time, used in the service of issuing electronic time stamps.

Valid Certificate - A Certificate that passes the validation procedure specified in RFC 5280.

Validity Period - From RFC 5280 (http://tools.ietf.org/html/rfc5280): "The period of time from notBefore through notAfter, inclusive."

1.6.2. Acronyms

Acronym	Description
AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CC	Common Criteria
CCADB	Common CA Database
CCTV	Closed Circuit TV
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CP/CPS	Certificate Policy and Certification Practice Statement
CRL	Certificate Revocation List
CARL	Certificate Authority Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As
DGA	Digital Government Authority
NIC	National Information Center
NTR	National trade register.
DN	Distinguished Name
DNS	Domain Name System

Acronym	Description
FIPS	Federal Information Processing Standards
EID	Electronic Identity Card
EAL	Evaluation Assurance Level
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IPSEC	Internet Protocol Security
ISO	International Standards Organization
KYC	Know Your Customer
NAFATH	Saudi national single sign-on and identity verification service operated by SDAIA
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS#1	Public Key Cryptography Standards (PKCS) #1
PKCS#7	Cryptographic Message Syntax
PKCS#10	Certification Request Syntax Specification
PKI	Public Key Infrastructure
RA	Registration Authority
RSA	Rivest-Shamir-Adleman (The names of the inventors of the RSA algorithm)
RTO	Recovery Time Objective
SDAIA	Saudi Data and Artificial Intelligence Authority
TLD	top-level domain
TSA	Timestamping Authority
TSU	Timestamping Unit
TSP	Trust Service Provider
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier, a URL, FTP address, email address, etc.
URL	Universal Resource Locator

1.6.3. References

This document refers to the following:

- Saudi National Root CA Certificate Policy (v3.7)
- Electronic Transactions Law (Royal Decree No M/18, 8 Rabi'1 – 1428H -26 March 2007)
- Personal Data Protection Law (PDPL), issued by Royal Decree No. M/19 dated 9 Safar 1443H, corresponding to 16 September 2021, as amended by Royal Decree No. M/148 dated 5 Ramadan 1444H, corresponding to 27 March 2023, and its Implementing Regulations.
- X.509 - The standard of the ITU-T (International Telecommunications Union-T) for Certificates.
- RFC3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities
- ETSI EN 319 421 v 1.2.1 (2023-05) – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
- ETSI EN 319 422 v 1.1.1 (2016-03) – Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

2. Publication and Repository Responsibilities

2.1. Repository

Signit maintains an online public repository that is available on a continuous basis (24 X 7) and accessible through a designated web address at: https://repository.pki.signit.sa/

Signit is responsible for ensuring that the repository contains current and relevant information relating to its certification services, including:

- the current and historical versions of this CP/CPS;
- subscriber agreements, relying party agreements, and related policy documentation;
- the Timestamping Policy and Practice Statement and associated disclosures, where applicable;
- Certification Authority certificates;
- Certificate Revocation Lists (CRLs), Certification Authority Revocation Lists (CARLs), and status service information (OCSP responder certificates);
- Timestamping Unit (TSU) certificates;
- applicable audit reports.

The repository is intended to provide relying parties and other stakeholders with access to authoritative information required to validate certificates issued under Signit PKI.

2.2. Publication of Certification Information

Signit is responsible for preparing and publishing certification information described in Section 2.1. Certificate status information is made available on a continuous basis (24 x 7) to support certificate validation.

Signit provides certificate validity status through:

- Regularly published CRLs and CARLs, including updates reflecting newly revoked certificates. Certificate profiles include a CRL Distribution Point (CDP) extension referencing the applicable revocation information;
- An Online Certificate Status Protocol (OCSP) responder compliant with RFC 6960, with responder locations identified within the Authority Information Access (AIA) extension of issued certificates.

Certificate status services are designed to be accessible at all times, subject to planned maintenance or unforeseen operational events.

2.3. Time or Frequency of Publication

Signit GB reviews this CP/CPS at least annually to ensure continued alignment with applicable standards, operational practices, and regulatory expectations. Where updates are required, revised versions are approved and published within five (05) days following governance approval.

If no substantive changes are required, the document review may still be recorded through a version update and documented change log entry.

Updated versions of the CP/CPS and related agreements become effective upon publication in the public repository.

2.3.1. CA Certificates

Certification Authority (i.e., CA) certificates and OCSP responder certificates are published to the repository promptly following issuance. These certificates remain publicly available until

expiration or replacement, after which they may be retained within an archive section for historical and audit purposes.

Operational use of newly issued CA or OCSP certificates is permitted only after successful publication within the repository.

2.3.2. Certificate Revocation Lists

2.3.2.1 Signit Licensed CA

CARLs issued by Signit Licensed CA are published at defined intervals according to the following rules:

- At minimum, once every twelve (12) months, at an agreed time and always prior to the NotAfter date of the currently active CARL. Additionally, a new CARL will be generated and published within 24 hours following the revocation of any Subordinate certificate,
- CARLs lifetime shall be set to 12 months.

2.3.2.2 Subordinate Certification Authorities

CRLs issued by subordinate CAs are published according to defined operational intervals:

- **Document Signing CAs**
  CRLs are refreshed at regular intervals not exceeding 24 hours, regardless of whether new revocations have occurred. CRLs lifetime shall be set to 26 hours.
- **Signit Timestamping CA**

  CRLs are refreshed at regular intervals not exceeding 30 days, regardless of whether new revocations have occurred. CRLs lifetime shall be set to 31days.

2.4. Access Controls on Repositories

Information published within Signit repository is publicly accessible for read-only access. Signit implements logical and physical security measures to prevent unauthorized modification, deletion, or insertion of repository content.

Access controls, monitoring mechanisms, and change management procedures are implemented to preserve the integrity and availability of published information.

3.Identification and Authentication

3.1. Naming

3.1.1. Types of Names

The types of names assigned to the CAs, and Subscriber certificates are detailed in Section 7 of this document. All such certificates contain X.501 Distinguished Names in the Issuer and Subject fields.

3.1.2. Need for Names to be Meaningful

Subscriber Certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate.

CAs certificates contain names with commonly understood semantics permitting the determination of the identity of the CA.

3.1.3. Anonymity or Pseudonymity of Subscribers

This CP/CPS does not permit anonymous or pseudonymous subscribers.

3.1.4. Rules for Interpreting Various Name Forms

Fields contained in Digital Certificates are following this CP/CPS and the Digital Certificate Profiles detailed in section 7.
The naming convention used by Signit is based on ISO/IEC 9595 (X.500) standards and ASN.1 syntax.

3.1.5. Uniqueness of Names

As per section 7 of this CP/CPS, Signit enforces uniqueness of subject DNs as follows:

Legal Entity Certificates - uniqueness is enforced through the combination of the organization's legal name, a unique organization identifier, and, where applicable, the Organizational Unit (OU) attribute. The OU field is used to distinguish between certificates issued to different departments, systems, or functional units within the same organization, ensuring that each certificate has a unique DN even when multiple certificates are issued to the same legal entity.

Natural Persons Certificates - uniqueness is enforced through the combination of Surname, Givenname, CN and unique serialnumber.

Signature verification Service Certificates - The uniqueness of the Distinguished Name is ensured through the combination of the organization's legal name, a unique organization identifier and the common name attribute value in the Subject field of the signature verification service certificate

TSA Service Certificates - The uniqueness of the Distinguished Name is ensured through the combination of the organization's legal name, a unique organization identifier and the common name attribute value in the Subject field of the TSU certificate.

OCSP Certificates - The OCSP responder unique name is included in the subject DN of issued OCSP certificate at each issuing CA level.

3.1.6. Recognition, Authentication, and Role of Trademarks

Applicants agree by submitting a certificate request to Signit Subordinate CAs that their request does not contain data which in any way interferes with or infringes upon the rights of any third parties in any jurisdiction with respect to trademarks, service marks, trade names, company names, "doing business as" (DBA) names, or any other intellectual property right, and that they are not presenting the data for any unlawful purpose whatsoever.

Signit has the right to revoke a certificate or certificates containing a disputed subject name, as well as upon receipt of a properly authenticated order from DGA, NIC or a court of competent jurisdiction mandating such action.

3.2. Initial Identity Validation

The following methods described in this Section are used to ascertain the identity of a Subscriber.

3.2.1. Method to Prove Possession of Private Key

The possession of the private key, corresponding to the public key for which a certificate is requested, is demonstrated through the submission of a Certificate Signing Request (CSR). The CSR complies with the PKCS#10 standard and includes the public key, which is digitally signed using the corresponding private key.

Under the Signit-managed key-generation model, private keys are generated and securely stored under the control of the Subscriber within a Hardware Security Module owned and operated by Signit. Access to these keys by the Subscriber is protected through multi-factor authentication mechanisms, designed to ensure a level of assurance of sole control equivalent to that provided where the key is held locally by the Subscriber.

Under the applicant-generated key-pair model for eSeal certificates, the key pair is generated by the applicant within its own cryptographic module as described in Section 6.1.1.2. Possession of the private key is demonstrated by the PKCS#10 certificate signing request uploaded through WebRA, which is signed using that private key and validated by Signit before the certificate request is approved.

3.2.2. Authentication of Organization Identity

The authentication of an organization's identity is performed in accordance with applicable laws and regulations of the Kingdom of Saudi Arabia and is based on documented and verifiable validation processes.

The organization's identity is established using reliable and authoritative data sources that provide official information about the legal entity, including its registered legal name, registered address, unique organization identifier, and details of its authorized representatives.

For this purpose, Signit verifies the existence and legal status of the organization by collecting and validating information from the Saudi Ministry of Commerce commercial registry (https://mc.gov.sa/en/eservices/Pages/default.aspx). This registry is periodically updated and is recognized as a Reliable Data Source for entities operating within the Kingdom of Saudi Arabia.

Where an organization cannot be verified through the Saudi Ministry of Commerce commercial registry, including government entities, foreign entities without a Saudi Commercial Registration, and non-profit, charitable or other legal entities registered outside the Commercial Registry, Signit verifies the organization's existence and legal status through the applicable official registry or other authoritative source designated by the relevant Saudi government authority for that entity

type, or, in the case of a foreign entity, through the equivalent official registry of its country of establishment.

Where the organization does not hold a Saudi Unified National Number, the identifier issued by that authoritative source is used in its place for the purpose of populating the OrganizationIdentifier field of the certificate, in accordance with Section 7.1.10.3.1.

Previously verified organization information may be relied upon by Signit for a maximum period of twelve (12) months from the date of verification. After that period, the information shall be re-confirmed against the applicable authoritative source before it is relied upon for a further certificate request. This requirement is in addition to any earlier update triggered by the Subscriber's obligation under Section 9.6.3 to notify Signit of changes to the entity's registered information.

Where deemed necessary, the Registration Authority (RA) Officer may conduct a physical site visit to confirm the organization's registered address and presence.
To ensure proper association between the certificate and its subject, the RA Officer verifies that the information provided in the certificate application matches exactly the information to be included in the issued certificate.

Upon successful completion of the verification process, the legal entity and its authorized representative are formally enrolled in Signit RA system. Verification of the authority and entitlement of the individual requesting the certificate on behalf of the organization is performed in accordance with Section 3.2.5 of this CP/CPS.

3.2.3. Authentication of Individual Identity

The Individual's identity who is the subscriber of a high assurance certificate is verified based on SDAIA NAFATH system. The identity verification may be performed directly through NAFATH as part of Signit's certificate application process, or through a Reliable KYC Provider. Where a Reliable KYC Provider is used, it verifies the Applicant's identity and the NAFATH authentication response and securely provides Signit with a digitally signed assertion containing the verified identity information required for certificate issuance.

Before issuing the certificate, Signit verifies the authenticity, integrity and validity of the signed assertion received from the Reliable KYC Provider.

Verified identity attributes may include full name, National ID number, date of birth, and other relevant identifiers required for certificate issuance.

The identity proofing process is detailed in a documented internal procedure maintained by Signit.

3.2.4. Non-verified Subscriber Information

All fields constituting the subscriber information written in the certificate are verified. The Subject or the Subscriber, as the case may be, is responsible for providing up-to-date, accurate and correct information during the registration process.

3.2.5. Validation of Authority

Signit verifies whether a natural person has specific rights, entitlements, or permissions, including the mandate to act on behalf of a legal entity to obtain a certificate (eSeal certificate).

For Legal Person certificates, this verification is performed as follows:

the authority of the Authorized Representative is established from the entity's commercial registration extract, or from another authoritative source identifying that individual, or from a formal delegation issued by the entity's Official Representative;

the authority of the Requester is established from the Entity Authorization Letter or equivalent corporate document issued by the Authorized Representative, as described in Section 4.2.1;

the RA Officer confirms that the individuals named in the submitted evidence match the individuals recorded in the certificate application and, where the evidence is not conclusive, seeks confirmation from the entity through a Reliable Method of Communication.

The evidence relied upon for this verification is retained with the certificate application in accordance with Section 5.5.1.

3.2.6. Criteria for Interoperation

Signit operates under the authority and framework of the Saudi National Root CA and fully adheres to the interoperability criteria defined in the Saudi National Root CA CP and CPS. Accordingly, Signit ensures that its certificate profiles, directory services, and status validation mechanisms conform to the technical and procedural requirements mandated by the Saudi National Root CA. Any interoperability, cross-certification, or trust relationship established by Signit shall strictly follow the provisions and approval processes outlined in Section 3.2.5 of the Saudi National Root CA CP.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-key

Routine re-key activities are performed to replace an existing key pair with a new key pair while maintaining continuity of service. The identification and authentication requirements depend on the type of certificate being re-keyed.

3.3.1.1. Signit CA(s) certificates

Routine re-key activities for CAs operated by Signit apply to Subordinate CAs under Signit operational responsibility. Re-keying of Subordinate CA certificates is performed through formally approved key ceremony procedures conducted under multi-person control and dual-authorization principles. New key pairs are generated within approved cryptographic modules and in accordance with the technical and procedural requirements defined in this CP/CPS. Unless formally modified, the certificate characteristics and policy identifiers remain consistent with the existing Certificate Profiles.

The lifecycle and renewal of Signit Licensed CA certificate are governed by the issuing Saudi National Root CA under the custody of the National Information Center (NIC). Signit Licensed CA certificate re-issuance or renewal process is therefore subject to the Saudi National Root CA governance framework and associated signing procedures. Signit participates in preparatory and coordination activities as required but does not independently perform the Saudi National Root CA certificate signing operation.

All CA re-key activities are formally authorized, recorded, and subject to audit oversight to ensure continued trust and compliance with applicable regulatory and audit requirements.

3.3.1.2. End-Entity Certificates

Except for Short-term certificates, which are generated per signing transaction and therefore not subject to routine re-key, identification and authentication for end-entity certificate re-key follow the same procedures applied during the initial certificate issuance process.

Signit verifies that the certificate to be re-keyed is valid, that the subject's identity and attributes remain accurate, and that any applicable subscriber agreements or terms remain current. Where applicable subscriber agreements or terms have been updated since the initial issuance, the re-key process shall require the subscriber to review and explicitly accept the updated terms prior to certificate issuance. Re-key requests shall not be completed until such acceptance is obtained.

End-entity re-key activities include certificates issued to natural persons, legal entities, and Signit-operated PKI service components such as Timestamping Units (TSU), Signature Validation services, and OCSP responders.

The re-key process results in the issuance of a new certificate with a newly generated key pair and unique serial number while maintaining consistency with the applicable certificate profile requirements.

All re-key operations are performed in accordance with documented operational procedures, logged for audit purposes, and subject to the same security controls and authorization requirements as initial certificate issuance.

3.3.2. Identification and Authentication for Re-key after Revocation

Identification and authentication procedures for re-key after revocation is same as during initial certification.

3.4. Identification and Authentication for Revocation Request

All requests regarding the revocation of a certificate are, prior to any action being taken, authenticated by checking if they came from an authorized source.

Signit Licensed CA

Revocation of Signit Licensed CA certificate may be initiated by Signit when circumstances defined in Section 4.9.1.3 occur.

Where revocation is required, Signit shall formally notify NIC, acting as the operator of the issuing Saudi National Root CA, and shall cooperate in the execution of the revocation process.

Because Signit Licensed CA certificate is issued under the custody of the Saudi National Root CA, the technical execution of the revocation is performed by the issuing Root CA in accordance with its policies and procedures.

Signit remains responsible for initiating revocation requests, providing supporting evidence, and ensuring timely coordination with the supervising authority.

Subordinate CAs

Revocation requests are processed by trusted roles within Signit, under the supervision of Signit GB, as part of an authorized and witnessed Key ceremony.

The request is validated by confirming that it comes from an authorized Signit function and that the approval has been formally documented according to internal procedures.

Once validated, the revocation request is executed through an authorized and witnessed key ceremony performed under multi-person control. The detailed circumstances revocation of Subordinate CA certificates are defined in Section 4.9.1.2 of this CP/CPS.

Signit shall notify NIC for any Subordinate CAs revocation.

Legal Person certificates

Acceptable procedures for authenticating the revocation requests include:

- Receiving a formal revocation request form fulfilling the following conditions:
  - The signature of a revocation request form by the subscriber or an applicant representative.
  - The verification of the identity of the requesters against the information available to the RA (provided during the subscriber registration);
  - Communication with the Subscriber to provide reasonable assurances that the revocation request is authentic. Such communication, depending on the circumstances, may include one or more of the following: telephone, e-mail or courier service.
- Communication from the requesting entity through which reasonable assurances that the person or organization requesting revocation is who they claim to be. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

Natural person certificates

Natural Person short-term certificates are issued with a validity period of 30 minutes. Due to this limited validity period, revocation is not applied to these certificates.

Time-Stamping Unit (TSU) and Signature Validation Service Certificates

Time-Stamping Unit (TSU) and signature validation service certificates are issued to Signit for the operation of its trust service components. Revocation requests for these certificates shall be authenticated before execution and may be initiated only by authorized Signit trusted roles responsible for PKI and Signit service operations.

Authentication includes confirming that the request originates from an authorized internal function and that the action has been formally approved in accordance with Signit operational procedures.

Revocation of TSU and signature validation service certificates may be initiated under the circumstances defined in Section 4.9.1.1. Such events are treated as critical incidents and are managed in accordance with Signit Disaster Recovery and Business Continuity Plan (DR/BCP). All revocation actions are logged and retained as auditable records.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

4.1.1. Who Can Submit a Certificate Application

For Signit Subordinate CA certificates:

Certificates applications to Signit Licensed CA are submitted by trusted roles within Signit, under the supervision of Signit GB, as part of an authorized key ceremony. The RA function, authorized by Signit GB, is responsible for setting up Subordinate CAs under Signit Licensed CA.

The approval of any new Subordinate CA shall be subject to formal authorization by the National Information Center (NIC) prior to activation.

For certificates issued to legal persons:

The Applicant representative (i.e., Requester) can submit certificate requests on behalf of the organization or entity. The Requester is responsible for the accuracy of information submitted as part of the certificate application. The RA officer ensures the entity authorized representative approves the certificate request by signing and stamping the certificate request form and the appended subscriber agreement.

Signit does not issue Certificates to entities on an internal blacklist of organizations from whom it will not accept certificate requests. This blacklist is queried by the RA officer whenever it receives any certificate request.

For certificates issued to Natural persons (short-term certificates):

Certificate applications may be initiated by the individual Applicant through an approved Signit channel or submitted on behalf of the Applicant by a Reliable KYC Provider through an approved connection with Signit.

Where a Reliable KYC Provider is used, it verifies the Applicant's identity using NAFATH and submits the certificate request together with a digitally signed assertion containing the verified identity information and other information required by Signit.

The Applicant must accept the Subscriber Agreement and provide the required consent before certificate issuance. Where a Reliable KYC Provider is used, it presents the applicable Subscriber Agreement to the Applicant, records the Applicant's acceptance and consent, and provides the required evidence to Signit.

Service Certificates (OCSP, TSU, Signature Validation Certificates)

Applications for system certificates (e.g., OCSP responder certificates, TSU certificates, Signature Validation certificates) are initiated by trusted roles and executed as controlled operational ceremonies approved by Signit GB, including validation of certificate templates and naming conventions.

4.1.2. Enrollment Process and Responsibilities

Subordinate CAs:

The lifecycle processes for subordinate CA certificates (issuance, re-key, revocation) are governed by Signit-approved key ceremony procedures. Following formal approval by Signit GB, the authorized trusted roles plan and execute the ceremony steps as documented in Signit Key Ceremony documentation.

Legal Entity Certificates:

The enrollment process includes, at minimum:

- The Requester obtains the applicable Subscriber Agreement from Signit repository and the certificate application form from the RA Officer.
- The legal entity's authorized representative signs the application form and accepts/ratifies the subscriber agreement.
- The requester authenticates to the Web RA portal (using multi-factor authentication credentials set up as part of the registration process outlined in an internal RA process document) and submits the certificate application including but not limited to the following:
    - Scanned copy of properly filled and signed application form along with the subscriber agreement.
    - Supporting evidence required for validation of the information contained in the certificate.
- The RA Officer reviews and validates the integrity and authenticity of all submitted documents, in addition to verifying the applicant's identity as specified in Section 3.2.2.
- The following key-generation models may be used:
    - **Signit-managed key-generation model:** Once the certificate request is approved by the RA Officer, the entity's key pair is generated remotely within Signit HSM. The CSR is created using the approved certificate fields and profile requirements, including the DN attributes, key size and key type, and submitted to the relevant Subordinate CA for certificate issuance.
    - **Applicant-generated key-pair model:** Where the key pair is generated by the applicant within an HSM approved by Signit for eSeal key generation and storage, the corresponding PKCS#10 CSR shall be uploaded through WebRA. Following validation and approval of the certificate request by the RA Officer, the CSR shall be submitted to the relevant Subordinate CA for certificate issuance.
- Before an applicant may use the applicant-generated key-pair model, Signit approves the cryptographic module proposed by the applicant. For this purpose the applicant provides:
    - identification of the cryptographic module, including manufacturer, model and firmware version;
    - evidence of its certification against the requirements of Section 6.1.1.2, in the form of a valid certificate reference issued by the applicable certification scheme;
    - confirmation of the location where the module is hosted and of the party operating it; and

- a written undertaking that the key pair is generated within the module, that the private key remains within it and is not exported in plaintext, and that Signit is notified without undue delay of any compromise or suspected compromise of the module.

- The RA Officer records the approval decision and the supporting evidence together with the certificate application. Approval applies to the specific cryptographic module identified, and is re-confirmed where that module is replaced or where its certification status changes. A certificate request under the applicant-generated key-pair model is not approved unless a valid module approval is in place.

Natural persons (short-term) certificates:

- The enrollment process for Short-term Signing Certificates is initiated through an approved Signit channel (e.g., a business application or portal) integrated with Signit PKI.
- The Applicant's identity is verified using NAFATH, either directly as part of Signit's enrollment process or through a Reliable KYC Provider.
- Where identity verification is performed directly, Signit verifies the NAFATH authentication response, presents the applicable Subscriber Agreement to the Applicant and obtains the Applicant's explicit consent for certificate issuance and use.
- Where a Reliable KYC Provider is used:
  - The Reliable KYC Provider directs the Applicant to NAFATH and verifies the authentication response received from NAFATH;
  - The Reliable KYC Provider presents the applicable Subscriber Agreement to the Applicant and obtains the Applicant's explicit consent for certificate issuance and use; and
  - The Reliable KYC Provider creates and digitally signs an assertion containing the verified subscriber information, evidence of the Applicant's consent and the information required to process the request. The signed assertion and request information are securely submitted to Signit.
- Signit validates either the NAFATH authentication response received directly or the signed assertion and request information received from the Reliable KYC Provider before proceeding with certificate issuance.
- Once consent and the required validations are recorded, the certificate is generated and securely delivered to the Subscriber for immediate use within the authorized transaction context.
- The private key is generated and stored in Signit HSM under the sole control of the Subscriber.

Service Certificates (OCSP / TSU / Signature Validation Certificates)

The RA officer and an authorized PKI administrator in trusted role oversee the execution of an operational ceremonies through which these certificates can be issued. Signit GB approves the operational ceremony documentation and validates the embedded certificate template and naming conventions against the provisions of this CP/CPS. Signit GB authorizes then the ceremony and confirms the list of involved trusted role staff.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

Subordinate CAs:

When a request for the issuance of a new Subordinate CA certificate is received, Signit GB performs the following actions:

- Confirms that the request for the establishment of a new Subordinate CA originates from the RA function within Signit and is justified based on operational, legal, or regulatory requirements.
- Validates the certificate profile, including the certificate template and Distinguished Name (DN) structure, ensuring compliance with the requirements defined in this CP/CPS.
- Reviews and approves the list of key ceremony attendees.
- Approves the Key Generation Script and schedules the Key Ceremony date.
- Upon approval, a formal Key Ceremony is conducted during which:
    - Signit Licensed CA private key is activated in accordance with Key ceremony procedures.
    - The Subordinate CA key pair is generated, and its certificate is signed by Signit Licensed CA.
    - The newly issued Subordinate CA certificate is published in the public repository.

Legal Persons Certificates:

- The Requester fills-in the organization registration form as follows:
    - Organization Information
        - Organization's Legal Name
        - Organization Identifier
        - Official Address
        - Main telephone number
    - Authorized Representative Information:
        - Full name and national identity or passport number of the Authorized Representative;
        - Position held within the entity;
        - Official email address and telephone number;
        - Evidence of the Authorized Representative's authority to act on behalf of the entity, such as the entity's commercial registration extract naming that individual, or a formal delegation issued by the entity's Official Representative.
    - Requester (Applicant Representative) Information:
        - Full name of the Requester authorized to submit certificate management requests on behalf of the entity;
        - Position held within the entity;
        - Official email address and telephone number.

- An entity authorization letter or equivalent corporate document, issued by the entity's Authorized Representative, establishes the Requester's authorization to act on behalf of the entity.
- The Requester submits the signed registration form, the authorization evidence as well as other required validation documentation to the RA officer via email,
- The RA officer performs the following minimum mandatory verification steps on the received registration request:
    - Conduct a blacklist check. If the applicant is in the blacklist, the certification application is rejected.
    - Validates the organization's identity and its authorized representative as described in section 3.2.2
    - Verify the authorization of certificate Requester as specified in section 3.2.5,
    - Verify the phone number of the organization by making a random call.
- If all the above validations are passed, the RA officer initiates a process on the Web RA Portal through which the entity and their Requester are registered on the portal based on the information collected from the Requester.
- At this point the requester would be able to login to the Web RA Portal and authenticates to the Web RA portal (using multi-factor authentication credentials set up as part of the registration process) and submits the certificate application including but not limited to the following:
    - Scanned copy of properly filled and signed application form along with the subscriber agreement.
    - Supporting evidence required for validation of the information contained in the certificate.
- The RA Officer is responsible for reviewing and verifying the completeness, integrity, and authenticity of the certificate request and all accompanying documentation.
- Following completion of the required verification, the RA Officer reviews and approves or rejects the certificate request. Under the Signit-managed key-generation model, the key pair and CSR are generated after RA approval. Under the applicant-generated key-pair model, the RA Officer validates the certificate application and the PKCS#10 CSR uploaded through WebRA. In both cases, only an approved CSR shall be submitted to the relevant Subordinate CA for certificate issuance.
- All related Subscriber registration data are stored along with the certificate application.

Natural persons (short-term) certificates:

- The Applicant initiates the certificate request through an approved Signit channel (e.g., a business application or portal) integrated with Signit certificate issuance platform.
- The Applicant's identity is verified using NAFATH, either directly as part of Signit's certificate application process or through a Reliable KYC Provider.
- Where identity verification is performed directly, Signit verifies the NAFATH authentication response and the retrieved identity information.
- For both routes, the Applicant reviews and confirms the retrieved identity attributes, provides explicit consent for their use in the certificate, and accepts the Subscriber

Agreement through the applicable approved channel before the certificate request is submitted for issuance

- Where a Reliable KYC Provider is used, the Reliable KYC Provider:
  - Verifies the Applicant's identity and the NAFATH authentication response;
  - Presents the applicable Subscriber Agreement and obtains the Applicant's explicit acceptance of its terms and consent to certificate issuance and use ;
  - Creates a digitally signed assertion containing the verified subscriber information, evidence of consent and the information required to process the request; and
  - Securely submits the signed assertion and request information to Signit.
- Signit validates the source, signature, integrity, validity and completeness of the signed assertion received from the Reliable KYC Provider and confirms that it is linked to the applicable certificate request.
- The certificate-issuance process continues only after the applicable NAFATH response or Reliable KYC Provider assertion, and the Applicant's consent have been successfully validated.
- Upon successful processing and approval of the certificate application, the private key is generated and securely stored in Signit Hardware Security Module (HSM) under the sole control of the Subscriber, and the Subscriber's identity is cryptographically bound to the certificate request.
- The certificate is issued with a short validity period (i.e. 30 min).
- Identity verification is re-performed for each issuance.
- The certificate request, identity-verification results, signed assertion, consent evidence, validation results and issuance actions are securely logged in Signit's system.

Service Certificates (OCSP / TSU / Signature Validation Certificates)

Issued only under internal ceremony controls, including governance approval of templates and naming conventions.

4.2.2. Approval or Rejection of Certificate Applications

Subordinate CAs are approved only through authorized key ceremonies after Signit GB confirms prerequisites and approvals.

Natural person (Short-term) certificates issued through automated workflows are approved or rejected based on real-time validation results. This includes validation of the NAFATH authentication response received directly by Signit or the signed assertion and request information received from a Reliable KYC Provider. Signit makes the final decision to approve or reject the certificate application. Requests that fail validation are rejected and the applicant is notified through the approved channel.

Legal person certificates are approved only after successful completion of required identity and authority validations. If required verification cannot be completed within five (5) business days due to missing or unverifiable information, the request may be rejected.

Service certificates are approved only through authorized internal ceremonies.

4.2.3. Time to Process Certificate Applications

No stipulations apply other than those mentioned in 4.2.2.

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

Subordinate CAs:

The required Signit operators, keys custodians and other relevant ceremony attendees gather at the ceremony room to conduct the certificate generation ceremony of the subject CA(s).

The key stages of the key ceremony conducted is summarized below:

- Identity verification is done for all the ceremony attendees by the ceremony auditor/witness,
- Ceremony authorization is verified by the ceremony auditor/witness as well as the key custodians,
- Verify the certificate request format (shall be in PKCS#10 format),
- Verify that the certificate request contains valid subscriber data as per the certificate application,

After the successful verification of the above, the following actions are performed:

- The operator submits the certificate request to Signit Licensed CA to perform the certificate signing operation. This certificate signing operation includes linting the Pre-certificate, the to-be-signed certificate (TBS), and the issued certificate using the industry-standard linting tools widely adopted across the sector.
- The operator and the ceremony auditor/witness validate the issued certificate's content against the defined profile, this CP/CPS and the information submitted in the certificate application,
- The certificate is then handed over to the RA function.

Further details on the certificate issuing process are documented in the designated key ceremony documentation.

Legal person certificates:

Once all the validation is done as described in section 4.2.1, the RA officer uses the web RA portal to initiate certificate issuance from the relevant CA based on the CSR generated.

The Certification Authority (CA) will validate the format and structure of the Certificate Signing Request (CSR) and generate a corresponding pre-certificate. The pre-certificate will undergo linting using industry-standard tools to assess its technical conformity and compliance (of each to-be-signed artifact prior to signing it), with applicable standards. Following successful validation, the final certificate will be generated in accordance with the predefined configured certificate template and made available for download from the web RA portal. The CA issues the certificate in "Active" state so that it is ready for use once deployed on the applicable target key store.

Each issued certificate begins its validity at the time of issuance.

Natural person (Short-term) certificates:

The certificate is issued by the CA only after receiving an approved certificate request from Signit signing service following successful processing of the certificate application. Communication between the systems takes place over secure network connections. The CA processes requests only from authenticated and authorized systems.

The CA validates the format and structure of the CSR then generates the certificate in accordance to the configured certificate template. The certificate is then provided to Signit signing service for immediate use with the corresponding private key in the authorized signing transaction.

Each issued certificate begins its validity at the time of issuance.

Service Certificates (OCSP / TSU / Signature Validation Certificates)

The issuance and management of these certificates happen as part of operational ceremonies that are approved by Signit GB to establish: (1) authorizing the ceremony execution, (2) approving the list of ceremony attendees involving the RA officer, a member of PKI operations management, and designated administrators from the PKI operations team, (3) validating embedded certificate templates and naming conventions against the provisions of this CP/CPS.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

Subordinate CA - publication of the issued CA certificate in the repository constitutes notification to stakeholders.

Legal entity certificates - the certificate is made available to the subscriber/Requester through the approved RA channel (i.e., WebRA portal) and an issuance notification may be sent through verified contact channels.

Natural person certificates - notification is provided through the approved user channel (e.g., business application interface).

Service Certificates (OCSP / TSU / Signature Validation certificates) - the designated administrator is notified upon receiving the certificate from RA officer.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Subordinate CAs - acceptance occurs when the CA certificate is successfully installed and activated within the intended CA environment following the key ceremony.

Natural person (Short-term) certificates - Acceptance is immediate and implicit upon issuance, as the certificate is generated on-demand and used directly by the Subscriber within the signing transaction. These certificates are intended for single-use scenarios and therefore do not require a separate acceptance procedure.

If a Short-term certificate is identified as containing incorrect or inconsistent data during its validity period, Signit shall terminate the related signing session and prevent further use of the

private key. If the certificate has already been used, the incident shall be recorded and investigated, and affected parties shall be notified where applicable. Due to the certificate's 30-minute validity period, revocation is not applied.

Any corrected certificate shall require a new identity verification and signing session.

Legal person certificates - acceptance occurs when the subscriber downloads and deploys the certificate, or if no objection is raised within 24 hours of availability through the approved portal/channel.

Service Certificates (OCSP / TSU / Signature Validation certificates) - A certificate deployed on the target system following completion of the authorized internal operational ceremony shall constitute acceptance of the certificate.

4.4.2. Publication of the Certificate by the CA

The CA does not publish end-user certificates apart from sharing it with the Subscriber.

CAs, OCSP responder, TSU and signature verification service certificates are published on Signit repository.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

Signit GB is notified whenever a CA certificate is issued. Where required, Signit may also notify relevant supervisory parties (i.e., NIC) of CA certificate events in accordance with applicable program requirements.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

The Subscriber uses their private key solely and exclusively for the intended purpose (as specified in the "keyUsage" and ''extendedKeyUsage'' fields of the certificate) and always for legal and authorized purposes, in accordance with the general requirements outlined in this CP/CPS and the Subscriber Agreement in force. Although the private key is securely generated and stored in Signit hardware security module (HSM), the key remains under the sole logical control of the Subscriber. Signit has no capability to access or use the Subscriber's private key, ensuring that only the Subscriber can initiate its use.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties providing services or directly relying on Certificates issued in accordance with the applicable CP/CPS must perform the following and assume the responsibility for having performed the following:

- Use software that complies with X.509 standards.
- Successfully perform public key operations as a condition of relying on a Certificate, compliant with RFC 5280.
- Validate a Certificate by using the CA's Certificate Authority Revocation Lists (CARLs) and Certificate Revocation Lists (CRLs) and OCSP in accordance with the Certificate path validation procedure. Signit supplies in this CP/CPS information about the appropriate

services available to verify the validity status of the certificate, such as OCSP and CRL (see also section 4.9.6).

- Untrust a Certificate if it has expired or is revoked.
- Rely on a Certificate only for appropriate applications (and context), considering all the limitations on the use of the Certificate specified in the Certificate, the applicable contractual documents, and the applicable CP/CPS.
- Assent to the terms of the applicable Relying Party Agreement as a condition of relying on a Certificate.

4.6. Certificate Renewal

Certificate Renewal is the act of issuing a new certificate with a new validity period while the identifying information and the public key from the old certificate are duplicated in the new certificate. Certificate renewal is not supported by the Subordinate CAs. Only certificate re-key is supported.

4.6.1. Circumstance for Certificate Renewal

Not applicable.

4.6.2. Who May Request Renewal

Not applicable.

4.6.3. Processing Certificate Renewal Requests

Not applicable.

4.6.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6. Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7. Certificate Re-Key

Certificate re-key refers to the process of issuing a new certificate that contains a newly generated key pair (including a new private key and corresponding public key) for a subject to whom a

certificate has previously been issued by the CA. During this process, subject attributes and other certified information may be updated

Short-term certificates are not subject to re-key, a new certificate is requested for every signing transaction

4.7.1. Circumstance for Certificate Re-Key

Certificate re-key may happen while the certificate is still active, after it has expired, or after a revocation.

4.7.2. Who May Request Certification of a New Public Key

As per the initial certificate issuance.

4.7.3. Processing Certificate Re-Keying Requests

As per the initial certificate issuance.

4.7.4. Notification of New Certificate Issuance to Subscriber

As per the initial certificate issuance.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

As per the initial certificate issuance.

4.7.6. Publication of the Re-Keyed Certificate by the CA

As per the initial certificate issuance.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

As per the initial certificate issuance.

4.8. Certificate Modification

The certificate modification is not supported. In case the Subscriber wants to change the certified information, or the certificate has been revoked due to any of the circumstances mentioned in Section 4.9 and wants to get a new certificate, the Subscriber shall apply for a certificate re-key.

4.8.1. Circumstance for Certificate Modification

Not applicable.

4.8.2. Who May Request Certificate Modification

Not applicable.

4.8.3. Processing Certificate Modification Requests

Not applicable.

4.8.4. Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6. Publication of the Modified Certificate by the CA

Not applicable.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9. Certificate Revocation and Suspension

Signit provides a continuous ability for subscribers to submit certificate requests. This is available through an online system that is accessible 24 x 7 to authenticated subscribers. Certificate suspension is prohibited. Only permanent certificate revocation is permitted. The revocation of subscribers' certificates is handled as per the subsections below.

4.9.1. Circumstances for Revocation

4.9.1.1. Subscriber Certificates

Short-term subscriber certificates are issued with a validity period of 30 minutes. Revocation is not applied to these certificates because their validity period is shorter than the time required to process a revocation request and publish the corresponding certificate status information.
Signit revokes an eSeal Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing the revocation.
2. The Subscriber notifies Signit that the original Certificate request was not authorized and does not retroactively grant authorization.
3. Signit obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise.
4. Signit is notified of, or obtains evidence of, the compromise or suspected compromise of the cryptographic module in which the Subscriber's private key is held under the applicant-generated key-pair model.
5. Signit is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate including but not limited to those identified in Section 6.1.1.2.

Additionally, Signit SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days if one or more of the following occurs:

6. Signit is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement.

7. Signit is made aware that the Certificate was not issued in accordance with the present CP/CPS.
8. Signit determines or is made aware that any of the information appearing in the Certificate is inaccurate.
9. The Certificate no longer complies with the requirements of Sections 6.1.1.2, 6.1.5 or 6.1.6 of this CP/CPS.
10. Signit obtains evidence that the Certificate was misused.
11. If a subscriber loses legal eligibility, is declared absent or deceased, or is dissolved or bankrupt.
12. Revocation is required by this CP/CPS for a reason that is not otherwise required to be specified in this section 4.9.1.
13. Signit is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.
14. The private key of Signit Licensed CA or Signit Subordinate CAs has been compromised.

Once the revocation request is approved, the certificate is permanently revoked and cannot be reinstated.

For TSU and signature verification service certificates

The TSU and signature verification service certificates are issued to Signit itself and are used in the operation of Signit trust services. While this CP/CPS does not define detailed operational revocation procedures for these certificates, revocation shall be triggered immediately if any of the following occurs:

- Compromise or suspected compromise of the private key.
- Cryptographic weaknesses affecting the private key or algorithm.
- Operational changes, such as decommissioning of the TSU or signature verification component.
- Policy or compliance updates that invalidate the continued use of the certificate.

Such incidents are treated as critical and managed in accordance with Signit Disaster Recovery and Business Continuity Plan (DR/BCP) to ensure continuity of services and mitigation of risk.

4.9.1.2. Circumstances for Subordinate CA revocation

The Certificate shall be revoked within seven (7) days if one or more of the following circumstances occurs. Where the relevant circumstance is CA private-key compromise, the Certificate shall instead be revoked within 24 hours in accordance with Section 4.9.12:

1. A formal, authenticated revocation request is submitted by an authorized Signit function (i.e., RA function).
2. The Subordinate CA fails to comply with the terms, policies, or procedures defined in this CP/CPS.
3. The Subordinate CA is found to have violated provisions of the Saudi e-Transactions Act or associated bylaws.
4. Signit identifies that the original request to establish the Subordinate CA was not properly authorized and retroactive authorization is not granted.
5. Evidence is obtained that the private key associated with the Subordinate CA certificate has been compromised or no longer complies with the key management requirements set out in Sections 6.1.5 and 6.1.6.
6. Signit detects or becomes aware of the Subordinate CA certificate being misused or used in a manner inconsistent with its intended purpose.

7. The certificate was issued in violation of this CP/CPS, or the Subordinate CA fails to operate in compliance with its obligations.
8. Any information in the Subordinate certificate is determined to be inaccurate, misleading, or outdated.
9. Signit ceases the operations of the Subordinate CA without insuring an appropriate succession plan.
10. Revocation is explicitly required by any provision of this CP/CPS.

4.9.1.3. Circumstances for Signit Licensed CA revocation

The Signit Licensed CA Certificate will be revoked by NIC within seven (7) days if one or more of the following circumstances occurs:

1. The revocation is requested in writing.
2. Signit fails to comply with the terms and conditions under which the license was granted by the DGA.
3. Signit has contravened any provisions of the Saudi e-Transactions Act and the associated bylaws.
4. Signit notifies the Issuing CA (i.e., Root CA) that the original certificate request was not authorized and does not retroactively grant authorization.
5. NIC obtains evidence that the CA Private Key corresponding to the Public Key in the Certificate has been compromised or no longer complies with the requirements of Sections 6.1.5 and 6.1.6.
6. NIC (i.e., Root CA) obtains evidence that Signit Subordinate CAs Certificates were misused.
7. NIC (i.e., Root CA) is made aware that the CA Certificates were not issued in accordance with or that CA has not complied with this document.
8. NIC (i.e., Root CA) determines that any of the information appearing in the Certificate is inaccurate or misleading.
9. Signit ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate.
10. Signit‘ right to issue Certificates under these Requirements expires or is revoked or terminated, unless the (i.e., Root CA) has made arrangements to continue maintaining the CRL/OCSP Repository.
11. Revocation is required by this policy and Certification Practice Statement.
12. Signit (i.e., subject) has failed to meet its obligations under its agreements with the Saudi National Root CA, those of any applicable CP, PDS and CPS or any other applicable Agreements.

4.9.2. Who Can Request Revocation

For Signit Licensed CA and Subordinate CAs certificates

A revocation of these certificates can be requested by:

1. Signit itself, or
2. DGA and/or NIC at its own discretion (as per revocation reasons listed in section 4.9.1).

For other types of certificates

Revocation can be requested by the following:

- The RA officer of Signit in the cases described in section 4.9.1.1.
- The Subscriber may submit a revocation request for his own certificate.

- Any relying party or application software supplier possessing evidence of compromise of the subscriber's certificate or its usage to promote malware.
- Signit at its own discretion (if for instance a compromise is known for the TSU key).
- Subscribers, relying parties, application software suppliers, and other third parties may submit Certificate Problem Reports to notify Signit of a suspected reasonable cause to initiate the certificate revocation process.

In all cases, only authorized revocation requests are accepted.

4.9.3. Procedure for Revocation Request

Signit Licensed CA:
A request to revoke a certificate shall identify the certificate to be revoked, specify the reason for revocation, and be submitted by an authorized representative of Signit. The revocation request shall be physically delivered to NIC (Root CA owner) or its designated authority and shall be authenticated in accordance with the procedures defined in the applicable agreement.
Subordinate CA
A revocation request for a Subordinate CA Certificate shall be submitted to Signit GB, which serves as the final authority to review and approve such requests.
Upon identification of the circumstances necessitating revocation (as described in Section 4.9.1), Signit GB shall convene an exceptional meeting within twenty-four (24) hours. The purpose of this meeting is to assess the incident, confirm the circumstances triggering the revocation, and determine the applicable revocation reason(s).
Signit GB may request additional information or supporting evidence, which must be provided within a maximum of seventy-two (72) hours. Upon completion of this process, Signit GB shall formally approve and endorse the revocation decision. This decision shall be documented in a report signed by Signit GB members and other relevant parties who participated in the decision-making process.
Following approval, Signit GB shall authorize the execution of a Subordinate CA Revocation Ceremony, which must be conducted no later than seventy-two (72) hours after authorization. The revoked CA certificate shall then be published in the Certificate Revocation List (CRL) of Signit Licensed CA.
Revocation handling by the RA officer of Signit for legal person certificates:

- The RA officer assigns a unique ID to the revocation request. The RA officer records the submitted documents under the assigned ID.
- The RA officer authenticates the Requester's identity as described in section 3.4.
- The RA officer validates the certificate revocation information.
- The RA officer performs any required investigation within the applicable time constraints (as listed in section 4.9.1 of this CP/CPS). This may include any required communication with the certificate subscriber.
- The RA officer executes the certificate revocation.
- The subordinate CA revokes the certificate, and the certificate status is updated[1].
- The RA officer notifies via email the subscriber/the entity requested the revocation of the completion of the certificate revocation operation.
- The RA officer updates their internal blacklist with the details of the revoked certificate, circumstances for revocation and based on this information, potentially change the risk

[1] The new certificate status will appear in the next CRL, while the OCSP responder will immediately make this new certificate status information available to relying party applications

profile of the applicant in the internal blacklist. Such information will be requested by the RA officer prior to processing future certificate requests for the applicant.

Certificate Revocation handling by the RA officer following a Certificate problems reporting:

Signit maintains a continuous 24/7 ability to internally respond to any high-priority revocation requests and certificate problem reports. Signit provides instructions for certificate revocation and certificate problem reporting on a dedicated page in its public repository, accessible at https://repository.pki.signit.sa/certificate_problem_report

Subscribers, relying parties, application software suppliers, and other third parties may submit certificate problem reports via **cert.problem@signit.sa** .

For any certificate problem report, the reporter is requested to include his contact details, suspected abuse and related Subject.

The RA officer begins the investigation of a certificate problem report within 24 hours of receipt and decides whether revocation or other appropriate actions are required based at least on the following criteria:

- The nature of the alleged problem,
- The number of Certificate Problem Reports received about a particular Certificate or Subject,
- The entity making the report (for example, a notification from an Anti-Malware Organization or law enforcement agency carries more weight than an anonymous complaint),
- Relevant local legislation.

In case of deciding that a certificate is going to be revoked because of the certificate problem report, the RA officer executes the revocation procedure as specified earlier in this section.

If Signit deems appropriate, it may forward the revocation reports to law enforcement authorities.

4.9.4. Revocation Request Grace Period

In this CP/CPS, the *revocation grace period* means the time needed for certificate revocation information to propagate through the revocation process and become available to relying parties via Signit's status services (OCSP and/or CRL).

Once Signit has authenticated and approved a valid revocation request and executes the revocation, Signit updates certificate status information through OCSP without undue delay and, in all cases, within the timeframes defined in Section 4.9.5.

The revoked certificate is also included in the next published CRL in accordance with the CRL issuance frequency defined in Section 4.9.7 (and Section 2.3).

Relying Parties that rely on CRLs (rather than OCSP) shall take this publication interval into account when determining certificate status.

4.9.5. Time Within Which CA Must Process the Revocation Request

Except for Short-term subscriber certificates, a proper end entity certificate revocation request is processed within 24 hours upon confirming that it originated from an authorized Subscriber or authorized entity. This process includes updating the certificate's status—immediately through the OCSP responder and in the next published Certificate Revocation List (CRL)—so that relying parties are promptly informed and rely on the most up-to-date status information.

For certificate problem reports, the RA officer of Signit begins investigations within 24 hours from receiving the report. The RA officer initiates communication with the Subscriber and where appropriate, with other concerned authorities (e.g. law enforcement authorities). A preliminary communication on the certificate problem is sent to the Subscriber and to the originator of the problem report.

The RA officer performs further investigations involving Signit GB, the subscriber and other relevant authorities (e.g. law enforcement authorities) to decide on the action to be taken on the subject certificate.

If the investigations results led to one of the certificate revocation circumstances listed in section 4.9.1, then the certificate will be revoked within the timeframe set forth in Section 4.9.1.

Based on the revocation circumstance, the RA officer may agree with subscriber on a plan to issue a new certificate.

Revocation Processing During Disruptive Events

In the event of a system disruption, disaster, or activation of Signit Business Continuity and Disaster Recovery (BC/DR) procedures, revocation requests received prior to, or during, such events are securely recorded and preserved.

Where immediate processing is temporarily not possible due to system unavailability, such revocation requests are processed without undue delay once CA systems are restored.

During recovery operations, the processing of pending revocation requests will be prioritized over certificate issuance activities. Signit ensures that certificate status information is promptly updated through OCSP and CRL publication following recovery.

Detailed operational procedures for handling revocation requests during disruptive events are defined in the Business Continuity and Disaster Recovery Plan.

4.9.6. Revocation Checking Requirement for Relying Parties

Before relying on the information contained in a certificate, the Relying Party shall validate the appropriateness of the certificate for the intended purpose and ensure that the certificate is valid. Signit makes available to relying parties a status information service for certificates based on the OCSP protocol, and access and download of Certificate Revocation Lists (CRLs).

4.9.7. CRL Issuance Frequency

CRLs are issued as per Section 2.3 of this CP/CPS.

4.9.8. Maximum Latency for CRLs

CRLs are issued according to 4.9.7 of this CP/CPS and published in a timely manner. The revocations that happen after the publication of latest CRL become effective immediately upon the publication of the new CRL.

4.9.9. On-Line Revocation/Status Checking Availability

Relying parties will be able to validate the certificates published in Signit Repository by means of a certificate status information service based on the OCSP protocol, or by consulting the CRL and CARL Revocation Lists. Both services are available 24 hours a day, 7 days a week.

Signit offers an OCSP responder that conforms to RFC 6960. The OCSP responder avails information immediately to relying party applications based on the CAs' actions on issued certificates.

The OCSP certificates contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

The actual OCSP URL to be queried by relying party organizations is referenced in the certificates issued by Signit.

4.9.10. On-Line Revocation Checking Requirements

The OCSP responder supports both HTTP GET and HTTP POST methods.

Subordinate CAs certificates:
Signit Licensed CA update information provided via their OCSP responders

- every twelve (12) months; and
- within 24 hours after revoking a Subordinate CA Certificate

For the status of Subscriber Certificates:

- OCSP responses have a validity interval greater than or equal to eight hours;
- OCSP responses have a validity interval less than or equal to ten days;
- For OCSP responses with validity intervals less than sixteen hours, then Subordinate CAs update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
- For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA updates the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

A certificate serial number within an OCSP request is one of the following two options:

1. "assigned" if a certificate with that serial number has been issued by the CA, using any current or previous key associated with that CA subject; or
2. "unused" if neither of the previous conditions are met.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused" (i.e., not issued by these CA) then the OCSP responder responds with a "revoked" status as defined by RFC 6960 (section 4.4.8. Extended Revoked Definition).

Signit operations team monitors the OCSP responder for requests for "unused" serial numbers as part of its security monitoring procedures and any such case will trigger further investigation.

4.9.11. Other Forms of Revocation Advertisements Available

Signit only use OCSP and CRL as methods for publishing certificate revocation information.

4.9.12. Special Requirements Related to Key Compromise

If Signit discovers, or has a reason to believe, that there has been a compromise of the private key of one of its CAs, it will immediately declare a disaster and invoke its business continuity plan. Signit will also:

- Determine the scope of certificates that must be revoked,
- Revoke impacted CA certificates within 24 hours,
- Generate and publish updated Certificate Revocation Lists (CRLs) without undue delay following revocation actions to support timely propagation of revocation information,
- Use reasonable efforts to notify entities, subscribers and potential relying parties that there has been a key compromise,
- generate a new CA key pair and re-establish certificate services, and
- initiate reissuance or replacement of affected end-entity certificates where necessary so that subscribers can continue using trusted certificates.

Signit maintains technical capabilities to support large-scale revocation events affecting multiple certificates resulting from key compromise, security incidents, or operational failures. Signit infrastructure and certificate management systems are designed to technically support large-scale revocation operations and the publication of revocation status information for significant numbers of certificates within a short period of time.

Relying Parties, Subscribers, or other authorized entities may report suspected private key compromise, certificate misuse, or other security concerns to Signit through the reporting channels defined in Section 1.5.2. Reports may include:

- Submission of a signed CSR, Private Key or other challenge response signed by the Private Key and verifiable by the Public Key, or
- The private key itself.

4.9.13. Circumstances for Suspension

Not Applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. Certificate Status Services

Refer to section 4.9.6 of this CP/CPS. In addition, the following provisions have been made.

4.10.1. Operational Characteristics

The CA publishes its CRLs at the public repository accessible to relying parties.

The CA's OCSP responder exposes an HTTP interface that is also publicly available to relying parties.

Revocation entries on a CRL or OCSP responses are not removed after the expiry date of the revoked certificates. The CRL includes the extension X.509 "ExpiredCertsOnCRL" as defined in ISO / IEC 9594-8 / Recommendation ITU-T X.509.

When providing the OCSP service, the OCSP response will develop the ArchiveCutOff extension, as specified in IETF RFC 6960, with the archiveCutOff date set in the CA certificate "notBefore" date value. The extension will be returned in the OCSP responses only for expired certificates.

4.10.2. Service Availability

The public repository where certificate information and CRLs are published is accessible 24 hours a day, 7 days a week, with a minimum annual availability target of 99.6%. This corresponds to approximately 1 day and 11 hours of cumulative downtime per year. The stated downtime represents the total downtime over the calendar year and should not be interpreted as the maximum duration of a single service interruption. Signit will make reasonable efforts to restore the affected service as soon as practicable following any unplanned interruption.

For informational purposes, this annual availability target is equivalent to the following indicative downtime thresholds:

- **Daily**: up to approximately 5 minutes 46 seconds
- **Weekly**: up to approximately 40 minutes 19 seconds
- **Monthly**: up to approximately 2 hours 55 minutes 19 seconds
- **Quarterly**: up to approximately 8 hours 45 minutes 57 seconds

These values are provided for illustrative purposes only and are derived from the annual availability target. They do not represent separate service availability commitments or independent service-level objectives.
Signit operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

Signit maintains a 24X7 ability to respond internally to high-priority certificate problem report as described in section 4.9.3 of this CPS. When appropriate, they forward such complaints to law enforcement authorities and/or revoke the Certificate that is the subject of the complaint.

4.10.3. Optional Features

No stipulation.

4.11. End of Subscription

Subscription period is linked to the certificate validity period. The subscription ends when the certificate is expired or revoked.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow and Recovery Policy and Practices

Key escrow is not supported by Signit.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not Applicable.

5.Facility, Management, and Operational Controls

5.1. Physical Security Controls

The PKI application and software components supporting Signit certification services are hosted within secure infrastructure environments located in the Kingdom of Saudi Arabia. Cryptographic components, including the Hardware Security Modules safeguarding CA private keys, are hosted within dedicated secure cages or racks at approved facilities in Saudi Arabia.

The approved infrastructure and facilities services providers manage the physical and environmental controls applicable to their respective facilities under their contractual responsibilities. Signit retains responsibility for the security configuration and operation of its PKI systems and maintains exclusive logical and cryptographic control of the HSMs and CA private keys.

5.1.1. Site Location and Construction

Signit operates its PKI applications, systems and supporting components with cryptographic components deployed within secure facilities located in the Kingdom of Saudi Arabia and hosted by approved infrastructure and facilities under the operational control of Signit.

PKI application services and supporting systems are hosted within enterprise-grade secure infrastructure deployed in Saudi-based regions. The infrastructure provider' data centers are designed and constructed to meet international security and resilience standards. Physical facility controls, including perimeter protection, structural safeguards, and environmental design, are managed by the infrastructure provider as part of its certified operational framework, which includes ISO/IEC 27001 and SOC 2 Type II compliance. These environments are logically isolated through network segmentation and controlled administrative access.

Cryptographic components including Hardware Security Modules (HSMs) are hosted within a Tier III data center facility located in the kingdom of Saudi Arabia. Signit operates dedicated secure cages/racks within this facility to host HSM devices and related critical infrastructure. The Tier III facility supports physical inspection, provides redundant power, cooling, audit logs and connectivity infrastructure to support high availability requirements, while physical access to Signit dedicated cage is restricted to Signit authorized personnel under controlled access procedures. These facilities further implement layered physical protection measures, including biometric access controls, intrusion detection mechanisms, manned guarding, and continuous CCTV monitoring. Access to secure areas is restricted to authorized personnel operating under trusted roles.

Signit Licensed CA operates in an offline configuration and is activated only during authorized key ceremony activities. Subordinate CAs operate within controlled environments that enforce strict separation of cryptographic material and administrative functions.

Primary and disaster-recovery facilities refer to Signit-controlled secure data center environments hosting cryptographic components. These sites are geographically separated within the Kingdom of Saudi Arabia to support operational resilience.

5.1.2. Physical Access

Within the facilities hosting Signit cryptographic components, access to Signit-dedicated secure areas is restricted to authorized Signit personnel performing Trusted Roles. These facilities implement layered physical protection measures, including biometric access controls, intrusion detection mechanisms, manned guarding, and continuous CCTV monitoring. Entry into secure zones requires authorization at multiple control points, and all physical access activities are logged and periodically reviewed.

Access to the innermost secure areas housing cryptographic modules or used for key-ceremony activities requires the presence of at least two authorized individuals performing appropriate Trusted Roles and is subject to dual-custody procedures. This requirement applies to physical access to secure infrastructure areas containing cryptographic systems, trusted time sources, or supporting security components.

Where access by authorized facilities provider personnel is operationally necessary, such access shall be approved in advance by Signit, limited to the defined purpose, logged, and continuously escorted by authorized Signit personnel. the facilities provider personnel are not granted logical or cryptographic access to HSMs, CA private keys, activation data, or key-ceremony material.

Systems hosted within Signit infrastructure are located in provider-managed facilities within the Kingdom of Saudi Arabia. Physical security controls for these facilities are managed by the infrastructure provider and remain outside Signit's direct operational control. Signit retains responsibility for logical access governance, strong authentication, administrative access restrictions, and the secure configuration of PKI systems deployed.

Equivalent physical and logical security principles shall be applied across the primary and disaster-recovery environments supporting Signit PKI services.

5.1.3. Power and Air Conditioning

Signit ensures that facilities hosting critical PKI infrastructure are designed to support continuous and stable operations.

Within the secure facilities hosting Signit cryptographic components, power supply is protected using uninterruptible power supply (UPS) systems and backup generators to maintain availability of cryptographic and supporting infrastructure during power disruptions. Environmental conditions within secure areas are maintained through controlled air-conditioning systems to ensure that equipment operates within manufacturer-recommended temperature and humidity ranges.

These facility controls are managed by the approved infrastructure and facilities providers under their contractual responsibilities where Signit specifies the applicable environmental protection requirements . Signit periodically reviews the provider's environmental controls and supporting certifications.

5.1.4. Water Exposures

Signit ensures reasonable precautions are implemented within its secure facilities to reduce the risk of damage caused by water exposure to its infrastructure and supporting equipment.

Critical systems are installed in controlled environments designed to minimize risks associated with leaks, flooding, or other environmental hazards.

Environmental protection measures — including safeguards against water exposure — are managed by the approved infrastructure and facilities services providers as part of the underlying facility operations.

5.1.5. Fire Prevention and Protection

Signit enforces fire prevention and protection measures within its secure facilities to safeguard the infrastructure and supporting systems from damage caused by fire or smoke. These measures are designed in accordance with applicable safety regulations in KSA and include monitoring and response mechanisms appropriate to the hosting environment.
Fire detection and protection controls are managed by the approved infrastructure and facilities services providers as part of the facility's physical security and environmental safeguards.

5.1.6. Media Storage

Signit manages the storage of removable media, appliances, and software in accordance with established internal procedures. Media containing sensitive or confidential information are stored within secure on-premises facilities under controlled access conditions.

Sensitive data media are protected using appropriate physical safeguards, including locked storage and fire-resistant containers, as applicable.

Critical copies required for operational continuity are securely replicated and stored at a designated disaster recovery location.

For PKI systems hosted within Signit infrastructure located in the Kingdom of Saudi Arabia, storage services are provided as part of the underlying platform. The physical protection and lifecycle management of storage hardware are handled by the infrastructure provider, while Signit maintains responsibility for logical access control, configuration, and protection of PKI data stored within this environment.

5.1.7. Waste Disposal

Signit ensures that media containing sensitive information are securely disposed of when no longer required. Within Signit-controlled secure facilities, paper records and physical storage media are destroyed prior to disposal using approved methods such as cross-cut shredding, secure wiping, or physical destruction, depending on the media type and level of sensitivity.

Cryptographic devices and related key-management components, including Hardware Security Modules (HSMs) where applicable, are decommissioned using controlled procedures to ensure that all sensitive information and cryptographic material are securely removed or permanently rendered unusable prior to disposal, transfer, or repurposing, in accordance with applicable laws and regulatory requirements in the Kingdom of Saudi Arabia.

For systems hosted within the service provider infrastructure, disposal and lifecycle management of physical storage hardware are handled by the infrastructure provider as part of their facility operations. Signit maintains responsibility for ensuring that logical access to PKI data is revoked and that sensitive information is securely removed from Signit-managed systems before decommissioning activities.

5.1.8. Off-Site Backup

Signit performs regular backups of critical PKI system data, configuration information, and audit logs to support operational continuity and disaster recovery.

Within Signit-controlled environments, backup copies containing sensitive information are stored in secure locations with equivalent protection measures to those applied at the primary facility. Backup processes are designed to preserve the confidentiality, integrity, and availability of PKI information.

Primary and disaster-recovery facilities hosting Signit infrastructure are geographically separated within the Kingdom of Saudi Arabia to support service resilience. Where applicable, backup data may be replicated between these locations using secure communication channels.

For PKI systems hosted within the service provider infrastructure located in the Kingdom of Saudi Arabia, backup capabilities are supported by the underlying platform. Physical protection of backup storage media is managed by the infrastructure provider, while Signit maintains responsibility for defining backup policies, access controls, and logical protection of backed-up data.

5.2. Procedural Controls

Signit operations team follows rigorous control procedures to enforce the segregation of duties, based on job responsibility, so that sensitive operations are not performed by a single member of trusted personnel. The roles requiring separation of duties, and the controls applied where full separation cannot be achieved, are set out in Section 5.2.4.

Access to systems supporting the service is restricted in accordance with the access control policy. Signit administers user access of the systems, including user account management and timely removal of access.

5.2.1. Trusted Roles

A Trusted Role is performed by an individual employee or contractor of Signit, or of an authorized Delegated Third Party, whose responsibilities directly affect the security of Signit certification services, including certificate management, system administration and operation, security oversight, audit-log and archive management, and cryptographic key lifecycle management.

Certain PKI operational Trusted Roles may be performed by personnel of an authorized Delegated Third Party engaged by Signit under a written agreement. Such personnel are subject to the same appointment, background check, authorization and oversight requirements as Signit personnel, as set out in Sections 5.3.1, 5.3.2 and 5.3.7. Signit retains full responsibility for all activities performed by a Delegated Third Party under this CP/CPS and maintains a record of the roles so delegated.

Before assuming a Trusted Role, personnel shall undergo appropriate background and security checks in accordance with Signit personnel security policies and applicable legal requirements. Access shall be formally authorized, limited to the privileges necessary for the assigned duties, and periodically (yearly) reviewed.

The following roles are classified as Trusted Roles within Signit:

- **PKI Director:** Owner of PKI strategy and responsible for overall direction and decision making.
- **PKI Policy Authority:** Responsible for the design and policies of the PKI.
- **Compliance and Security:** Responsible for oversight of compliance and executing security management.
- **PKI Operations Manager:** Responsible for PKI operations team.
- **PKI Administrators:** Responsible for CA software configuration and maintenance.
- **IT Operations Manager:** Responsible for IT operations team.
- **System Administrator:** Responsible for system and infrastructure configuration and maintenance.
- **Network Administrator:** Responsible for network devices configuration and maintenance.
- **Security Administrator:** Responsible for executing security monitoring and configuration.
- **Registration Authority Officer:** Responsible for vetting and approving subscriber certificate requests.
- **PKI Custodians:** Responsible for maintaining and securing the CA HSM activation material, rack access and safe access.

5.2.2. Number of Persons Required per Task

The most sensitive tasks such as the following require the presence of two or more persons:

- Physical access to secure areas hosting Signit PKI infrastructure,
- Access to and management of Hardware Security Modules (HSMs) and associated cryptographic components

All operational activities performed by the personnel having trusted roles are logged and maintained in a verifiable and secure audit trail.

5.2.3. Identification and Authentication for each Role

Before exercising the responsibilities of a trusted role:

- Signit GB confirms the identity and history of the employee by carrying out background and security checks
- Authorized personnel are issued physical access credentials where required to enter secure facilities
- Logical system access is provisioned according to role-based access controls and strong authentication requirements.

5.2.4. Roles Requiring Separation of Duties

Signit assigns responsibilities to ensure that critical PKI functions remain segregated. Roles requiring separation of duties include:

- Those performing approval of the issuance of Certificates. (RA officers)
- Those performing installation, configuration, and maintenance of the CAs systems. (System and Network Administrators)
- Those with overall responsibility for administering the CAs' services. (PKI Administrators)

- Those performing duties related to cryptographic key life cycle management. (key custodians)
- Those with overall responsibility for administering the implementation of the CAs' security practices and for performing CA systems auditing. (Compliance and Security officers)

Signit assigns Trusted Roles and responsibilities to maintain appropriate segregation of duties for security-sensitive PKI functions. Where personnel perform more than one operational responsibility, Signit ensures that incompatible functions are appropriately segregated through technical or procedural controls, including multi-person authorization, independent review, access restrictions and audit logging.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

Prior to engagement of an PKI staff member, whether as an employee, agent, or an independent contractor, Signit ensures that checks are performed to establish the background, qualifications and experience needed to perform within the competence context of the specific job. Such checks include:

1. Verify the Identity of Such Person: Verification of identity MUST be performed through:
   A. Personal (physical) presence of such person before trusted persons who perform human resource or security functions, and
   B. Verification of well-recognized forms of government-issued photo identification; and
2. Verify the Trustworthiness of Such Person: Verification of trustworthiness includes background checks, which address at least the following, or their equivalent:
   A. Criminal convictions for serious crimes,
   B. Misrepresentations by the candidate,
   C. Appropriateness of references, and
   D. Any clearances as deemed appropriate

5.3.2. Background Check Procedures

All employees filling trusted roles are selected based on integrity, background investigation and security clearance. Signit ensures that these checks are performed once yearly for all personnel holding trusted roles.

5.3.3. Training Requirements

Signit ensures that its employees receive adequate training and possess the necessary experience to perform the duties outlined in their employment contracts and job descriptions before undertaking any operational or security functions. This training is regularly updated and conducted annually for CA personnel.

The training program covers a wide range of topics and is delivered by a combination of experienced CA staff and third-party experts specializing in security and PKI. The key topics include:

- Security policies within Signit
- Hands-on training with relevant products

- Disaster recovery and business continuity procedures
- Operational processes
- RA processes
- Specific duties expected of employees

Signit maintains records of all personnel who complete the required training and regularly evaluates the effectiveness of the training provided. Personnel performing trusted roles, including RA Officers, shall complete the applicable training and demonstrate the competence required for their assigned responsibilities before being authorized to perform their duties. The method used to assess competence shall be appropriate to the relevant role and may include written examinations, practical assessments or supervisory evaluation.

Training records, including attendance records, assessment results and certificates, where applicable, shall be retained for at least five (5) years in accordance with Signit's record-retention policy and applicable legal requirements.

5.3.4. Retraining Frequency and Requirements

The training curriculum is delivered to all Signit staff. The training content is reviewed and amended on a yearly basis to reflect the latest leading practices and the CA systems' configuration changes.

5.3.5. Job Rotation Frequency and Sequence

Signit GB ensures that any change in Signit staff will not affect the operational effectiveness, continuity, and integrity of the offered certification services.

5.3.6. Sanctions for Unauthorized Actions

To maintain accountability on Signit staff, Signit GB sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems, according to the relevant human resources policy and procedures, and the applicable law in the Kingdom of Saudi Arabia.

5.3.7. Independent Contractor Requirements

Independent contractors and their personnel are subject to the same background checks as Signit staff. The background checks include:

A. Criminal convictions for serious crimes,
B. Misrepresentations by the candidate,
C. Appropriateness of references,
D. Any clearances as deemed appropriate,
E. Privacy protection, and
F. Confidentiality conditions.

5.3.8. Documentation Supplied to Personnel

Signit GB documents all training materials and makes them accessible to CA staff.

Additionally, Signit GB ensures that key operational documentation is available to relevant staff members. At a minimum, this includes the CP/CPS document, security policies, operational guides, and technical documentation relevant to each trusted role.

5.4. Audit Logging Procedures

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. This covers activities such as key life cycle management, including key generation, backup, storage, recovery, destruction and the management of cryptographic devices, the CA and OCSP responder.

Security audit log files for all events relating to the security of the CA, RA and OCSP responders shall be generated and preserved.

These logs shall be reviewed by the security officer team and are also subject to review as part of the regular internal audits performed by the compliance function of Signit on the CAs operations.

5.4.1. Types of Events Recorded

Audit logs are generated for all events relating to the security and services of the CAs systems. At a minimum, each audit record includes the following:

- The date and time the event occurred.
- A success or failure indicator of the event (e.g. CA signing event, revocation event, certificate validation event)
- The identity of the entity and/or operator that caused the event.
- Description of the event.

Where possible, the audit logs are automatically generated and where not possible, a logbook or paper forms are used. The audit logs, both electronic and non-electronic, are retained by the PKI operations team and may be made available during compliance audits.

Following events occurring in relation to the CAs operations are recorded:

1. CAs certificates and key life cycle events, including:
    1. Key generation, backup, storage, recovery, archival and destruction;
    2. Cryptographic device life-cycle management events.
    3. Certificate requests, renewal, and re-key requests, and revocation;
    4. Approval and rejection of Certificate requests;
    5. Generation of CRLs;
    6. Signing of OCSP responses; and
    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate life-cycle management events, including:
    1. Certificate requests, renewal, and re-key requests, and revocation;
    2. Identity-verification and authentication activities, including the receipt and validation of NAFATH authentication responses or signed assertions received from Reliable KYC Providers;
    3. The identity of the Reliable KYC Provider that submitted the certificate request, where applicable;
    4. The Applicant's consent and acceptance of the applicable Subscriber Agreement;

5. Approval and rejection of certificate requests;
6. Issuance of certificates.

3. Security events, including:
    1. Successful and unsuccessful PKI system access attempts;
    2. PKI and security system actions performed;
    3. Relevant router and firewall activities (as described in Section 5.4.1.1); and
    4. Security profile changes;
    5. System platform issues (e.g. crashes), hardware failures, and other anomalies
    6. Entries to and exits from the CA facility.
    7. Installation, update and removal of software on a Certificate System;

For Signit Timestamping CA, the following is recorded:

- Time-stamp requests and created timestamps.
- Events related to TSA administration (including certificate management, key management, and clock synchronization)
- Events relating to the life cycle of TSA keys and certificates.

Signit GB also ensures that the following information, not produced by these CA, is maintained (either electronically or manually) by the operations team:

1. CA personnel, security profiles rotations/changes.
2. All versions of this CP/CPS.
3. Minutes of meetings.
4. Compliance internal audit reports.
5. Current and previous versions of Subordinate CAs configuration and operations manuals.

5.4.1.1. Router and firewall activities logs

Router and firewall activities logged include:

1. Successful and unsuccessful login attempts to routers and firewalls; and
2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and
3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and
4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2. Frequency of Processing Log

Signit GB ensures that designated personnel conduct regular reviews of log files to verify their integrity and promptly identify any anomalous events. The following audit log review cycle is established by Signit:

- Security Officers review the audit and security logs of online CA systems monthly to ensure the integrity of logging processes and confirm that daily monitoring is functioning correctly

- Quarterly reviews of physical access logs and user management on PKI systems are carried out by the Security Officer team to ensure compliance with physical and logical access policies

- Annually, the compliance function performs an internal audit of CA operations. During this audit, the compliance officer requests samples of log review reports and collected audit logs from the previous audit cycle.

- All evidence from audit log reviews, including the outcomes and any remediation actions taken, is collected and archived for future reference.

5.4.3. Retention Period for Audit Log

Signit retains system-generated audit records, including electronic and manual logs, for a minimum period of two (2) years in an accessible form to support operational monitoring, security investigations, and compliance activities. After this period, audit logs are securely archived and retained for the total archive retention period specified in Section 5.5.2. Retention applies to CA certificate and key lifecycle events, Subscriber certificate lifecycle events, and security-related activities, and archived records are preserved in a manner that maintains their integrity, confidentiality, and availability for audit and legal purposes.

5.4.4. Protection Of Audit Log

Audit logs are protected by a combination of physical, procedural, and technical security controls as follows:

- Signit' systems generate cryptographically protected audit logs,
- The security of audits logs is maintained while these logs transit by the backup system and when these logs are archived,
- The access control policies enforced on Signit systems ensure that read access only is granted to personnel having access to audit logs as part of their operational duties,
- Only authorized roles can obtain access to systems where audit logs are stored and any attempts to tamper with audit logs can be tracked to the respective Signit staff.

5.4.5. Audit Log Backup Procedures

Audit logs are backed up through automated and controlled backup procedures designed to ensure their integrity, availability, and recoverability.
Backup copies of PKI system audit logs are retained within secure environments under Signit administrative control. Backup data is protected against unauthorized access, modification, or deletion through logical access controls and monitoring mechanisms.
A secondary copy of audit log backups is maintained at the disaster recovery location to support business continuity and disaster recovery objectives. Where infrastructure services support automated replication or archival storage, backup data may be securely replicated to the disaster recovery region to ensure resilience and long-term preservation of audit records.

5.4.6. Audit Collection System (Internal vs. External)

Audit collection processes are primarily managed through systems operated under Signit administrative control. Automated audit logging functions are activated at system startup and remain active throughout system operation until shutdown, ensuring continuous recording of relevant security and operational events.

Where PKI components operate within service provider infrastructure, audit records are generated and retained through logically controlled logging mechanisms configured and supervised by Signit. The underlying infrastructure may provide supporting logging capabilities;

however, Signit remains responsible for defining audit requirements, monitoring log integrity, and ensuring compliance with this CP/CPS.

If any automated audit mechanism fails or if the integrity, availability, or confidentiality of audit data is suspected to be compromised, Signit GB will assess the impact and may suspend affected CA operations until the issue is investigated and resolved.

5.4.7. Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8. Vulnerability Assessments

Signit performs regular vulnerability assessments and risk evaluations to ensure the ongoing security of its Certification Authority (CA) services, supporting PKI systems, and operational infrastructure.

An annual Risk Assessment is conducted to identify internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of Certificate Data or Certificate Management Processes. This assessment evaluates the likelihood and potential impact of identified risks and reviews the effectiveness of existing security controls, policies, and operational procedures.

Technical vulnerability scanning is performed on a regular basis and after significant infrastructure or configuration changes. At minimum:

- Vulnerability scans are conducted at least every three (3) months on public and private IP addresses associated with CA systems and supporting PKI infrastructure.
- Additional assessments are carried out following major system upgrades, architectural changes, or security-relevant events.

These activities cover all environments under Signit operational control, including PKI systems running in Signit environment, on-premises infrastructure and trusted time sources, and the secure communication channels between them.

Signit is responsible for vulnerability management of the operating systems, applications, PKI components, and configurations it manages, while the underlying physical infrastructure is secured by the approved infrastructure and facilities services providers under their certified security framework.

In addition to internal assessments, independent third-party vulnerability assessments and penetration tests are performed at least annually or following significant changes to the PKI environment. The results of these assessments are reviewed by Signit governance and security management, and remediation actions are tracked through the risk management process.

Evidence of vulnerability assessments, penetration testing activities, and remediation efforts is maintained for audit and compliance purposes.

5.5. Records Archival

5.5.1. Types of Records Archived

Signit maintains archived records that are sufficient to demonstrate the proper operation of its Certification Authority (CA) services and to support verification of the validity of any certificate issued under this CP/CPS, including expired or revoked certificates. Archived information is preserved in a secure manner and made available to authorized auditors and regulatory authorities upon justified request.

The records retained for archival purposes include, but are not limited to, the following:

- Audit logs and security monitoring data as described in Section 5.4;
- Information relating to certificate lifecycle activities, including certificate application data, evidence of NAFATH authentication, signed assertions received from Reliable KYC Providers, evidence of the authority of the Authorized Representative and the Requester, evidence of the Applicant's consent and acceptance of the applicable Subscriber Agreement, Signit's validation results, issuance records and revocation actions;
- Applicable policies, procedures, subscriber agreements, agreements with Reliable KYC Providers, and compliance or audit documentation relevant to CA operations;
- Cryptographic device lifecycle records, key management events, and key ceremony documentation where applicable;
- Records of Signit approval of cryptographic modules used under the applicant-generated key-pair model, including the evidence provided by the applicant and the approval decision, as described in Section 4.1.2;
- System administration, configuration management, and change control records associated with PKI services and supporting infrastructure.

5.5.2. Retention Period for Archive

Signit retains archived records, including audit logs, security documentation, and certificate lifecycle information, for a minimum period of ten (10) years to support compliance, audit, and security investigation requirements. Records related to certificate verification, issuance, and revocation remain archived for the full retention period regardless of certificate expiration or revocation status. Archived information is securely protected and accessible only to authorized personnel and qualified auditors when required.

5.5.3. Protection of Archive

Records are archived in such a way that they cannot be deleted or destroyed. Controls are in place to ensure that only authorized personnel can manage the archive without modifying integrity, authenticity, and confidentiality of the contained records.

5.5.4. Archive Backup Procedures

Signit maintains one controlled version of each digital archive at the primary site, with a replicated copy stored at the disaster recovery location to ensure availability and resilience. Archived data is not duplicated beyond this controlled replication model. Documented operational procedures define how archive records are created, securely transferred, stored, and restored when required, ensuring the integrity and traceability of archived information throughout its lifecycle.

5.5.5. Requirements for Timestamping of Records

All recorded and archived events include accurate date and time information. Signit CA systems synchronize their system clocks with trusted time sources to ensure consistency and integrity of audit records.

Systems deployed within the Signit PKI infrastructure, including virtual machines, databases, firewalls, load balancers, and supporting services, synchronize with the infrastructure provider's Network Time Protocol (NTP) service, which is aligned with authoritative UTC time sources.

Cryptographic components and related infrastructure hosted within the on-premises secure environment use internally configured time synchronization services aligned with trusted UTC sources.

Time synchronization mechanisms are monitored to ensure reliable timestamp accuracy across Signit PKI environments.

Time synchronization is maintained with an accuracy of ±1 second or better relative to UTC. Operational procedures are implemented to regularly monitor time synchronization status and detect and correct any clock drift to ensure the reliability and consistency of audit records.

5.5.6. Archive Collection System (Internal or External)

Only authorized and authenticated personnel are permitted to access archived material. Signit operates a controlled archive collection system supported by documented backup, restore, and archival procedures that define how archive data is created, securely transmitted, stored, and retrieved. Access to archived records is restricted to trusted roles, and archive handling activities are performed in accordance with defined operational procedures to preserve the integrity, confidentiality, and availability of the archived information.

5.5.7. Procedures to Obtain and Verify Archive Information

Only authorized and authenticated personnel are permitted to access archived material. Signit operations follow documented backup, restore, and archive procedures that define how archived information is created, securely transmitted, stored, and retrieved. These procedures also describe the operation of the archive collection system and ensure that archived records remain protected and verifiable throughout their lifecycle.

5.6. Key Changeover

Signit Certification Authorities perform periodic key changeover to maintain the long-term security and integrity of the PKI. During a key changeover, a new key pair is generated and used for future certificate signing operations. Previously used CA private keys remain protected with the same level of security as active keys and are retained only for signing Certificate Revocation Lists (CRLs) for certificates issued under the former key until all such certificates have expired or been revoked. After this period, the old keys are securely retired in accordance with established key lifecycle management procedures.

Refer to Section 6.3.2 of this CP/CPS document for key changeover frequency.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

If Signit detects a suspected security incident, attempted intrusion, or any form of compromise affecting its Certification Authority systems or supporting infrastructure, an investigation is immediately initiated to determine the nature, scope, and potential impact of the event. Where compromise of a CA private key is suspected, Signit activates its Incident Management and Response Procedures without delay. Depending on the outcome of the investigation, actions may include rebuilding affected systems, revoking impacted certificates, or formally declaring the CA key compromised.

Signit activates its incident response procedures and notifies the NIC without undue delay in situations including, but not limited to:

- Suspected or confirmed compromise of CA systems or cryptographic components;
- Physical or electronic attempts to access or penetrate secure PKI environments;
- Denial-of-Service (DoS) attacks or abnormal traffic affecting CA availability;
- Any event that prevents the CA from issuing a CRL within the timeframe defined by the nextUpdate field of the currently valid CRL.

All incident handling activities are conducted in accordance with documented operational and security procedures to ensure timely containment, recovery, and communication with relevant stakeholders.

5.7.2. Recovery Procedures if Computing Resources, Software, and/or Data are Corrupted

Signit maintains backup copies of critical systems, software, databases, configuration information, and cryptographic materials required to restore Certification Authority operations in the event of corruption or failure. When computing resources, applications, or data are suspected to be compromised or corrupted, recovery activities are performed in accordance with Signit documented Business Continuity and Disaster Recovery Plan. These procedures define the steps required to restore system integrity, re-establish trusted operations, and ensure continuity of certification services within defined recovery objectives.

5.7.3. Recovery procedures after key compromise

Compromise or suspected compromise of a Signit Certification Authority private keys, or of its associated activation data, is treated as a critical security incident and immediately triggers the response procedures defined in Signit Incident Management, Business Continuity, and Disaster Recovery Plans.

Upon identification of such an event, Signit convenes its designated governance board (i.e., Signit GB) to assess the impact, take required operational decisions, and coordinate internal and external communications. Response actions may include suspension of affected services, revocation of impacted certificates, generation of new key material, and controlled restoration of trusted operations in accordance with established key compromise and CA termination procedures.

5.7.4. Business Continuity Capabilities after a Disaster

In case of a disaster affecting servers, software, or data, the disaster recovery and business continuity plan is activated to restore the minimum required CA operational capabilities in a timely manner. The plan covers Signit PKI components and cryptographic components hosted within the secure facilities.

In particular, the plan targets the recovery of the following services, either in the primary location, or the disaster recovery location:

- Certification services (issuance and revocation)
- Public repository where CRLs and CAs certificates are published
- OCSP services

Failover scenarios to the disaster recovery location are made possible considering the CA backup system that enables the continuous replication of critical CAs data from the primary site to the disaster recovery site. That allows a recovery of the CAs critical services at the disaster recovery location within the allowed Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

The business continuity plan defines the following:

- The conditions for activating the plan,
- Emergency procedures,
- Fallback procedures,
- Resumption procedures,
- A maintenance schedule for the plan;
- Awareness and education requirements;
- The responsibilities of the individuals;
- Recovery point objective (RPO) & Recovery time objective (RTO);
- Regular testing of contingency plans.
- The CAs' plan to maintain or restore the CAs' 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;
- What constitutes an acceptable system outage and recovery time
- How frequently backup copies of essential business information and software are taken;
- The distance of recovery facilities to the main site; 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.

5.8. CA or RA Termination

If Signit determines that termination of its CA services is deemed necessary, Signit GB executes its termination plan that has been approved. The termination plan must at minimum:

- Ensure that any disruption caused by the termination of the CA is minimized as much as possible
- Ensure proper arrangements for the retention of archived logs, as specified in Section 5.5
- Ensure proper arrangements for maintaining the validation status service URLs specified in certificates that remain valid for the applicable period after termination,

- Ensure prompt notification of termination is provided to Subscribers, Authorized Relying Parties, Application Software Providers and other relevant stakeholders (e.g. NIC). This notification should be published in the public repository and communicated through other mediums and methods as determined by the DGA.
- Where applicable, ensure communication with relevant parties and facilitate the transfer of archived CAs' records to an appropriate custodian.
- Ensure the development and execution of a plan to assist, as much as possible, Subordinate CAs' subscribers in transitioning to another TSP,
- ensure that a process for revoking all Digital Certificates issued by the Subordinate CAs at the time of termination is maintained.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1.1. Signit key generation

Signit key generation ceremony is planned and is subject to the formal authorization of Signit GB director.

During the ceremony, Signit ensures that the CA private keys are generated using Common Criteria-certified HSMs (trustworthy systems) and a dedicated machine to be set up by authorized Signit personnel only. The detailed key ceremony activities are documented in a key ceremony procedure and related ceremony log which are not publicly accessible documents.

The CAs Key Generation Ceremonies are witnessed by an external WebTrust auditor with the aim to produce a report opinion that Signit:

- Conducts the KGC with formal authorization from Signit GB
- Ensures the KGC takes place in the presence of authorized personnel with trusted roles,
- Has the KGC witnessed by a Qualified Auditor (see Section 8: Compliance Audit and Other Assessments)
- Properly distributes secrets, activation data, and key shares to trusted operatives and key custodians
- Records and securely stores a video of the entire key generation ceremony for audit purposes

6.1.1.2. Subscriber's Key Pair Generation

The subscriber keys are generated according to the below requirements:

Certificate type	Key generation requirements
Certificates issued to legal persons (eSeal certificates)	Under the Signit-managed key-generation model, the key pair is generated within Common Criteria certified hardware cryptographic devices operated by Signit. Under the applicant-generated key-pair model, the key pair shall be generated within a cryptographic module provided by the applicant, certified to at least FIPS 140-2 Level 3 or to an equivalent Common Criteria certification, and approved by Signit in accordance with Section 4.1.2. Key generation algorithms and key sizes shall be used as specified under Sections 6.1.5 and 6.1.6 of this CP/CPS.
Certificates issued to natural persons	Subscribers' key pairs are generated within the memory of Common Criteria-certified hardware cryptographic devices operated by Signit for its remote electronic signature service. Key pairs shall be generated using key generation algorithm and key sizes as specified under sections 6.1.5 and 6.1.6 of this CP/CPS.
TSU certificates / Signature Validation certificates	The key pair generation occurs within the memory of Common Criteria certified hardware cryptographic devices operated by Signit. Key generation algorithm and key sizes will be used as specified under sections 6.1.5 and 6.1.6 of this CP/CPS.

Signit rejects a certificate request if the requested public key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key.

6.1.2. Private Key Delivery to Subscriber

Not Applicable.

6.1.3. Public Key Delivery to Certificate Issuer

Signit accepts CSRs in a format compliant with PKCS#10 protocols, provided they originate from authenticated users.

6.1.4. CA Public Key Delivery to Relying Parties

Signit CAs public key certificates are published on the public repository.

6.1.5. Key Sizes

Signit Licensed CA key size is 4096-bit RSA.

Subordinate CAs, OCSP Responders, Time-Stamping Units (TSUs), and Signature Validation Service certificates use ECC NIST P-384 (secp384r1) keys.

Subscriber certificates use at least ECC NIST P-256 (secp256r1) keys.

6.1.6. Public Key Parameters Generation and Quality Checking

Signit Licensed CA and Subordinate CAs generate their private and public key pairs using state-of-the-art cryptographic parameter generation methods to ensure strong key integrity and security.

The HSMs and associated cryptographic software used for key generation by the Intermediate and Subordinate CAs comply with the requirements of FIPS 186 for random number generation and primality testing

6.1.7. Key Usage Purposes (as per X.509 v3 key usage field)

Certificates issued by Signit contain a key usage bit string in accordance with [RFC 5280]. Refer to section 7 of this CP/CPS.

6.1.7.1. Signit Licensed CA

Private Keys corresponding to Signit Licensed CA Certificates shall not be used to sign Certificates except in the following cases:

- Certificates for Subordinate CAs,
- CARL and certificates for the OCSP responder.

6.1.7.2. Subordinate CAs

Private Keys corresponding to Signit Subordinate CAs Certificates shall not be used to sign Certificates except in the following cases:

- Signing subscriber certificates and CRLs.
- Signing OCSP responder certificates.

- Issuing Time Stamping Unit (TSU) certificates, where applicable, by the designated Signit Timestamping CA.

6.1.7.3. Subscriber Certificates

The key usage extension is set in accordance with the certificate profile requirements specified in Section 7.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

Signit CA private keys and subscriber private keys generated under the Signit-managed key-generation model are generated, stored and protected within Common Criteria certified Hardware Security Modules. These cryptographic modules are deployed within secure facilities under Signit control, located in the most restricted physical security zone as described in Section 5.1, and remain under the exclusive logical and cryptographic control of Signit. The private key remains protected within the cryptographic module and cannot be exported in plaintext.

Under the applicant-generated key-pair model, the eSeal key pair is generated and stored within a cryptographic module provided by the applicant that is certified to at least FIPS 140-2 Level 3, or to an equivalent Common Criteria certification, and that has been approved by Signit in accordance with Section 4.1.2. Signit does not restrict where such a module is hosted. It may be deployed at the applicant's own premises or in a hosting environment selected by the applicant, provided that the module meets the certification requirement and has been approved by Signit. The private key remains protected within the module and cannot be exported in plaintext. Signit approves the cryptographic module but does not operate it.

6.2.2. Private Key (m out of n) Multi-person Control

The CA's private keys are continuously controlled by multiple authorized personnel. Trusted roles related to CA private key management (and associated secrets) are documented in Signit KGC procedures and other internal documentation.

Signit staff are assigned to trusted roles by Signit GB, ensuring segregation of duties and enforcing the principles of multi-person control and split knowledge. Multi-person control of the CA private keys is implemented using an "m-of-n" split key knowledge scheme, where at least two (2) out of three (3) key custodians must be concurrently present, along with HSM administrators, to activate or re-activate the CA private key.

Signit GB keeps written, auditable, records of tokens and related password distribution to trusted operatives and key custodians. In case trusted operatives or key custodians are to be replaced, it will keep track of the renewed tokens and/or password distribution.

6.2.3. Private Key Escrow

Not applicable.

6.2.4. Private Key Backup

Signit CA private keys are generated, stored, and remain protected within Common Criteria-certified HSMs, using dedicated, cryptographically isolated partitions. Backup and recovery capability is achieved through secure HSM-to-HSM key replication to a geographically separate disaster recovery (DR) site. At no time are CA private keys exported or handled outside HSM protection.

The replicated private keys are maintained under security controls equivalent to those applied to the primary keys, including multi-person control, split knowledge, and strict role-based access restrictions. Activation or recovery of CA private keys at the DR site is subject to the same authorization requirements and trusted role separation as production operations and is performed only in accordance with documented disaster recovery procedures.

All key backup, replication, and recovery activities are logged, monitored, and subject to periodic review. Disaster recovery procedures are tested in accordance with Signit business continuity and disaster recovery policies.

6.2.5. Private Key Archival

Not Applicable.

6.2.6. Private Key Transfer into or from a Cryptographic Module

Signit CA private keys may be transferred between approved cryptographic modules only where required for authorized backup, replication, disaster recovery or migration to another approved cryptographic module.

Such transfer shall be performed through a secure, authenticated and cryptographically protected HSM-to-HSM mechanism, under multi-person control and in accordance with Signit Key Management Policy.

The destination cryptographic module shall provide a security level equivalent to or higher than that of the source module, meet the requirements specified in Section 6.2.11 and be formally approved for use within Signit PKI.

CA private keys shall not be exported or otherwise exposed in plaintext outside the protected cryptographic-module environment. Where required for backup, disaster recovery or migration, a cryptographically protected HSM backup file containing encrypted CA private-key material may be copied to an authorized laptop or approved storage media. The private-key material shall remain encrypted under HSM protection and shall be capable of restoration only into an approved destination HSM. The authorized laptop or storage media containing the encrypted backup file shall be securely stored in a designated safe and handled under multi-person control.

CA private keys shall not be stored or processed within the PKI application environment hosted by the infrastructure provider.

Each transfer shall be formally authorized and performed as part of an approved key-transfer, backup or migration ceremony by appropriately assigned Trusted Roles under dual control. The transfer mechanism shall preserve the confidentiality, integrity and authenticity of the private key

throughout the operation. Detailed transfer and migration activities shall be performed in accordance with Signit Key Management Policy and the applicable ceremony documentation.

6.2.7. Private key Storage on Cryptographic Module

No further stipulation other than those stated in clauses 6.2.1, 6.2.2, 6.2.4 and 6.2.6.

6.2.8. Method of Activating Private Key

6.2.8.1. Signit Licensed CA and Subordinate CAs

The private keys are activated inside the HSM as part of audited key ceremonies attended by several trusted personnel and relevant Signit personnel. The principles of dual control and split knowledge are enforced so that each trusted personnel involved in the ceremony holds his own set of secrets/activation data/key share. The activation procedure shall use a PIN entry device attached to the HSMs.

Signit Licensed CA private key remains active only for the duration of the activity requiring Signit Licensed CA activation (e.g. certification, CRL generation), after which it is kept offline.

The activation procedure is documented in the key ceremony documentation.

6.2.8.2. Subscribers

For Natural Person certificates, the subscriber's remote-signing private key is activated using a secure protocol compliant with EN 419 241-2, Level of Assurance 2. The protocol requires the subscriber's involvement in activating the private key for the authorized signing operation.

For eSeal certificates issued under the Signit-managed key-generation model, the private key is held within a Signit operated Hardware Security Module and is activated only upon an authenticated and authorized request from the Subscriber, using the authentication mechanisms established during registration. Subscribers are responsible for protecting the credentials and activation data used for this purpose.

For eSeal certificates issued under the applicant-generated key-pair model, the private key is held within the applicant's own cryptographic module. The Subscriber is responsible for activating and protecting access to the private key in accordance with the obligations set out in this CP/CPS and the applicable Subscriber Agreement.

6.2.9. Method of Deactivating Private Key

6.2.9.1. Signit Licensed CA and Subordinate CAs

Signit Licensed CA private key is deactivated at the end of the ceremony which prevents any further use of the private keys. This activity applies to the principles of dual control and split knowledge and is always witnessed by the relevant personnel (e.g., auditor). At the end of the ceremony, all material used during the ceremony is put back in the respective safes.

For Subordinate CAs, the private keys are deactivated only when the CA system is properly shut down, in accordance with the manufacturer's Hardware Security Module (HSM) operational documentation.

This procedure likewise adheres to the principles of dual control and split knowledge and is witnessed by the relevant personnel. After completion, all materials used during the ceremony are securely stored in their designated safes.

6.2.9.2. Subscribers

For eSeal certificates issued under the Signit-managed key-generation model, the private key is deactivated at the end of each authorized signing operation and remains inaccessible until the Subscriber is again authenticated and authorized.

For eSeal certificates issued under the applicant-generated key-pair model, the Subscriber is responsible for deactivating and protecting access to the private key in accordance with the obligations set out in this CP/CPS and the applicable Subscriber Agreement.

For Short-term certificates, the subscriber's private key is generated for a single signing session and is securely deleted immediately after the session ends, irrespective of whether a valid signature was produced. This ensures that the key does not persist beyond the intended session scope, in compliance with the recommended security practices.

6.2.10. Method of Destroying Private Key

6.2.10.1. Signit Licensed CA and Subordinate CAs

At the end of their lifetime, Signit private keys are irrevocably destroyed in the presence of authorized personnel acting as trusted roles.

The CA keys are destroyed by permanently removing them from any hardware module the keys are stored on. Any backup copies of the CA private keys, including backups stored on backup media, will also be securely and permanently destroyed as part of the key destruction process.

The CA private keys destruction outside the context of the end of its lifetime applies to investigation and special authorization from Signit GB. The key destruction process is detailed in the dedicated key ceremony documentation. The destruction procedure shall enforce the principle of multi-person control and split knowledge. Any associated records are archived, including a report evidencing the key destruction process.

6.2.10.2. Subscribers

For eSeal certificates issued under the Signit-managed key-generation model, the private key is destroyed within the Signit Hardware Security Module upon expiry or revocation of the certificate, or upon a documented request from the Subscriber, in accordance with Signit internal procedures.

For eSeal certificates issued under the applicant-generated key-pair model, the Subscriber is responsible for destroying the private key upon expiry or revocation of the certificate, in accordance with the obligations set out in this CP/CPS and the applicable Subscriber Agreement.

For Short-term certificates, the subscriber's private key is generated for a single signing session and is securely deleted immediately after the session ends, irrespective of whether a valid signature was produced. This ensures that the key does not persist beyond the intended session scope, in compliance with the recommended security practices.

6.2.11. Cryptographic Module Rating

Hardware Security Modules used to protect Signit CA private keys and subscriber private keys under the Signit-managed key-generation model shall be Common Criteria certified. Cryptographic modules used under the applicant-generated key-pair model shall be certified to at least FIPS 140-2 Level 3, or to an equivalent Common Criteria certification.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

Refer to Section 5.5 for archival conditions.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

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

Key/Certificate	Key Algorithm and Length	Maximum validity period
Signit Licensed CA	RSA 4096	Validity period determined at issuance and shall not exceed the remaining validity of the signing Root CA certificate
Signit Digital Signing CA	ECC P-384	Defined at issuance and limited by the validity of Signit Licensed CA certificate
Signit Corporate Signing CA	ECC P-384	Defined at issuance and limited by the validity of Signit Licensed CA certificate
Signit Timestamping CA	ECC P-384	Defined at issuance and limited by the validity of Signit Licensed CA certificate

After its validity period, the old CA and its private key will only be used for signing CRLs while there are active certificates issued by it.

The following constraints apply to validity periods of certificates issued by Signit:

- The validity period of Signit Licensed CA certificate shall not exceed the validity period of the Saudi National Root CA certificate.

- The validity period of any Document Signing CAs certificates shall not exceed the validity period of Signit Licensed CA certificate.
- The validity period of any Signit Timestamping CA certificate shall not exceed the validity period of Signit Licensed CA certificate.
- The validity period of OCSP responder certificates shall not exceed the validity period of the issuing CA certificate.
- The validity period of end-entity certificates shall not exceed the validity period of the issuing CA certificate.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

6.4.1.1. Signit CAs

The CAs private keys and HSM activation data is generated during their private key generation ceremonies. Refer to Section 6.1.1 and 6.2.8 of this CP/CPS for further details.

6.4.1.2. Subscribers

Subscribers shall set and protect the activation data for their private keys to the extent necessary to prevent the loss, theft, unauthorized disclosure, and use of these private keys. Such obligations are presented to the subscribers as part of the Subscriber Agreement.

For Short-term certificates, the activation data will be set at the time of signature and will expire after the signing key has been used.

6.4.2. Activation Data Protection

6.4.2.1. Signit CAs

Signit key management policy and ceremony procedures ensure that the principles of multi-person control and split knowledge are permanently enforced to protect Signit keys and HSMs activation data. During the KGCs, activation data are permanently under the custody of the designated Signit staff. Refer to Section 6.1 and 6.2 for further details.

6.4.2.2. Subscribers

Subscribers protect the activation data for their private keys to the extent necessary to prevent the loss, theft, unauthorized disclosure, and use of these private keys. Such obligation is presented to the subscribers as part of the Subscriber Agreement.

For Short-term certificates, activation data are not retained beyond the intended use of the signing key.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Signit implements computer security controls to protect all Signit PKI systems. These controls follow recognized security standards, vendor hardening guidance, and Signit internal security policies governing trust services.
Signit PKI systems and supporting components operate under the following technical security measures:

- Clear separation of duties and enforcement of dual-control principles for sensitive PKI operations
- Strong physical and logical access controls based on trusted roles and least-privilege access
- Mandatory multi-factor authentication for privileged accounts and roles capable of influencing certificate issuance or CA operations
- Secure remote administrative access through controlled network entry points and encrypted communication channels
- Continuous logging and monitoring of application activity, system events, and security-relevant actions
- Endpoint protection and continuous security monitoring across PKI systems and supporting infrastructure
- Operating system and platform hardening in accordance with vendor recommendations and security best practices
- Network segmentation using controlled security zones, firewalls, and traffic filtering mechanisms to restrict communications to authorized services and protocols only
- Controlled patch and vulnerability management processes to maintain secure system configurations
- Backup, recovery, and resilience mechanisms aligned with Signit business continuity objectives

These controls apply consistently across Signit PKI environments, including HSM-connected systems and supporting infrastructure and all hosted components. For the physical security controls are managed by the approved infrastructure and facilities providers while Signit retains full responsibility for logical security configuration, access governance, monitoring, and operational control of PKI systems.

Internal procedures define how these technical controls are implemented, monitored, and periodically reviewed to ensure continued compliance with applicable trust service and regulatory requirements.

6.5.2. Computer Security Rating

Signit deploys CA software evaluated against recognized assurance standards, including Common Criteria EAL4 or equivalent, where applicable.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Hardware and software used for Signit services are obtained from trusted suppliers and delivered in sealed and tamper-evident packaging. Installation, configuration, and deployment activities are

performed only by authorized personnel holding trusted roles and in accordance with documented operational procedures.

All systems, applications, and updates follow a formal change and configuration management process. No software, patch, or hardware component is deployed into the production environment before testing, validation, and approval by the PKI operations team.

Signit ensures that CA systems, supporting platforms, and all PKI components are hardened according to vendor security recommendations and recognized industry practices.

6.6.2. Security Management Controls

Systems supporting Signit CA operations are dedicated to certification services and related security functions. Applications, services, network connections, and software components not required for PKI operations are not installed or enabled.

A formal configuration management process ensures that system configurations, modifications, and upgrades are documented, reviewed, and approved by authorized personnel. Baseline configurations are maintained to ensure consistency and detect unauthorized changes.

Security monitoring mechanisms include malware protection, integrity monitoring where applicable, and centralized logging of security-relevant events.

Signit maintains a documented vulnerability management process to identify, assess, and remediate security weaknesses affecting CA systems and supporting infrastructure. Critical vulnerabilities are evaluated and remediated within ninety-six (96) hours of identification, unless a documented risk assessment determines that immediate remediation would introduce greater operational risk. In such cases, compensating controls are implemented where appropriate.

6.6.3. Life Cycle Security Controls

Signit enforces policies and procedures governing the full life cycle of systems and infrastructure supporting certification services. All software releases, configuration changes, and system updates are formally documented and subject to change control procedures. Production configurations are reviewed on a regular basis, in accordance with Signit change management procedures, to detect deviations from approved configuration baselines and identify potential security issues.

Security patches and updates are applied within defined timeframes based on their severity, in accordance with documented patch management procedures. Where the application of a patch is deferred due to identified risks, the justification is documented and appropriate mitigating controls are implemented.

In addition to software and configuration management, Signit enforces comprehensive security controls throughout the entire life cycle of hardware and systems from secure procurement of trusted equipment, through installation, operation, and maintenance, to secure disposal and data eradication at the end of their service life. Access to critical systems is strictly limited to authorized personnel only, and all changes and activities are logged and monitored to safeguard the integrity, confidentiality, and availability of Signit certification services.

6.7. Network Security Controls

Signit implements layered network security controls to protect certification services and supporting systems across its PKI environments.
Network traffic is filtered through managed firewalls and monitored using intrusion detection and security monitoring capabilities. The infrastructure is segmented into dedicated network zones based on operational roles and security requirements, ensuring that systems communicate only where strictly necessary.
Communication between systems is restricted through defined network boundaries. Only approved services, protocols, ports, and communication paths required for certification operations are permitted. All unnecessary services, interfaces, and network pathways are disabled or blocked by default.
Secure encrypted communication channels are used for data exchanges between PKI systems components and cryptographic infrastructure. Administrative access to PKI systems is permitted only through controlled network entry points using authenticated and encrypted connections. Critical PKI components, including issuing systems, certificate management services, HSM-connected systems, and time synchronization services, operate within restricted and monitored network zones. Network activity is logged and subject to continuous monitoring to detect unauthorized or anomalous behavior.
These controls collectively support the confidentiality, integrity, and availability of Signit certification services.

6.8. Timestamping

Signit ensures that Certification Authority (CA) systems maintain accurate and consistent system time through synchronization with trusted time sources aligned with authoritative UTC references.

The PKI systems and cryptographic components synchronize with the Network Time Protocol (NTP) service provided by the infrastructure provider, which is aligned with authoritative time sources. Cryptographic components and related infrastructure hosted within Signit-controlled facilities use internally configured time synchronization services to maintain consistent system time across PKI components.

Time synchronization mechanisms are configured to ensure consistency across all PKI systems and cryptographic components. Controls are in place to detect significant clock drift and apply controlled corrections where necessary to preserve time integrity.

Events related to material time adjustments, including clock changes exceeding one second, are recorded as auditable events. These controls support the integrity of certificate issuance, validation, and audit logging activities. Operational controls related to electronic timestamp generation are defined separately within the dedicated Time-Stamping Policy and Practice Statement.

7.Certificate, CRL, OCSP, and TSA Profiles

7.1. Certificate Profile

7.1.1. Certificate Extensions

Signit comply with RFC 5280 in all certificates it issues.

The certificates issued by Signit Timestamping CA are compliant with the specifications included in ETSI EN 319 422 – Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.

The ''privateKeyUsagePeriod'' extension is used within TSU certificates.

This CP/CPS specifies extensions used in all certificates issued by Signit PKI hierarchy (refer to section 7.1.10,7.1.11).

7.1.2. Version Number(s)

Signit issue X.509 version 3 certificates as defined in RFC 5280.

7.1.3. Algorithm Object Identifiers

Certificates are issued with algorithms indicated by the following OID:

Algorithm	Object Identifier
sha256WithRSAEncryption	OBJECT IDENTIFIER ::= { iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
ecdsa-with-SHA384	OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }

7.1.4. Name Forms

As defined in sections 7.1.10 and 7.1.11

7.1.5. Name Constraints

Name constraints extension is not supported.

7.1.6. Certificate Policy Object Identifier

Certificate policy object identifiers are used as per RFC 3739 and RFC 5280.

Signit uses certificate policy object identifiers defined for the Saudi National PKI OID schema. The used OIDs are specified as part of the certificate profiles in Sections 7.1.10 and 7.1.11

Two certificate policy object identifiers are defined for eSeal certificates issued to legal persons, reflecting the two key generation models described in Section 6.1.1.2:

2.16.682.1.101.5000.1.4.1.4.1.2.2.1 is asserted where the key pair is generated and held under the Signit-managed key-generation model;

2.16.682.1.101.5000.1.4.1.4.1.2.2.2 is asserted where the key pair is generated and held under the applicant-generated key-pair model.

Exactly one of these identifiers is asserted in each eSeal certificate. The full list of object identifiers allocated by Signit is set out in Section 1.2.

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

Signit contains a CP/CPS Policy Qualifier that points to the applicable CP/CPS.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

Certificate policies extensions must be processed as per RFC 5280.

7.1.10. Signit Certificate Profiles

7.1.10.1. Signit Licensed CA

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

* CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	NIC Root CA Signature.	NIC Root CA's signature value
Version	False	M	S		
Version		M	S	2	Version 3
SerialNumber	False	M	D		
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M	S		
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption

Issuer	False	M	S		The issuer field is defined as the X.501 type "Name"
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	National Center for Digital Certification	UTF8 encoded
Organizational Unit		M	S	Saudi National Root CA	UTF8 encoded
Validity	False	M	D		Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	The certificate validity SHALL be less than or equal to the NotAfter value of the issuing CA certificate.	Validity period determined at issuance and shall not exceed the remaining validity of the signing Root CA certificate .The Saudi Root CA which expires on 29th , November 2029
Subject	False				
CountryName		M	D	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Licensed CA	UTF8 encoded
SubjectPublicKeyInfo	False	M	D		
AlgorithmIdentifier		M	D	RSA (OID: 1.2.840.113549.1.1.1) NULL	
SubjectPublicKey		M	D	Key length: 4096	
AuthorityKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Issuer public key	MUST be identical to the subjectKeyIdentifier field
Subject Properties					
SubjectKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.ncdc.gov.sa	OCSP responder URL

	AccessMethod			M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation			M	S	http://web.ncdc.gov.sa/certs/snrcasha256.crt	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints			False	M			
	DistributionPoint	fullName		M	S	http://web.ncdc.gov.sa/crl/nrcaparta<n>.crl	
		directoryName				CN=CRL1 OU=Saudi National Root CA O=National Center for Digital Certification C=SA	
	DistributionPoint	fullName		M	S	http://web.ncdc.gov.sa/crl/nrcacomb<n>.crl	
Key Usage Properties							
keyUsage			True	M	S		
	keyCertSign, cRLSign			M	S	True	
Policy Properties							
certificatePolicies			False	M			
	PolicyIdentifier			M	S	2.16.682.1.101.5000.1.2.1.1	
	policyQualifiers:policyQualifierId			M	S	id-qt 1	
	policyQualifiers:qualifier:CP/CPSuri			M	S	http://web.ncdc.gov.sa	
Basic Constraints Properties							
basicConstraints			True	M	S		
	cA			M	S	True	

7.1.10.2. Signit Subordinate CAs

7.1.10.2.1. Signit Digital Signing CA

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

* CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Signit Licensed CA Signature	Signit Licensed CA's signature value
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			

AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			The issuer field is defined as the X.501 type "Name"
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Licensed CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	The certificate validity SHALL be less than or equal to the NotAfter value of the issuing CA certificate.	Defined at issuance and limited by the validity of Signit Licensed CA certificate
Subject	False				
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Digital Signing CA	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	s	ECDSA (OID: 1.2.840.10045.2.1) secp384r1 (OID: 1.3.132.0.34)	
SubjectPublicKey		M	D	Value of the key	
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Root CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			

	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	http://ocsp.pki.signit.sa	OCSP responder URL
	AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		M	S	http://repository.pki.signit.sa/cert/lic_ca.p7b	Signit Licensed CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://repository.pki.signit.sa/crl/lic_ca.crl	CARL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties						
keyUsage		True	M			
	keyCertSign, cRLSign		M	S	True	
Enhanced Key Usage Properties						
enhancedKeyUsage		False	M	S		
	Microsoft Document Signing		M		1.3.6.1.4.1.311.10.3.12	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.682.1.101.5000.1.4.1.4.1.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:CPSuri		M	S	https://repository.pki.signit.sa/cp_cps	
Basic Constraints Properties						
basicConstraints		True	M			
	cA		M	S	True	
	pathLenConstraint		M	S	0	

7.1.10.2.2. Signit Corporate Signing CA

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

* CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption

	SignatureValue		M	D	Signit Licensed CA Signature	Signit Licensed CA's signature value
Version		False	M			
	Version		M	S	2	Version 3
SerialNumber		False	M			
	CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature		False	M			
	AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer		False	M			The issuer field is defined as the X.501 type "Name"
CountryName			M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName			M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName			M	S	Signit Licensed CA	UTF8 encoded
Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	The certificate validity SHALL be less than or equal to the NotAfter value of the issuing CA certificate.	Defined at issuance and limited by the validity of Signit Signit Licensed CA certificate
Subject		False				
CountryName			M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName			M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName			M	S	Signit Corporate Signing CA	UTF8 encoded
SubjectPublicKeyInfo		False	M			
	AlgorithmIdentifier		M	s	ECDSA (OID: 1.2.840.10045.2.1) secp384r1 (OID: 1.3.132.0.34)	
	SubjectPublicKey		M	D	Value of the key	

Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Root CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.signit.sa	OCSP responder URL
AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		M	S	http://repository.pki.signit.sa/cert/lic_ca.p7b	Signit Licensed CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://repository.pki.signit.sa/crl/lic_ca.crl	CARL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M			
keyCertSign, cRLSign		M	S	True	
Enhanced Key Usage Properties					
enhancedKeyUsage	False	M	S		
Microsoft Document Signing		M		1.3.6.1.4.1.311.10.3.12	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.682.1.101.5000.1.4.1.4.1.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:CP/CPSuri		M	S	https://repository.pki.signit.sa/cp_cps	
Basic Constraints Properties					
basicConstraints	True	M			
cA		M	S	True	
pathLenConstraint		M	S	0	

7.1.10.2.3. Signit Timestamping CA

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

* CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	Signit Licensed CA Signature	Signit Licensed CA's signature value
Version	False	M	S		
Version		M	S	2	Version 3
SerialNumber	False	M	D		
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M	S		
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M	S		The issuer field is defined as the X.501 type "Name"
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Licensed CA	UTF8 encoded
Validity	False	M	D		Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	The certificate validity SHALL be less than or equal to the NotAfter value of the issuing CA certificate.	Defined at issuance and limited by the validity of Signit Signit Licensed CA certificate
Subject	False				
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements".

					PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Timestamping CA	UTF8 encoded
SubjectPublicKeyInfo	False	M	D		
AlgorithmIdentifier		M	s	ECDSA (OID: 1.2.840.10045.2.1)	
				secp384r1 (OID: 1.3.132.0.34)	
SubjectPublicKey		M	D	Value of the key	
Authority Properties					
AuthorityKeyIdentifier	False	M	D		Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Root CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M	S		
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	*http://ocsp.pki.signit.sa*	OCSP responder URL
AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		M	S	*http://repository.pki.signit.sa/cert/lic_ca.p7b*	Signit Licensed CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M	S		
DistributionPoint		M	S	*http://repository.pki.signit.sa/crl/lic_ca.crl*	CARL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M	S		
keyCertSign, cRLSign		M	S	True	
ExtendedKeyUsage	False	M			
id-kp-timeStamping		M	S	True	
Policy Properties					
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.16.682.1.101.5000.1.4.1.4.1.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:CPSuri		M	S	https://repository.pki.signit.sa/cp_cps	
Basic Constraints Properties					

basicConstraints		True	M	S		
	cA		M	S	True	
	pathLenConstraint		M	S	0	

7.1.10.3. Signit End-entity Certificates

7.1.10.3.1. Legal Person (eSeal) Certificate Profile

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
SignatureValue		M	D	Subordinate CA Signature.	Client Auth Subordinate CA's signature value
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
Issuer	False	M			The issuer field is defined as the X.501 type "Name"
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Corporate Signing CA	UTF8 encoded

Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using Generalised Time
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	The certificate validity SHALL be less than or equal to the NotAfter value of the issuing CA certificate.	Suggested validity for the end user certificate is up to 03 years
Subject		False				
CountryName			M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
localityName			M/O	D	City / locality	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
stateOrProvinceName			M/O	D	State / province / region	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
OrganizationName			M	D	organization's legal name	UTF8 encoded
OrganizationIdentifier			M	D	An identification of the subject organization, distinct from the organization name, which is specifically intended to uniquely identify the legal entity in a standardized and verifiable manner. It should be the Unified National Number (e.g., NTRSA-<UNN>)	UTF8 encoded
SerialNumber			O	D	Signit platform-generated unique entity identifier (opaque hash)	PrintableString encoded
OrganizationalUnit			O	D	organizational unit name within the legal entity	UTF8 encoded

businessCategory		O	D	Business sector / category of organization	UTF8 encoded
CommonName		M	D	Full organization registered name. shall contain a name commonly used by the subject to represent itself. This name needs not be an exact match of the fully registered organization name	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	s	ECDSA (OID: 1.2.840.10045.2.1)	
				Secp256r1 (OID: 1.2.840.10045.3.1.7) Or Secp384r1 (OID: 1.3.132.0.34)	
SubjectPublicKey		M	D	Value of the key	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate Issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.signit.sa	OCSP responder URL
AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		M	S	http://repository.pki.signit.sa/cert/corp_ca.p7b	Legal Subordinate CA Certificate/ Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://repository.pki.signit.sa/crl/corp_ca.crl	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported

						as a minimum
Key Usage Properties						
keyUsage		True	M			
	Digital signature contentCommitment		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.682.1.101.5000.1.4.1.4.1.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:CP/CPSuri		M	S	https://repository.pki.signit.sa/cp_cps	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.682.1.101.5000.1.4.1.4.1.2.2.1 (remote eSeal) or 2.16.682.1.101.5000.1.4.1.4.1.2.2.2 (local eSeal)	Exactly one identifier is asserted. The ...2.2.1 identifier is used where the key pair is generated and held under the Signit-managed key-generation model. The ...2.2.2 identifier is used where the key pair is generated and held under the applicant-generated key-pair model. See Sections 1.2, 6.1.1.2 and 7.1.6.

7.1.10.3.2. Short-term Signing Certificate Profile

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384

SignatureValue		M	D	Subordinate CA Signature.	Natural Person Subordinate CA signature value
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
Issuer	False	M			The issuer field is defined as the X.501 type "Name"
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Digital Signing CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[30]** minutes	Suggested validity for the end user certificate is up to 30 minutes
Subject	False				
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
GivenName		M	D	Individual's authenticated given name	UTF8 encoded
Surname		M	D	Individual's authenticated surname	UTF8 encoded
SERIALNUMBER		M	D	Individual Unique Identifier generated by Signit. The value consists of a 64-character hexadecimal SHA-256 hash derived from the subscriber's National ID combined with a secret salt maintained by Signit.	PrintableString encoded
localityName		M/O	D	City / locality	UTF8 encoded. Mandatory if the stateOrProvinc

					eName field is not present, optional if the stateOrProvinceName is present.
stateOrProvinceName		M/O	D	State / province / region	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
CommonName		M	D	Individual's full name	UTF8 encoded
Description		O	D	Intended to contain a Partially masked National ID for human-readable display purposes only. The value shall not be used as the authoritative subject identifier or relied upon for identity validation, authentication, authorization, or automated processing.	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	s	ECDSA (OID: 1.2.840.10045.2.1) Secp256r1 (OID: 1.2.840.10045.3.1.7)	
SubjectPublicKey		M	D	Value of the key	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate Issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	O			
AccessMethod		O	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		O	S	http://ocsp.pki.signit.sa	OCSP responder URL
AccessMethod		O	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		O	S	http://repository.pki.signit.sa/cert/dig_ca.p7b	Subordinate CA Certificate/Chain download URL over HTTP
ext-etsi-valassured-ST-certs	False	M	S	ext-etsi-valassured-ST-certs	Short-term certificate for which revocation does not apply
Subject Properties					

SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M			
Digital signature contentCommitment		M	S	True	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.682.1.101.5000.1.4.1.4.1.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:CP/CPSuri		M	S	https://repository.pki.signit.sa/cp_cps	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.16.682.1.101.5000.1.4.1.4.1.2.1.1	OID Referring to Short-term Signing Certificate

7.1.10.3.3. Timestamping Unit (TSU) Certificates Profiles

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
SignatureValue		M	D	Subordinate CA Signature.	TSA Subordinate CA's signature value
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
Issuer	False	M			The issuer field is defined as the X.501 type "Name"

CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Timestamping CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	The certificate validity SHALL be less than or equal to the NotAfter value of the issuing CA certificate.	Suggested validity for the end user certificate is up to 03 years
Subject	False				
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	Signit for Information Systems Technology	UTF8 encoded
OrganizationIdentifier		M	D	An identification of the subject organization, distinct from the organization name, which is specifically intended to uniquely identify the legal entity in a standardized and verifiable manner. It should be the Unified National Number (e.g., NTRSA-<UNN>)	UTF8 encoded
CommonName		M	D	Signit Timestamping Service G1 - [year]	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	s	ECDSA (OID: 1.2.840.10045.2.1) secp384r1 (OID: 1.3.132.0.34)	
SubjectPublicKey		M	D	Value of the key	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the subordinate issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			

	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	http://ocsp.pki.signit.sa	OCSP responder URL
	AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		M	S	http://repository.pki.signit.sa/cert/tsa_ca.p7b	Subordinate CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://repository.pki.signit.sa/crl/tsa_ca.crl	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties						
keyUsage		True	M			
	Digital signature		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.682.1.101.5000.1.4.1.4.1.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:CP/CPSuri		M	S	https://repository.pki.signit.sa/cp_cps	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.682.1.101.5000.1.4.1.4.1.2.3.1	
Extended Key Usage Properties						
extendedKeyUsage		True	M			
	timeStamping		M	S	True	
Private Key Usage Period		False	M			
	GeneralizedTime		M	D	notBefore notAfter	This extension indicates the period of use of the private key corresponding to the certified public key. A new Key pair will be generated each 12 months

7.1.10.3.4. Signature Validation Certificate Profile

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
SignatureValue		M	D	Subordinate CA Signature.	Legal Person Subordinate CA signature value
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
Issuer	False	M			
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Corporate Signing CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	The certificate validity SHALL be less than or equal to the NotAfter value of the issuing CA certificate.	Suggested validity for the end user certificate is up to 03 years
Subject	False	M			
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
OrganizationIdentifier		M	S	An identification of the subject organization, distinct from the organization name, which is specifically intended to uniquely identify the legal entity in a standardized and verifiable manner. It should be the Unified National Number (e.g., NTRSA-<UNN>)	UTF8 encoded

CommonName		M	S	Signature Verification Service	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	ECDSA (OID: 1.2.840.10045.2.1)	
				secp384r1 (OID: 1.3.132.0.34)	
SubjectPublicKey		M	D	Value of the key	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	SHA-1 Hash of the Infrastructure CA's public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M			
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.signit.sa	OCSP responder URL
AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		M	S	http://repository.pki.signit.sa/cert/corp_ca.p7b	Subordinate CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M			
DistributionPoint		M	S	http://repository.pki.signit.sa/crl/corp_ca.crl	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Policy Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
Certificate Policies	False	M			
policyIdentifier		M	S	2.16.682.1.101.5000.1.4.1.4.1.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:CP/CPSuri		M	S	https://repository.pki.signit.sa/cp_cps	
Certificate Policies	False	M			
policyIdentifier		M	S	2.16.682.1.101.5000.1.4.1.4.1.2.2.3	OID Referring to Signature Validation Certificate

7.2. CRL & CARL Profiles

CRL profile is in accordance with X.509 version 2 and the IETF RFC 5280. Signit will issue version 2 CRLs that contain the following fields:

7.2.1. Signit Licensed CA CARL Profile

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
CertificateList		M			
TBSCertificate					
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	The signature of the CA issuing the CRL.	The signature of the authority issuing the CRL.
Version	False	M			
Version			S	1	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	SA	
OrganizationName		M	S	Signit for Information Systems Technology	
CommonName		M	S	Signit Licensed CA	
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
thisUpdate		M	D	<creation time>	
NextUpdate		M	D	<Creation time> + [**12**] months	**Validity period** is 12 months for CRLs issued by Signit Licensed CA
RevokedCertificates	False	M			
CertificateSerialNumber		M	D	Serial of the revoked certificates	
revocationDate		M	D	Date when revocation was processed by the CA	UTC time of revocation
crlEntryExtension	False	M			
reasonCode		M	D		Identifies the reason for the certificate revocation
CRLExtensions	**False**	**M**			
AuthorityKeyIdentifier	False	M	D	160-bit SHA-1 hash of the public key of the CA issuing the CRL	
CRL Number	False	M	D		Sequential CRL Number

	expiredCertsOnCRL	False	M	D	<GeneralizedTime indicating the date from which expired certificate revocation information is retained>	OID = 2.5.29.60. Extension indicating that the CRL contains revocation information for expired certificates

7.2.2. Subordinate CAs CRL Profiles

7.2.2.1. Signit Digital Signing CA CRL

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
CertificateList		M			
TBSCertificate					
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
SignatureValue		M	D	The signature of the CA issuing the CRL.	The signature of the authority issuing the CRL.
Version	False	M			
Version			S	1	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
Issuer	False	M			
CountryName		M	S	SA	
OrganizationName		M	S	Signit for Information Systems Technology	
CommonName		M	S	Signit Digital Signing CA	
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
thisUpdate		M	D	<creation time>	
NextUpdate		M	D	<Creation time> + **[1] day** + 2 hours	
RevokedCertificates	False	M			
CertificateSerialNumber		M	D	Serial of the revoked certificates	
revocationDate		M	D	Date when revocation was processed by the CA	UTC time of revocation
crlEntryExtension	**False**	**M**			
reasonCode		M	D		Identifies the reason for the certificate revocation
CRLExtensions	**False**	**M**			

	AuthorityKeyIdentifier	False	M	D	160-bit SHA-1 hash of the public key of the CA issuing the CRL	
	CRL Number	False	M	D		Sequential CRL Number
	expiredCertsOnCRL	False	M	D	<GeneralizedTime indicating the date from which expired certificate revocation information is retained>	OID = 2.5.29.60. Extension indicating that the CRL contains revocation information for expired certificates

7.2.2.2. Signit Corporate Signing CA CRL

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
CertificateList		M			
TBSCertificate					
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
SignatureValue		M	D	The signature of the CA issuing the CRL.	The signature of the authority issuing the CRL.
Version	False	M			
Version			S	1	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
Issuer	False	M			
CountryName		M	S	SA	
OrganizationName		M	S	Signit for Information Systems Technology	
CommonName		M	S	Signit Corporate Signing CA	
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
thisUpdate		M	D	<creation time>	
NextUpdate		M	D	<Creation time> + **[1] day** + 2 hours	
RevokedCertificates	False	M			
CertificateSerialNumber		M	D	Serial of the revoked certificates	
revocationDate		M	D	Date when revocation was processed by the CA	UTC time of revocation
crlEntryExtension	False	M			
reasonCode		M	D		Identifies the reason for the certificate revocation

CRLExtensions		False	M			
	AuthorityKeyIdentifier	False	M	D	160-bit SHA-1 hash of the public key of the CA issuing the CRL	
	CRL Number	False	M	D		Sequential CRL Number
	expiredCertsOnCRL	False	M	D	<GeneralizedTime indicating the date from which expired certificate revocation information is retained>	OID = 2.5.29.60. Extension indicating that the CRL contains revocation information for expired certificates

7.2.2.3. Signit Timestamping CA CRL

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
CertificateList		M			
TBSCertificate					
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
SignatureValue		M	D	The signature of the CA issuing the CRL.	The signature of the authority issuing the CRL.
Version	False	M			
Version			S	1	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
Issuer	False	M			
CountryName		M	S	SA	
OrganizationName		M	S	Signit for Information Systems Technology	
CommonName		M	S	Signit Timestamping CA	
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
thisUpdate		M	D	<creation time>	
NextUpdate		M	D	<Creation time> + 30 days + 1 day	
RevokedCertificates	False	M			
CertificateSerialNumber		M	D	Serial of the revoked certificates	
revocationDate		M	D	Date when revocation was processed by the CA	UTC time of revocation
crlEntryExtension	False	M			

	reasonCode		M	D		Identifies the reason for the certificate revocation
CRLExtensions		**False**	**M**			
	AuthorityKeyIdentifier	False	M	D	160-bit SHA-1 hash of the public key of the CA issuing the CRL	
	CRL Number	False	M	D		Sequential CRL Number
	expiredCertsOnCRL	False	M	D	<GeneralizedTime indicating the date from which expired certificate revocation information is retained>	OID = 2.5.29.60. Extension indicating that the CRL contains revocation information for expired certificates

7.2.3. Version Number(s)

Signit support X509 v2 CRLs.

7.2.4. CRL and CRL Entry Extensions

Signit use the CRL and CRL entry extensions as described in section 7.2.

7.3. OCSP Profile

The OCSP profile complies with the requirements of RFC 6960.

7.3.1. Signit Intermediate OCSP Responder Certificate

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	CA's Signature.	CA's Signature.
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			

AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			The issuer field is defined as the X.501 type "Name"
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Licensed CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + validity period	**Validity period** is 12 months for OCSP Certificates
Subject	False	M			
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Licensed CA OCSP	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		**M**			
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	
Authority Properties					
AuthorityKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of the public key of the CA issuing the OCSP Certificate	When this extension is used, this field MUST be supported as a minimum
keyUsage	True	M			
digitalSignature		M	S	True	
extKeyUsage	False	M			
id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck	False	M			

7.3.2. Subordinate CAs OCSP Responder Certificate

7.3.2.1. Signit Digital Signing CA OCSP Responder Certificate

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
SignatureValue		M	D	CA's Signature.	CA's Signature.
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
Issuer	False	M			The issuer field is defined as the X.501 type "Name"
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Digital Signing CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + validity period	**Validity period** is 12 months for OCSP Certificates
Subject	False	M			
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Digital Signing CA OCSP	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	ECDSA (OID: 1.2.840.10045.2.1) secp384r1 (OID: 1.3.132.0.34)	
SubjectPublicKey		M	D	Value of the key	

Extensions		**M**			
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	
Authority Properties					
AuthorityKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of the public key of the CA issuing the OCSP Certificate	When this extension is used, this field MUST be supported as a minimum
keyUsage	True	M			
digitalSignature		M	S	True	
extKeyUsage	False	M			
id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck	False	M			

7.3.2.2. Signit Corporate Signing CA OCSP Responder Certificate

*CE = Critical Extension.

*O/M: O = Optional, M = Mandatory.

*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
SignatureValue		M	D	CA's Signature.	CA's Signature.
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
Issuer	False	M			The issuer field is defined as the X.501 type "Name"
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Corporate Signing CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	

NotAfter		M	D	Certificate generation process date/time + validity period	**Validity period** is 12 months for OCSP Certificates
Subject	False	M			
CountryName		M	S	SA	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Corporate Signing CA OCSP	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	ECDSA (OID: 1.2.840.10045.2.1) secp384r1 (OID: 1.3.132.0.34)	
SubjectPublicKey		M	D	Value of the key	
Extensions		**M**			
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	
Authority Properties					
AuthorityKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of the public key of the CA issuing the OCSP Certificate	When this extension is used, this field MUST be supported as a minimum
keyUsage	True	M			
digitalSignature		M	S	True	
extKeyUsage	False	M			
id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck	False	M			

7.3.2.3. Signit Timestamping CA OCSP Certificate

*CE = Critical Extension.
*O/M: O = Optional, M = Mandatory.
*CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
SignatureValue		M	D	CA's Signature.	CA's Signature.
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			

AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	ECDSA with SHA-384
Issuer	False	M			The issuer field is defined as the X.501 type “Name”
CountryName		M	S	SA	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Timestamping CA	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + validity period	**Validity period** is 12 months for OCSP Certificates
Subject	False	M			
CountryName		M	S	SA	Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Signit for Information Systems Technology	UTF8 encoded
CommonName		M	S	Signit Timestamping CA OCSP	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	ECDSA (OID: 1.2.840.10045.2.1) secp384r1 (OID: 1.3.132.0.34)	
SubjectPublicKey		M	D	Value of the key	
Extensions		**M**			
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	
Authority Properties					
AuthorityKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of the public key of the CA issuing the OCSP Certificate	When this extension is used, this field MUST be supported as a minimum
keyUsage	True	M			
digitalSignature		M	S	True	
extKeyUsage	False	M			
id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck	False	M			

7.4. OCSP Request and Response Formats

7.4.1. OCSP Request Format

Profile describes OCSP request according to RFC 6960.

Field		O/M	Value	Comment
tbsRequest				
Version			v1(0)	See 4.1.2 of RFC 5280
request				
CertID		M		
	hashAlgorithm	M		hashAlgorithm is the hash algorithm used to generate the issuerNameHash and issuerKeyHash values. Supported hash algorithms are SHA-256, SHA-384 and SHA-512.
	issuerNameHash	M		Hash of issuer's DN
	issuerKeyHash	M		Hash of issuer's public key
	serialNumber	M		CertificateSerialNumber
nonce		O	INTEGER	Optional nonce provided by the requester. When present, the OCSP responder echoes the same nonce value in the corresponding response.

7.4.2. OCSP Response Format

Profile describes OCSP response according to RFC 6960.

Field		Value	Comment
responseStatus		"0" Response has valid confirmations	Result of the query. If the value of responseStatus is other than "0", the responseBytes field is not set.
responseBytes			
responseStatus		"0" Response has valid confirmations	Result of the query. If the value of responseStatus is other than "0", the responseBytes field is not set.
BasicOCSPResponse			
tbsResponseData			
	version	v1 (value = 0)	Version of the response format
	responderID	C = SA O = <The full registered name of the subject> CN = <A name commonly used by the subject to represent itself>	Distinguished name of the OCSP responder. The information MUST correspond to the certificate that was used to sign the response.
	producedAt		The time at which the OCSP responder signed this response.
	responses		
	certID		In accordance with RFC 6960
	hashAlgorithm	Depending on the hash algorithm used in request	hashAlgorithm is the hash algorithm used to generate the issuerNameHash and issuerKeyHash values. Supported hash algorithms are SHA-256, SHA-384 and SHA-512.

	issuerNameHash		Hash of issuer's DN
	issuerKeyHash		Hash of issuer's public key
	SerialNumber		CertificateSerialNumber
	certStatus		Status of the certificate: • Good – certificate issued and has not been revoked. • Revoked – certificate is revoked. The certificate has been revoked, or the serial number has not been issued by the CA. For non-issued serial numbers, the response uses the extended revoked definition defined in RFC 6960 section 4.4.8 • Unknown – the OCSP responder is unable to determine the certificate status because the issuing CA referenced in the OCSP request is not recognized or not managed by the OCSP responder(i.e., the OCSP responder does not recognize the issuing CA of the certificate).
	thisUpdate		The most recent time at which the status being indicated is known by the responder to have been correct.
	nextUpdate	ThisUpdate + 8 hours	The time at or before which newer information will be available about the status of the certificate
	ArchiveCutoff	the CA's certificate "notBefore" time and date value	According to RFC 6960 clause 4.4.4. "archive cutoff" date set to the CA's certificate "notBefore" time and date value According to ETSI EN 319 411-2 / CSS-6.3.10-10.
	id-pkix-ocsp-extended-revoke	Null	Non-critical extension. Indicates that the OCSP responder supports the extended definition of “revoked” for non-issued certificate serial numbers, in accordance with RFC 6960 section 4.4.8
	signatureAlgorithm	Sha256withRSAEncryption (for Signit Licensed CA OCSP responder) / ecdsa-with-SHA384 (for Subordinate CAs OCSP responder)	Signing algorithm
	signature		signature value
	certs		Certificate corresponding to the private key used to sign the response. Only OCSP responder certificate is included in the OCSP response.

7.5. Timestamp Request and Response Formats

7.5.1. TSA Request Format

Profile describes TSA request according to RFC 3161.

Field	Value	Comment

Version	v1	the version of the Time-Stamp request
messageImprint		contain the hash of the datum to be time-stamped
hashAlgorithm	AlgorithmIdentifier	Supported has algorithms are:SHA256,SHA384,SHA512
hashedMessage	OCTET STRING	
reqPolicy	2.16.682.1.101.5000.1.4.1.4.1.1.2	The TSA policy OID under which the Time-Stamp Token is issued.
nonce	64 bit integer	The nonce, if included, allows the client to verify the timeliness of the response when no local clock is available. The nonce is a large random number with a high probability that the client generates it only once (e.g., a 64 bit integer). In such a case the same nonce value MUST be included in the response, otherwise the response shall be rejected.
certReq	True or False	if set to true, then the TSA's public key certificate field from the SignedData structure MUST be present in the response. If the certReq field is missing or if the certReq field is present and set to false then the certificates field from the SignedData structure MUST not be present in the response

7.5.2. TSA Response Format

Profile describes TSA Response according to RFC 3161

Field	Value	Comment
Status		
status	granted (0) grantedWithMods (1) rejection (2) waiting (3) revocationWarning (4) revocationNotification (5)	When the status contains the value zero or one, a TimeStampToken MUST be present. When status contains a value other than zero or one, a TimeStampToken MUST NOT be present.
timeStampToken		
version	v1	version of the time-stamp token
policy	2.16.682.1.101.5000.1.4.1.4.1.1.2	The TSA policy OID included in the response SHALL be identical to the policy OID specified in the corresponding TimeStampReq.
messageImprint	OCTET STRING	MUST have the same value as the similar field in TimeStampReq
hashAlgorithm	Depending on the hash algorithm used in request	Supported has algorithms are: SHA256,SHA384,SHA512
hashedMessage	OCTET STRING	
serialNumber	Integer up to 160 bits	an integer assigned by the TSA to each TimeStampToken
genTime	GeneralizedTime (UTC time)	the time at which the time-stamp token has been created by the TSA
Accuracy	1 (second)	accuracy specifies the maximum deviation of the TSA's reported time from true UTC, expressed in seconds, milliseconds, or microseconds
ordering	False	
nonce	64 bit integer	The same nonce value MUST be included in the request, otherwise the response shall be rejected.
tsa		if certReq set to true in request, then the TSA's public key certificate field from the SignedData structure MUST be present.

8. Compliance Audit and Other Assessments

8.1. Frequency or Circumstances of Assessment

Signit undergoes periodic external assessments performed by an independent WebTrust-qualified practitioner in accordance with the WebTrust for Certification Authorities audit framework. These assessments evaluate Signit conformity with applicable policies, operational practices, and technical controls governing certification services.

Certification operations conducted by Signit are assessed through successive audit periods, each not exceeding twelve (12) months.

Signit acknowledges and accepts independent audits of its certification practices. Audit reports are published within three (3) months following the end of the audit period. Upon issuance, audit results and relevant findings are communicated to the Digital Government Authority (DGA) and National Information Center (NIC) as required by applicable trust service obligations.

Signit GB reviews audit outcomes, evaluates identified observations or non-conformities, and oversees the implementation of corrective or preventive actions to maintain continued compliance.

In addition to external audits, Signit performs internal compliance reviews at least annually as part of its operational oversight activities. Assessments may also be initiated upon request from DGA, NIC or other competent authorities to verify continued alignment with applicable certificate policies.

8.2. Identity/Qualifications of Assessor

The external WebTrust audits will be performed by qualified auditors that fulfil the following requirements:

- Independence from the subject of the audit
- Ability to conduct an audit that addresses the criteria specified in WebTrust for Certification Authorities
- Employ individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and third-party attestation function
- Licensed by WebTrust
- Bound by law, government regulation or professional code of ethics
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

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

Signit are audited for compliance to the WebTrust Principles and Criteria for Certification Authorities.

The auditor shall provide an audit report to Signit and ensure that the report is made available to the relevant stakeholders involved in the certification hierarchy and regulatory oversight, as applicable, including the entities responsible for higher-level certification authorities and the applicable licensing framework.

8.5. Actions Taken as a Result of Deficiency

Issues and findings resulting from the assessment are reported to Signit GB.

Regarding compliance audits of Subordinate CA operations, any notable exceptions or deficiencies discovered during the audit process prompt a decision on necessary actions. This decision is made by Signit GB with input from the auditor.

In the event of exceptions or deficiencies, Signit GB is responsible for developing and implementing a corrective action plan, which must also be communicated to the DGA. Upon completion of the corrective measures, Signit GB initiates a follow-up audit to verify that all identified deficiencies have been properly addressed and resolved.

8.6. Communication of Results

Audit Reports, including identification of corrective measures taken or being taken by Signit, shall be provided to Signit and DGA as applicable.

External audits reports are published on Signit public repository.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

Applicable fees, if any, are to be agreed upon by Signit and subscribers.

9.1.2. Certificate Access Fees

No fees will be charged to access the certificates issued.

9.1.3. Revocation Or Status Information Access Fees

No fees will be charged for the certificate revocation and status information access.

9.1.4. Fees for Other Services

Signit may charge fees for additional trust services or related offerings according to its commercial policies.

9.1.5. Refund Policy

Not Applicable.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Insurance or financial responsibility arrangements applicable to Signit certification services, if any, are defined through applicable contractual agreements and internal governance decisions. Where required by applicable regulations, Signit shall ensure that appropriate financial protection or equivalent arrangements are established to support its certification operations.

9.2.2. Other Assets

Signit GB ensures the availability of sufficient financial resources to support the continuous operation of Signit. These resources are allocated to guarantee the fulfillment of its obligations in accordance with the provisions of this Certificate Practice Statement (CP/CPS).

9.2.3. Insurance or Warranty Coverage for End-Entities

Refer to section 9.2.1.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

All information obtained during the provision of services that is not intended for public disclosure, including information acquired by Signit in the course of operating and providing Trust Services,shall be treated as confidential.

9.3.2. Information Not within the Scope of Confidential Information

Any information not defined as confidential (refer to section 9.3.1) is deemed public. This includes the information published on the public repository.

9.3.3. Responsibility to Protect Confidential Information

Signit protects confidential information through adequate training and policy enforcement with its employees, contractors, and suppliers.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

Signit observes personal data privacy rules and privacy rules as specified in the present CP/CPS. Refer to section 9.4.2 for the scope of private information and to section 9.4.3 for the items that are not considered as private information.

Both private and non-private information can be subject to data privacy rules if the information contains personal data.

Only limited trusted personnel are permitted to access Signit private information for the purpose of certificate lifecycle management.

Signit will not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. When Signit releases private information, it will ensure through reasonable means that this information is not used for any purpose apart from the requested purposes. Parties granted access will secure the private data from compromise, and refrain from using it or disclosing it to other third parties. Also, these parties are bound to observe personal data privacy rules in accordance with the relevant laws in the Kingdom of Saudi Arabia.

Private information will not be disclosed by Signit to subscribers except for information about themselves and only covered by the contractual agreement between Signit and the subscribers

Signit respects all applicable privacy, private information, and where applicable trade secret laws and regulations, as well as its published privacy policy in the collection, use, retention, and disclosure of non-public information.

All communications channels with Signit shall preserve the privacy and confidentiality of any exchanged private information. Data encryption shall be used when electronic communication channels are used with the CA systems.

9.4.2. Information Treated as Private

All personal information that is not publicly available in the content of a certificate or CRL are considered as private information.

9.4.3. Information Not Deemed Private

Information included in the certificate or CRL is not considered as private.

9.4.4. Responsibility to Protect Private Information

Signit participants receiving private information must prevent it from being compromised or unveiled to third parties and shall comply with all applicable privacy laws and terms specified in Section 9.4.1.

9.4.5. Notice and Consent to Use Private Information

Signit ensure that collected personal information is used for the purpose of certificate life cycle management only as consented by the subscribers.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

Signit will not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. Refer to section 9.4.1 for more details.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. Intellectual Property Rights

Signit owns and reserves all intellectual property rights associated with Signit databases, repository, the CAs digital certificates and any other publication originating from Signit GB, including this CP/CPS.

Signit use software from third-party PKI products suppliers. This software remains the intellectual property of the product suppliers, and its usage by Signit bound by license agreements between Signit and these suppliers.

9.6. Representations and Warranties

9.6.1. CA Representations and Warranties

Signit provides representations and warranties in accordance with this CP/CPS, 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:
    - this CP/CPS;
    - Documented Operations Policies and Procedures; and
    - Within applicable agreements, Saudi Law and regulations.
- At the time of Certificate issuance; Signit implemented procedures for verifying accuracy of the information contained within it before installation and first use;
- Implemented procedures for reducing the likelihood that the information contained in the Certificate is not misleading;
- Maintaining 24x7 publicly accessible repositories with current information and replicates the relevant certificate information as well as CRLs;

- The Hardware Security Modules used by Signit for the generation and storage of CA private keys, and for subscriber private keys generated under the Signit-managed key-generation model, are Common Criteria certified. Cryptographic modules used under the applicant-generated key-pair model are provided by the applicant and meet the requirements of Section 6.1.1.2. Signit takes reasonable precautions to prevent any loss, disclosure or unauthorized use of the CA private keys. CA private keys are generated using a multi-person-control "m-of-n" split-knowledge scheme;
- Backing up of the CAs signing Private Keys 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 the Operations Policies and Procedures;
- Provide certificate and key management services in accordance with this CP/CPS; and
- Ensure that Signit personnel use private keys issued for the purpose of conducting CA duties only for such purposes

9.6.2. RA Representations and Warranties

Signit warrants that it performs RA functions as per the stipulations specified in this CP/CPS. This includes the defined registration activities performed by Reliable KYC Providers. Signit remains responsible for validating the information received from Reliable KYC Providers and for approving or rejecting certificate applications.

9.6.3. Subscriber Representations and Warranties

Subscribers of certificates issued under this CP/CPS shall:

- Provide accurate and complete information during registration and in any certificate request submitted to Signit;
- Use the certificate only for the purposes stated in Section 1.4.1 and in accordance with this CP/CPS and the applicable Subscriber Agreement;
- Protect the private key, its activation data, and any credentials used to access Signit certificate services against loss, disclosure and unauthorized use;
- Promptly request revocation where the private key is compromised or suspected of compromise, or where any information contained in the certificate is no longer accurate;
- Promptly notify Signit of any change to the entity's registered information, including its legal name, commercial registration details, Authorized Representative or Requester;
- Cease all use of the certificate upon its expiry or revocation.

For eSeal certificates issued under the applicant-generated key-pair model, the Subscriber is additionally responsible for generating and holding the key pair within a cryptographic module meeting the requirements of Section 6.1.1.2, and for notifying Signit without undue delay of any compromise or suspected compromise of that module.

For Natural Person short-term certificates, the private key is generated within Signit cryptographic module for the duration of a single signing session and is securely deleted at the end of that session. The obligations relating to private key protection and to requesting revocation therefore do not apply to these certificates. For such certificates, the Subscriber's obligations are limited to

providing accurate identity information, giving explicit consent through the approved channel, and using the certificate in accordance with the applicable Subscriber Agreement.

9.6.4. Relying Party Representations and Warranties

Relying Parties who rely upon the certificates issued under Signit 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 revoked by accessing current revocation status information available at the location specified in the certificate to be relied upon; and
- Determine that such certificate provides adequate assurances for its intended use.

9.6.5. Representations and Warranties of Other Participants

Reliable KYC Providers shall:

- Perform their registration activities in accordance with this CP/CPS and their agreement with Signit;
- Verify and authenticate Applicants using NAFATH;
- Ensure that the signed assertions and request information submitted to Signit are accurate, complete and authentic;
- Present the applicable Subscriber Agreement and obtain the Applicant's explicit acceptance of its terms and consent to certificate issuance and use;
- Protect subscriber information and the keys used to sign assertions against unauthorized access or use; and
- Promptly notify Signit of any error, suspected compromise or security incident affecting the registration information submitted to Signit.

9.7. Disclaimers Of Warranties

To the maximum extent permitted under the laws of the Kingdom of Saudi Arabia, and except in cases of fraud or deliberate misconduct, Signit shall not be held liable for:

- The accuracy, completeness, or correctness of information contained in a certificate where such information has been provided by the Subscriber, who remains solely responsible for the validity of all data submitted for inclusion in the certificate.
- Any indirect, consequential, or incidental damages arising from the use, non-use, issuance, revocation, or reliance on certificates or digital signatures.
- Any unlawful or improper actions performed by Subscribers, Relying Parties, or third-party participants, including violations related to intellectual property, malicious software, or unauthorized access to information systems.

- Service interruptions, delays, or failures resulting from circumstances beyond Signit reasonable control.

- Any misinterpretation or misuse of information contained in this CP/CPS or other publicly available documentation related to Signit services by Subscribers or Relying Parties.

9.8. Limitations of Liability

- Signit shall not be liable to Subscribers where any loss, damage, or claim results from the Subscriber's negligence, fraud, or wilful misconduct.
- Signit assumes no liability for the use of Certificates or associated Public-Key/Private-Key pairs for purposes other than those explicitly permitted under this CP/CPS and the applicable agreements.
- Signit shall not be liable for any direct or indirect damages resulting from service interruptions or events beyond its reasonable control.
- Relying Parties remain responsible for performing all required validation steps and shall bear the consequences of failing to meet their obligations under this CP/CPS.
- Subscribers remain fully responsible for the accuracy and legitimacy of all information provided for inclusion in a certificate, even after issuance.
- Except as required by applicable law, Signit does not accept financial or other liability for damages arising from the lawful operation of its Certification Authority services.

9.9. Indemnities

Not Applicable.

9.10. Term And Termination

9.10.1. Term

This CP/CPS is approved by Signit GB and shall remain in force until amendments are published on its public repository.

9.10.2. Termination

Amendments to this document are applied and approved by Signit GB and marked by an indicated new version of the document. Upon publishing on the public repository, the newer version becomes effective. The older versions of this document are archived on its repository.

9.10.3. Effect of Termination and Survival

Signit GB coordinates communications towards the relevant stakeholders in relation to the termination (and related effects) of this document.

9.11. Individual Notices and Communications with Participants

Notices related to this CP/CPS can be addressed to Signit GB contact address as stated in section 1.5.

9.12. Amendments

When changes are required to be done on this CP/CPS. Signit GB will incorporate any such change into a new version of this document and, upon approval, publish the new version. The new document will carry a new version number.

9.12.1. Procedure for Amendment

Refer to Section 9.12.

9.12.2. Notification Mechanism and Period

Upon publishing on Signit repository, the newer version of the CP/CPS becomes effective. The older versions of this document are archived on Signit public repository.

Signit GB coordinates communication in relation to the amendments of this CP/CPS and related effects.

Signit GB reserve the right to amend this CP/CPS without notification for amendments that are not material, including without limitation corrections of typographical errors or minor enhancements.

9.12.3. Circumstances under which OID Must Be Changed

Signit GB reserves the right to amend content of any published CP/CPS. Any major change of this CP/CPS will not alter the OID of the CP/CPS published in the public repository. The OID value corresponds to the current applicable and valid version for the CP/CPS.

9.13. Dispute Resolution Provisions

All disputes associated with the provisions of this CP/CPS and Signit services, shall be first addressed by Signit GB legal function. If mediation by Signit GB legal function is not successful, then the dispute shall be adjudicated by the relevant courts of Kingdom of Saudi Arabia.

9.14. Governing Law

The laws of the Kingdom of Saudi Arabia shall govern the enforceability, construction, interpretation, and validity of this CP/CPS.

9.15. Compliance with Applicable Law

This CP/CPS and the provision of Signit services comply with the relevant and applicable laws of the Kingdom of Saudi Arabia. Signit imposes no restrictions on potential end users. The services are provided on a non-discriminatory basis and are accessible to individuals with disabilities.

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 Signit CP/CPS or any of its rights or duties under this CP/CPS, without the prior written consent of Signit.

9.16.3. Severability

If any provision of this CP/CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP/CPS remains valid and enforceable. Each provision of this CP/CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4. Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5. Force Majeure

Signit shall not be liable for any failure or delay in their performance under the provisions of this CP/CPS due to causes that are beyond their reasonable control, including, but not limited to unavailability of interruption or delay in telecommunications services.

9.17. Other Provisions

No stipulation.