Timestamping Authority Policy and Practice Statement

Classification : Public

Version : 1.0

Date : 26 – July - 2026

Document Control

☐ Draft ☐ Final ☐ New Version ☒ Approved

Version	Action	Reviewer	Date	Notes
0.1	Initial Draft Version	Signit	03-Mar-2026	N/A
0.2	Review based on Auditor feedback and fixing typos	Signit	06-Jul-2026	N/A
0.3	Review and Sanity Check	Signit	22-Jul-2026	N/A
0.4	Legal Review and Sanity Check	Signit	23-Jul-2026	N/A
1.0	Approval	Signit	26-Jul-2026	N/A

Sign off

Role: Signit PKI Director

Name: Mohamed El Abbouri

Date: 26 – July - 2026

Signature:

Table Of Contents

1.Introduction

1.1. Overview

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:** The 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:

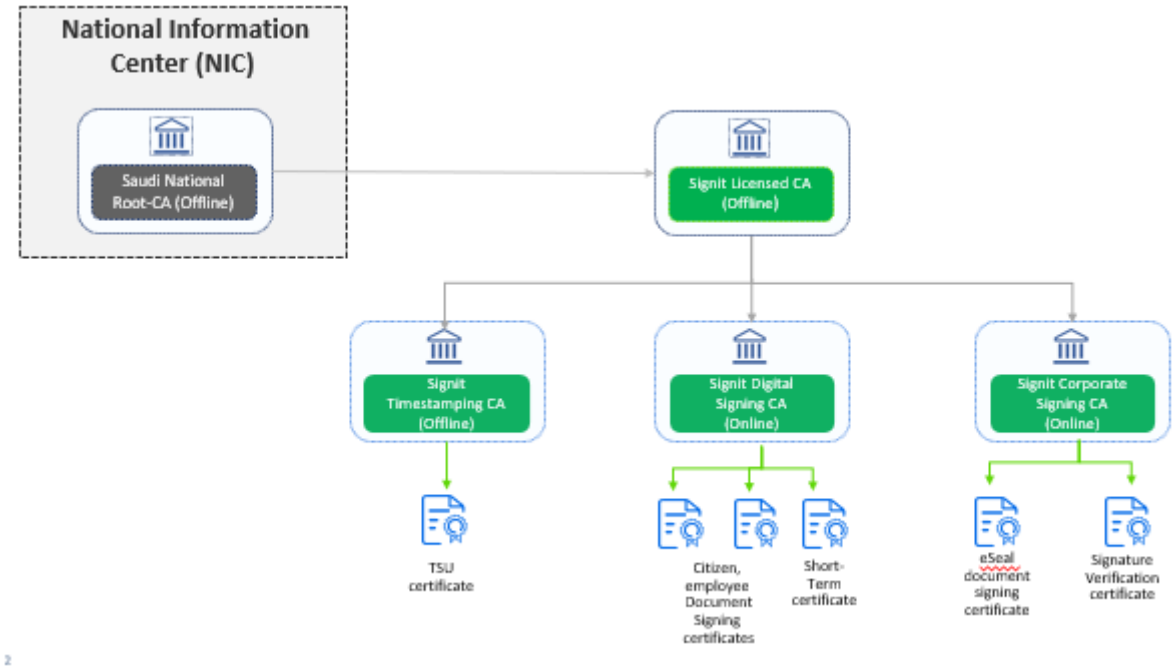

Figure 1 – Signit PKI hierarchy

As part of its trust services, Signit, acting as a Trust Service Provider (TSP), owns and operates a timestamping service branded as the “Signit Timestamping Authority Service” (the “Signit-TSA Service”).

Signit is fully responsible for the governance, operation, security, compliance, and provision of the Signit-TSA Service.

The Signit-TSA Service operates using a hybrid infrastructure model. Supporting timestamping applications and related services are hosted within Oracle Cloud Infrastructure (OCI), while cryptographic components, including the Timestamping Unit (TSU) signing keys and Hardware

Security Modules (HSMs), are hosted within Signit-controlled secure facilities. The TSU synchronizes with a trusted government-operated time source traceable to UTC, while cloud-hosted components synchronize using the OCI time service. Technical and operational controls ensure consistent and reliable time synchronization across both environments.

The Signit-TSA Service includes:

- operation of the Signit Timestamping Authority (Signit-TSA), the trust service responsible for issuing electronic Time-Stamp Tokens (TSTs);
- operation of one or more Timestamping Units (TSUs) responsible for generating and signing Time-Stamp Tokens in accordance with IETF RFC 3161;
- operation of the Timestamping Certification Authority (TSA CA) responsible for issuing, renewing, and revoking certificates for the TSUs;
- implementation and monitoring of trusted time synchronization mechanisms that ensure the time used for timestamp generation remains traceable to Coordinated Universal Time (UTC);
- maintenance of the security, logging, backup, monitoring, and audit controls supporting the secure operation of the timestamping service.

The present document, titled **"**Signit Timestamping Authority Policy and Practice Statement**"**, defines the policies, technical controls, and operational practices governing the Signit-TSA Service.

The timestamping service is implemented in accordance with applicable legal and regulatory requirements and recognized industry standards for timestamping services.

This document is administered and approved by the Signit GB and is made publicly available through the Signit repository.

1.2. Scope

This document specifies the policy, security requirements, and operational practices applicable to the Signit Timestamping Authority (Signit-TSA) for the issuance of electronic time-stamp tokens.
It defines:

- the rules and conditions governing the issuance of time-stamps;
- the obligations and responsibilities of Signit as the Trust Service Provider operating the TSA;
- the conditions of use applicable to requesters and relying parties; and
- the controls implemented to ensure the integrity and reliability of the timestamping service.

The Signit-TSA issues time-stamp tokens in accordance with IETF RFC 3161, binding a data hash to a specific point in time.

Time-stamps issued under this policy may be used to support electronic signatures, electronic seals, or to establish the existence and integrity of electronic data at a specific point in time, independently of any signature process.

This document may be used by independent parties to assess whether the Signit-TSA Service operates in accordance with applicable legal, regulatory, and industry requirements within the Kingdom of Saudi Arabia.

2. Definition and abbreviations

2.1. Definitions

Coordinated Universal Time (UTC) - time scale based on the second as defined in Recommendation ITU-RTF460-6.

Relying party - recipient of a time-stamp who relies on that time-stamp.

Re-Key - Certificate re-key refers to the issuance of a new certificate with a new subject public key for a subject to whom a certificate has previously been issued by the CA. Subject attributes and other certified attributes can be updated.

Subscriber - legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations.

Time-stamp - data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

Time-stamp token - data object defined in IETF RFC 3161 [1], representing a time-stamp
Time-stamp policy: named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements.

Time-Stamping Authority (TSA) - DTSP providing time-stamping services using one or more time-stamping units. In the context of this document, it is Signit.

Time-stamping service - trust service for issuing time-stamps. In the context of this documents, it is Signit – TSA.

Time-Stamping Unit (TSU) - set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.

TSA Disclosure statement - set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements.

TSA practice statement - statement of the practices that a TSA employs in issuing time-stamp.

TSA system - composition of IT products and components organized to support the provision of time-stamping services.

2.2. Abbreviations

For the purpose of the present document, the following abbreviations apply:

BIPM	Bureau International des Poids et Mesures
BTSP	Best practices Time-Stamp Policy
CA	Certification Authority
DTSP	Digital Trust Service Provider
GMT	Greenwich Mean Time
DGA	Digital Government Authority
NIC	National Information Center
IT	Information Technology
GB	Governance Board
TAI	International Atomic Time
TSA	Time-Stamping Authority
TSP	Trust Service Providers
TSU	Time-Stamping Unit
TST	Time Stamp Token
UTC	Coordinated Universal Time

3. General Concepts

3.1. Time-stamping services

The Signit-TSA Service consists of the issuance of electronic Time-Stamp Tokens (TSTs) generated using dedicated timestamping systems.

The service is operated by Signit, acting as a Timestamping Authority (TSA), and is made available to authorized requesters and relying parties.

The timestamping service is implemented in accordance with IETF RFC 3161 using HTTP-based transport mechanisms. Each Time-Stamp Token includes a time-stamping policy identifier that specifies the policy under which the timestamp was issued.

Signit is fully responsible for the provision of the timestamping service and for ensuring that the security, availability, accuracy, and performance requirements defined in this document are met.

The Signit-TSA Service operates using a hybrid infrastructure model. Timestamping application components are deployed within Oracle Cloud Infrastructure (OCI), while cryptographic components, including the Timestamping Units (TSUs) and their signing keys, are hosted within Signit-controlled secure facilities. Supporting cloud-hosted components synchronize using the OCI time service, while the TSUs synchronize with a government-operated time source that is traceable to Coordinated Universal Time (UTC).

The timestamping service is supported by:

- one or more Timestamping Units (TSUs) responsible for generating and signing Time-Stamp Tokens;
- dedicated TSU signing keys protected within Hardware Security Modules (HSMs);
- time synchronization mechanisms that continuously synchronize the TSUs with the government-operated time source, monitor clock drift, and ensure that the time used for timestamp generation remains traceable to Coordinated Universal Time (UTC);
- secure supporting infrastructure, systems, monitoring, and operational controls.

If reliable time synchronization cannot be maintained, timestamp issuance is suspended until the integrity of the time source is restored.

The Signit-TSA Service ensures the use of reliable time sources and appropriate protection of all system components involved in timestamp issuance.

3.2. Time Stamping Authority (TSA)

The Signit Timestamping Authority (Signit-TSA) is the trust service operated by Signit for issuing electronic time-stamp tokens.

Signit, acting as a Digital Trust Service Provider (DTSP), is the legal entity responsible for the governance, operation, security, and compliance of the Signit-TSA Service.

Time-Stamp Tokens are generated and cryptographically signed by dedicated Timestamping Units (TSUs) under Signit's operational control.

The system clocks used for timestamp issuance are synchronized with Coordinated Universal Time (UTC) through controlled and monitored time synchronization mechanisms aligned with trusted external time sources traceable to UTC.

Time synchronization is continuously monitored to detect clock drift. Acceptable time accuracy thresholds are defined internally, and procedures are in place for the detection, escalation, and handling of time-related incidents that could affect the integrity of the timestamping service.

If reliable time synchronization cannot be assured, timestamp issuance may be suspended until time integrity is restored.

3.3. Subscriber

A Subscriber is a natural or legal person that contracts with Signit for access to the Signit-TSA Service and submits time-stamp requests.

The Subscriber may be:

- an organization that uses the service directly or provides access to its employees or authorized users under its responsibility; or
- an individual end-user contracting directly with Signit.

Where the Subscriber is an organization, the organization is responsible for ensuring that its end-users comply with the obligations applicable under this document. The organization remains accountable for any failure of its end-users to comply with such obligations and shall ensure that its end-users are appropriately informed of the applicable terms and requirements.

Where the Subscriber is an individual end-user, the individual is directly responsible for compliance with the obligations defined in this document

3.4. Time-stamp policy and TSA practice statement

A Time-Stamp Policy is a formally defined and uniquely identified set of rules that specifies the applicability, security requirements, and assurance level associated with Time-Stamp Tokens issued under that policy. Each Time-Stamp Policy is identified by a unique object identifier (OID).

The TSA Practice Statement (TSA-PS) describes the operational practices, technical controls, and procedures implemented by the Signit Timestamping Authority (Signit-TSA) to meet the requirements defined in the applicable Time-Stamp Policy.

In the context of the Signit-TSA Service, the Time-Stamp Policy and the TSA Practice Statement are consolidated into this single document, which defines both the applicable policy requirements and the manner in which those requirements are implemented.

The relationship between the Time-Stamp Policy and the TSA Practice Statement follows a structured policy/practice model, whereby:

- the Time-Stamp Policy defines the applicable requirements and assurance objectives; and
- the TSA Practice Statement describes how those requirements are implemented, maintained, and enforced by the Signit-TSA.

Time-Stamp Tokens issued by the Signit-TSA include a reference to the applicable Time-Stamp Policy identifier under which they are generated.

4. Timestamp Policies

4.1. Overview

This Time-Stamp Policy defines the rules, requirements, and assurance level applicable to the issuance of Time-Stamp Tokens (TSTs) by the Signit Timestamping Authority (Signit-TSA).

The Signit-TSA signs Time-Stamp Tokens using dedicated private keys reserved exclusively for timestamping purposes. These private keys (TSU private keys) are generated, stored, and used within certified Hardware Security Modules (HSMs) and are never exported in plaintext form.

Each Time-Stamp Token includes the applicable Time-Stamp Policy Object identifier and reflects a time value synchronized with Coordinated Universal Time (UTC). The timestamping service is designed to maintain time accuracy within ±1 second relative to UTC.

Time-stamp requests are processed in accordance with IETF RFC 3161 using HTTP-based transport mechanisms.

4.2. Identification

The object identifier (OID) assigned to this Timestamping Policy and Practice Statement, which also serves as the Time-Stamp Policy identifier included in all Time-Stamp Tokens issued by the Signit-TSA, is: 2.16.682.1.101.5000.1.4.1.4.1.1.2

This OID is included in all Time-Stamp Tokens issued by the Signit-TSA and identifies the policy under which the timestamp was generated.

By including this OID in the issued Time-Stamp Tokens, the Signit-TSA indicates that the timestamp has been generated in accordance with the requirements defined in this document.

The URL of the Signit-TSA service is: https://tsa.pki.signit.sa/

This Time-Stamp Policy and Practice Statement document is publicly available to subscribers, requesters, and relying parties.

4.3. User Community and Applicability

The user community of the Signit-TSA Service includes:

- Subscribers or authorized requesters that submit time-stamp requests; and
- Relying parties that verify and rely upon the issued Time-Stamp Tokens.

Time-Stamp Tokens issued under this policy are intended to support high-assurance electronic signature and electronic seal use cases. However, they may be used by any application requiring reliable evidence that specific data existed at or before a given point in time.

5. Policies and Practices

5.1. Risk Assessment

Signit performs a formal risk assessment process applicable to the Signit-TSA Service in order to identify, evaluate, and manage risks affecting the confidentiality, integrity, availability, and reliability of the timestamping service.

An annual risk assessment is conducted covering all systems, processes, personnel, and assets supporting the Timestamping Service. The assessment:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of:
    - Time-Stamp Token (TST) data,
    - Timestamping Unit (TSU) private keys and certificates,
    - Time synchronization mechanisms and trusted time sources,
    - Supporting infrastructure and certificate management processes;
2. Assesses the likelihood and potential impact of identified threats, taking into account:
    - The sensitivity of timestamping operations,
    - The criticality of time accuracy and integrity,
    - The protection of cryptographic key material; and
3. Evaluates the adequacy and effectiveness of existing administrative, technical, physical, and organizational controls designed to mitigate identified risks.

Where risks exceed acceptable thresholds, mitigation measures are defined and implemented through a formal risk treatment plan. Risk treatment actions are tracked, reviewed, and approved under Signit's governance framework.

The risk assessment process is reviewed periodically and updated when significant changes occur to the operational environment, infrastructure, regulatory landscape, or threat profile. Evidence of risk assessments and associated treatment actions is retained for audit and compliance purposes.

5.2. Trust Service Practice Statement

Signit ensures the quality, security, availability, and proper operation of the Signit Timestamping Authority (Signit-TSA) Service through the implementation of documented policies, procedures, and security controls governing the provision of timestamping services.

These policies and controls are subject to regular review to ensure continued effectiveness and alignment with applicable regulatory and industry requirements. Periodic internal reviews are conducted to verify adherence to defined procedures, and independent external audits may be performed to assess the effectiveness of implemented controls.

The Signit GB, acting as the management authority, is responsible for maintaining, approving, and overseeing the policies and practices applicable to the Signit-TSA Service. This includes ensuring that the timestamping service operates in accordance with applicable trust service standards and internal governance requirements.

This Timestamping Authority Policy and Practice Statement, which also defines the applicable Time-Stamp Policy, together with other publicly available documents relevant to the Signit-TSA Service, is published in the Signit repository: https://repository.pki.signit.sa/

Operational documentation containing confidential or security-sensitive information is maintained under strictly controlled conditions and disclosed only where appropriate and authorized.

Signit provides appropriate notice of material changes to this Policy in accordance with its policy management and change control procedures.

5.3. Terms and Conditions

This section defines the terms and conditions applicable to the use of the Signit Timestamping Authority (Signit-TSA) Service. These provisions apply to all Subscribers and Relying Parties who request, receive, or rely upon Time-Stamp Tokens (TSTs) issued by Signit-TSA

5.3.1. Trust service policy applied

The Signit-TSA Service is operated in accordance with this Timestamping Authority Policy and Practice Statement (TSA-PPS).

Each Time-Stamp Token (TST) includes an Object identifier (OID) that uniquely identifies the policy under which the timestamp was issued. The inclusion of this identifier signifies that the timestamp has been generated in conformity with this TSA-PPS.

The Signit-TSA Service is designed and operated to meet the applicable requirements of IETF RFC 3161 and relevant regulatory requirements in the Kingdom of Saudi Arabia (KSA). This policy applies to all timestamps issued by Signit-TSA unless explicitly stated otherwise.

5.3.2. Timestamp format

The Signit-TSA accepts timestamp requests whose message imprint is computed using

- SHA-256,
- SHA-384 or
- SHA-512.

TimeStamp Tokens are signed using ECDSA P-384 with SHA-384. Requests using unsupported hash functions are rejected.

5.3.3. Accuracy of Time

The Signit Timestamping Authority (Signit-TSA) uses time that is traceable to Coordinated Universal Time (UTC) through one or more trusted time sources.

The Signit-TSA operates using a hybrid infrastructure model. Timestamping application components deployed within Oracle Cloud Infrastructure (OCI) synchronize using the OCI time service, while Timestamping Units (TSUs) and associated cryptographic components hosted within Signit-controlled secure facilities synchronize with a trusted government-operated time source traceable to Coordinated Universal Time (UTC).

Time synchronization mechanisms are configured to ensure consistency across all components involved in timestamp generation. Synchronization status is monitored, and defined operational thresholds are established to detect and manage time deviations.

Under normal operating conditions, the time used for timestamp generation achieves an accuracy of ±1 second or better relative to UTC.

If the integrity or accuracy of the time source cannot be assured within the defined thresholds, appropriate operational controls are applied to prevent the issuance of unreliable timestamps until normal operating conditions are restored.

Records relating to significant time synchronization events and adjustments are maintained in accordance with Signit's audit logging and retention requirements.

5.3.4. Verification of the Timestamp

5.3.4.1. Verification of timestamp Issuer

The Timestamping Unit (TSU) certificate and the corresponding certification path are published to enable Relying Parties to verify the origin and authenticity of issued Time-Stamp Tokens. Such information is made available through the public repository at: https://repository.pki.signit.sa

Relying Parties verify the authenticity of a Time-Stamp Token by:

- Validating the digital signature contained within the Time-Stamp Token in accordance with IETF RFC 3161;
- Using the public key contained in the applicable TSU certificate; and
- Validating the associated certification path up to a trusted Certification Authority.

Successful validation confirms that the Time-Stamp Token was generated and cryptographically signed by a TSU operated under the responsibility of the Signit Timestamping Authority (Signit-TSA).

5.3.4.2. Verification of timestamp revocation status

The revocation status of the Timestamping Unit (TSU) certificate used to sign a Time-Stamp Token may be verified using the Certificate Revocation List (CRL) and/or the Online Certificate Status Protocol (OCSP) services provided by the issuing Certification Authority.

Information necessary to obtain certificate status is identified in the CRL Distribution Point (CDP) and Authority Information Access (AIA) extensions of the TSU certificate.

Relying Parties are responsible for validating the revocation status of the TSU certificate in accordance with applicable standards at the time of verification. Such validation enables the Relying Party to determine whether the TSU certificate was valid at the time the Time-Stamp Token was generated.

The issuance, management, and revocation of TSU certificates are performed under Signit's Certification Authority governance framework and are distinct from the operational function of timestamp generation.

5.3.5. Service Availability

The Signit-TSA Service is designed and operated to provide high availability through the implementation of resilient infrastructure, redundancy, monitoring, and business continuity arrangements appropriate for a trusted timestamping service. These measures include, where applicable:

- Redundant system components to reduce single points of failure;
- Redundant network connectivity; and
- Protected power supply arrangements, including backup power mechanisms.

While these measures are intended to support continuous service operation, uninterrupted availability cannot be guaranteed. Service interruptions are monitored, recorded, and managed in accordance with documented incident management and business continuity procedures.

5.3.6. Subscriber Obligations

When obtaining a Time-Stamp Token (TST), the Subscriber shall:

- Submit timestamp requests in accordance with the HTTP-based Time-Stamp Protocol defined in IETF RFC 3161;
- Use methods, software, or toolkits that are technically compatible with the Signit-TSA Service;
- Verify the authenticity and integrity of each received Time-Stamp Token by validating the digital signature and associated certification path as described in Section 5.3.4 of this document; and
- Validate the revocation status of the applicable Timestamping Unit (TSU) certificate using the published CRL and/or OCSP services at the time of verification.

Subscribers are responsible for ensuring that timestamps are used in a manner consistent with this Policy and applicable legal or contractual requirements.

Subscribers are not required to assess the internal security controls of the Signit-TSA beyond the verification mechanisms defined in this document and applicable standards.

5.3.7. Relying party Obligations

When relying on a Time-Stamp Token (TST), a Relying Party shall:

1. Verify the authenticity and integrity of the Time-Stamp Token by validating the digital signature and associated certification path in accordance with Section 5.3.4 of this document and IETF RFC 3161;
2. Validate the revocation status of the applicable Timestamping Unit (TSU) certificate using the published Certificate Revocation List (CRL) and/or Online Certificate Status Protocol (OCSP) services to determine whether the TSU certificate was valid at the time of timestamp verification;
3. Consider any limitations, constraints, or intended usage conditions defined in this Timestamping Authority Policy and Practice Statement; and
4. Take any additional precautions appropriate to the specific transaction, legal context, or regulatory environment in which the timestamp is relied upon.

Failure to perform the above verification steps may affect the reliability of reliance placed upon the Time-Stamp Token.

5.3.8. Limitation of use of Service

The Signit Timestamping Authority (Signit-TSA) Service provides electronic Time-Stamp Tokens intended to establish reliable evidence that specific data existed at or before a particular point in time. The service is designed for lawful use in electronic transactions, record preservation, and other applications requiring time-based evidence.

The Signit-TSA does not review, validate, or assess the content, legality, accuracy, or appropriateness of the data submitted for timestamping. Responsibility for the content and lawful use of any Time-Stamp Token rests solely with the Subscriber or Relying Party.

Time-Stamp Tokens shall be used in accordance with this Timestamping Authority Policy and Practice Statement and applicable laws and regulations. Any use of a Time-Stamp Token that is inconsistent with this Policy or applicable legal requirements is outside the intended scope of the Signit-TSA Service.

To the maximum extent permitted under the laws of the Kingdom of Saudi Arabia, Signit shall not be liable for indirect, incidental, consequential, special, or punitive damages arising from or related to the use of, or reliance upon, the Signit-TSA Service, including but not limited to loss of profits, revenue, goodwill, business opportunity, or data.

Nothing in this section shall exclude or limit Signit's liability where such exclusion or limitation is prohibited by applicable law, or for damages resulting directly from fraud, willful misconduct, or material breach of this Timestamping Authority Policy and Practice Statement.

5.3.9. Retention Period

Signit retains records and data associated with the operation of the Signit Timestamping Authority (Signit-TSA) Service in accordance with applicable regulatory and legal requirements. Retained records include, where applicable:

- Timestamp requests;
- Issued Time-Stamp Tokens;
- Relevant audit logs; and
- Operational records necessary to demonstrate the integrity, authenticity, and proper functioning of the timestamping service.

Unless otherwise required by applicable law or supervisory authority, records related to timestamp issuance are retained for a minimum period of seven (07) years from the date of issuance.

Records relating to the issuance, management, and revocation of Timestamping Unit (TSU) certificates are maintained under Signit's Certification Authority governance framework and are subject to the retention requirements defined for Certification Authority operations.

Records are protected against unauthorized access, alteration, or destruction and are maintained in a manner that supports evidentiary integrity and audit verification.

5.3.10. Limitation of liability

The Signit-TSA Service is operated in accordance with this Timestamping Authority Policy and Practice Statement and applicable terms and conditions.

To the maximum extent permitted by the laws of the Kingdom of Saudi Arabia, Signit shall not be liable for indirect, incidental, consequential, special, or punitive damages arising out of or in connection with the use of, or reliance upon, the Signit-TSA Service.

Such limitation includes, without limitation, damages relating to:

- Loss of profits, revenue, or business opportunity;
- Loss or damage to reputation or goodwill;
- Loss of contracts or customers;
- Loss of use of, or damage to, software, data, systems, or equipment; or
- Losses arising under or in connection with third-party agreements.

Nothing in this section shall exclude or limit liability where such exclusion or limitation is prohibited by applicable law, or for damages resulting directly from fraud, willful misconduct, or material breach of this Timestamping Authority Policy and Practice Statement.

For the purposes of this section, the term “loss” includes partial loss, reduction in value, or complete loss.

5.3.11. Applicable Legal System, Complaint, Dispute Resolution

The laws of the Kingdom of Saudi Arabia shall govern the enforceability, construction, interpretation, and validity of the present document. All disputes associated with this document will be in all cases resolved according to the laws of the Kingdom of Saudi Arabia.

5.4. Information Security Policy

Signit maintains and enforces a documented information security policy applicable to all personnel, suppliers, and contractors involved in the operation and support of the Signit Timestamping Authority (Signit-TSA) Service.

The information security policy defines the principles, governance framework, and control objectives for protecting the confidentiality, integrity, and availability of information assets associated with the timestamping service. This includes systems, cryptographic components, time synchronization mechanisms, audit records, and supporting infrastructure.

The information security policy is aligned with Signit’s overall risk management framework and applicable regulatory and industry standards governing trust service providers.

The policy is reviewed at least annually and additionally whenever significant changes occur to the operational environment, threat landscape, infrastructure, or applicable regulatory requirements. Where necessary, controls are updated to address identified risks and ensure continued effectiveness.

5.5. TSA Obligations

5.5.1. General Obligations

The Signit Timestamping Authority (Signit-TSA) operates in conformity with the policies and procedures defined in this Timestamping Authority Policy and Practice Statement.

Compliance with applicable regulatory requirements and industry standards is subject to periodic internal review and, where applicable, independent external audit.

5.5.2. TSA Obligations toward Subscribers

In providing the timestamping service, the Signit-TSA shall:

1. Operate the service using appropriately secured, managed, and maintained systems and software suitable for trusted timestamp generation;
2. Perform timestamp issuance in accordance with this Timestamping Authority Policy and Practice Statement and applicable operational procedures;
3. Maintain time synchronization controls to support timestamp accuracy of ±1 second relative to UTC under normal operating conditions, as defined in Section 5.3.3;

4. Maintain qualified and appropriately trained personnel responsible for the secure and continuous operation of the timestamping service;
5. Conduct internal oversight and, where applicable, independent assessments to support ongoing compliance with legal, regulatory, and policy requirements; and
6. Monitor and manage the timestamping infrastructure to detect, prevent, and respond to operational disruptions, security incidents, or conditions that may affect the integrity or availability of the service.

5.6. Information for relying parties

Refer to section 5.3.7 for Relying Party Obligations.

6. TSA Management and Operations

6.1. Internal Organization

Signit operates and manages the Signit Timestamping Authority (Signit-TSA) under a formally established internal governance and operational structure designed to ensure compliance with applicable regulatory requirements and recognized industry standards.

Signit retains full responsibility and accountability for the provision, operation, security, and oversight of the Signit-TSA Service.

The internal organizational framework supporting the Signit-TSA ensures that:

- Roles and responsibilities relating to timestamping operations are formally defined, documented, and communicated across relevant operational, security, and compliance functions.
- Trusted roles are assigned to qualified personnel who have successfully completed background verification, role-specific training, and authorization procedures prior to assuming operational responsibilities.
- Separation of duties is enforced to prevent unauthorized or erroneous actions, and dual control is applied to critical TSA processes where required, including cryptographic key management and secure facility access.
- Governance oversight is performed by Signit management through established PKI governance structures, which provide supervisory control over TSA operations, security posture, compliance activities, and risk management.
- Security, operational, and compliance policies applicable to the TSA service are documented, approved, implemented, and subject to periodic review.

Signit maintains an active security management program applicable to the Signit-TSA Service. This program addresses, at minimum:

- Risk management and periodic risk assessment
- Logical and physical access control applicable to all environments supporting the Signit-TSA Service, including Signit-controlled facilities and cloud-hosted infrastructure.
- Incident detection and response
- Business continuity and disaster recovery
- Vulnerability management and security monitoring
- Ongoing personnel awareness and training

This internal organization enables Signit to operate a controlled, resilient, and well-governed timestamping service that supports the integrity, authenticity, and availability of issued Time-Stamp Tokens in accordance with this Timestamping Authority Policy and Practice Statement

6.2. Personnel Security

The Signit Timestamping Authority (Signit-TSA) is operated within a controlled organizational environment supported by formal personnel security measures designed to protect the confidentiality, integrity, and availability of the timestamping service.

Signit ensures that managerial, technical, and operational personnel involved in timestamping activities possess appropriate skills, knowledge, and experience relevant to their assigned responsibilities. Competence areas include, as applicable:

- Timestamping and trust service operations
- Cryptographic principles and key management
- Information security controls
- Risk management and incident response
- Regulatory and policy compliance

Signit defines Trusted Roles as positions involving access to, control over, or influence on sensitive systems, cryptographic material, or security-critical functions supporting the Signit-TSA Service. Trusted Roles include, but are not limited to:

- TSA Operators
- System Administrators
- Network Administrators
- Security Officers
- Cryptographic Key Custodians (including M-of-N custodians where applicable)
- Compliance personnel

For individuals assigned to Trusted Roles, Signit performs identity verification and background screening in accordance with established human resources procedures and applicable regulatory requirements. Identity verification is conducted using government-issued or otherwise recognized identification documents, and background checks are proportionate to the sensitivity of the assigned role.

Before being granted Trusted Role status, the following conditions must be satisfied:

- Formal authorization by designated management
- Completion of required training and acknowledgment of applicable security policies
- Provisioning of logical access strictly limited to assigned responsibilities
- Issuance of physical access credentials where access to secure facilities is required

Access to sensitive TSA systems, cryptographic components, and security-critical functions is:

- Role-based
- Restricted to authorized personnel
- Logged and monitored
- Subject to periodic review

Personnel security controls are reviewed in accordance with Signit's HR processes and Information Security Policy to ensure their continued effectiveness and alignment with operational risk, applicable legal and regulatory requirements, and recognized industry

standards. The applicable review processes and frequencies are defined within those internal policies and procedures.

These measures collectively support the secure and trustworthy operation of the Signit-TSA Service.

6.3. Asset Management

Signit maintains a comprehensive, accurate, and up-to-date inventory of information assets supporting the operation of the Signit Timestamping Authority (Signit-TSA) Service. Assets include information, hardware, software, cryptographic components, systems, and applications that support or may impact the provision of timestamping services.

Each asset is assigned an appropriate classification level based on its sensitivity, criticality, and business value, taking into account the results of periodic risk assessments. Asset classification determines the level of protection, access control, monitoring, handling, and lifecycle management applied.

Assets supporting the Signit-TSA Service include, but are not limited to:

- Timestamping application systems
- Hardware Security Modules (HSMs) and cryptographic devices
- Trusted time synchronization infrastructure
- System platforms and databases
- Network and security infrastructure
- Audit logging and monitoring systems

Signit operates a hybrid infrastructure model. Asset management controls apply across:

- Cloud-hosted PKI and TSA systems deployed within Oracle Cloud Infrastructure (OCI) in the Kingdom of Saudi Arabia; and
- Cryptographic components and related infrastructure hosted within Signit-controlled secure facilities.

For cloud-hosted environments, the underlying physical infrastructure is managed by the cloud service provider under its certified security framework. Signit retains responsibility for logical configuration, access governance, cryptographic asset management, and protection of timestamping-related systems deployed within that environment.

Changes to TSA-related systems, applications, or configurations are managed through documented change management procedures. These procedures ensure that:

- Changes are reviewed and risk-assessed prior to implementation;
- Security, integrity, and availability impacts are evaluated;
- Changes are approved by authorized personnel;

- Implementation activities are documented and traceable.

Where hardware components supporting the Signit-TSA Service are installed, replaced, or decommissioned, the following controls are applied:

- Delivery, transport, storage, and installation are conducted in a controlled and monitored manner to preserve integrity and traceability;
- Security and approval requirements equivalent to those applied during initial deployment are enforced;
- Only authorized and qualified personnel performing trusted roles are permitted to conduct hardware-related activities.

Asset management activities, including the asset inventory, asset classification, ownership, and lifecycle management, are reviewed in accordance with Signit's Asset Management Policy and related procedures, which form part of Signit's Information Security Policy framework. These policies and procedures define the applicable review process and frequency to ensure continued alignment with operational risk, applicable legal and regulatory requirements, and recognized industry standards.

These measures support the confidentiality, integrity, availability, and traceability of assets used in the provision of the Signit-TSA Service and contribute to the reliability and trustworthiness of issued Time-Stamp Tokens.

6.4. Access Control

Signit implements appropriate physical and logical access controls to protect facilities, systems, hardware, software, cryptographic components, and information supporting the Signit Timestamping Authority (Signit-TSA) Service.

Access to TSA-related systems and information is granted strictly on the basis of the principle of least privilege and is limited to authorized personnel whose access is necessary for the performance of assigned responsibilities. Logical access controls include:

- Strong authentication mechanisms;
- Role-based authorization;
- Access logging and monitoring;
- Periodic review of access rights; and
- Timely revocation of access when no longer required.

Access rights are reviewed at defined intervals and adjusted promptly in accordance with documented access management procedures.

Sensitive operational activities, including cryptographic operations and access to Hardware Security Modules (HSMs), are performed within highly restricted physical areas under controlled conditions. Physical access to secure facilities hosting cryptographic components is:

- Restricted to authorized personnel performing trusted roles;

- Logged and subject to periodic review;
- Enforced through layered physical protection mechanisms;
- Subject to dual control where required for security-critical activities.

Signit operates a hybrid infrastructure model. Access control measures apply across:

- Cloud-hosted TSA systems deployed within Oracle Cloud Infrastructure (OCI) in the Kingdom of Saudi Arabia; and
- Cryptographic and related infrastructure hosted within Signit-controlled secure facilities.

For cloud-hosted environments, the underlying physical security of data centers is managed by the cloud service provider under its certified security framework. Signit retains responsibility for logical access governance, identity and access management configuration, and administrative control of TSA systems deployed within the cloud environment.

Physical security controls within Signit-controlled facilities are designed to prevent unauthorized access, tampering, or compromise of TSA-related systems and cryptographic assets. These controls operate within defined security perimeters and support continuous monitoring appropriate to the criticality of the service.

Access control mechanisms are reviewed in accordance with Signit's Access Control Policy and related procedures, which form part of Signit's Information Security Policy framework. These policies and procedures define the applicable review process and review frequency to ensure continued alignment with operational risk, applicable legal and regulatory requirements, and recognized industry standards.

6.5. Cryptographic Controls

6.5.1. TSU Key Generation

The generation of Timestamping Unit (TSU) signing key(s) supporting the Signit Timestamping Authority (Signit-TSA) Service is performed within a physically secured environment under the operational control of Signit.

TSU key generation activities are conducted:

- By personnel assigned to trusted roles;
- Under dual control and separation of duties;
- Within secure facilities hosting cryptographic components;
- In accordance with documented key ceremony procedures.

Access to perform TSU key generation is strictly limited to authorized personnel whose responsibilities require such access. All key generation activities are logged and formally documented to ensure traceability and auditability.

TSU signing keys are generated, stored and used exclusively within Hardware Security Modules (HSMs) that comply with at least FIPS PUB 140-2 Level 3 or equivalent. The cryptographic module enforces:

- Protection of private keys against unauthorized disclosure;
- Controlled key usage;
- Tamper detection and response mechanisms;
- Secure key storage and lifecycle management.

TSU private keys are generated within the HSM and are not exported in plaintext form.

Time-Stamp Tokens are signed using cryptographic algorithms and key lengths approved by Signit for the Timestamping Service. The Signit-TSA currently supports ECDSA using NIST P-384 (secp384r1) keys with SHA-384 for signing Time-Stamp Tokens. The lifecycle management of TSU certificates and TSU key pairs is governed by the Signit CP/CPS.

These controls ensure that TSU key generation and management maintain the integrity, confidentiality, and trustworthiness required for secure timestamp issuance

6.5.2. TSU Private Key protection

Signit ensures that Timestamping Unit (TSU) private keys remain confidential and maintain their integrity throughout their lifecycle.

TSU private keys are generated, stored, and used exclusively within Hardware Security Modules (HSMs) that comply with FIPS 140-2 Level 3. The HSM enforces:

- Non-exportability of private keys in plaintext form;
- Protection against unauthorized disclosure or use;
- Role-based access control;
- Tamper detection and response mechanisms.

Access to HSMs and TSU private key usage functions is restricted to authorized personnel assigned to trusted roles. Such access is:

- Subject to dual control and separation of duties;
- Logged and monitored;
- Performed only within physically secured facilities under Signit control.

Where backup of TSU private keys is permitted under Signit key management procedures, key backup, storage, and recovery operations are performed:

- Within secure cryptographic modules or protected key storage mechanisms;
- Under dual control by personnel in trusted roles;
- In a physically secured environment;
- In accordance with documented key ceremony and key lifecycle procedures.

Personnel authorized to perform TSU private key management functions are strictly limited to those whose responsibilities require such access and who have been formally designated under Signit trusted role procedures.

These controls collectively ensure the confidentiality, integrity, and controlled use of TSU private keys supporting the Signit-TSA Service.

If a TSU private key is suspected or confirmed to be compromised, its use for issuing Time-Stamp Tokens shall cease immediately. The corresponding TSU certificate shall be revoked, a replacement TSU key pair shall be generated in accordance with the documented key generation procedures, and timestamp issuance shall resume only after the new TSU certificate has been issued and activated. All such events shall be managed in accordance with Signit's incident management and key compromise procedures.

6.5.3. TSU Public Key Certificate

Signit ensures that the information required by Relying Parties to verify the integrity and authenticity of Time-Stamp Tokens is made publicly available.

The Timestamping Unit (TSU) public key certificate used to verify signatures on Time-Stamp Tokens is issued under the Signit PKI and is managed in accordance with Signit's applicable certification policies and practices.

The TSU certificate, together with the associated certification path information necessary to perform signature and certificate validation, is published in a publicly accessible repository to enable Relying Parties to validate issued Time-Stamp Tokens.

The repository is available at: https://repository.pki.signit.sa/

Signit remains responsible for ensuring that TSU certificate information published for verification purposes is current, valid, and updated without undue delay, including following issuance, re-key, or revocation events.

6.5.4. Rekeying TSU's Key

The operational lifetime of Timestamping Unit (TSU) key pairs is controlled through defined key usage and certificate validity parameters.

TSU public key certificates are issued with a maximum validity period of three (3) years. However, the associated TSU private key is used for signing Time-Stamp Tokens (TSTs) only during a defined operational usage period not exceeding one (1) year.

Upon expiration of the defined operational usage period, a new TSU key pair is generated in accordance with the documented key generation procedures, and a new TSU certificate is issued under the Signit PKI hierarchy. The previous TSU key is retired from active signing operations.

The limitation of the operational signing period reduces long-term cryptographic exposure while allowing previously issued Time-Stamp Tokens to remain verifiable throughout the validity period of the corresponding TSU certificate.

Upon expiration of a TSU signing key, the TSU private key shall no longer be used to issue Time-Stamp Tokens and will be securely destroyed or permanently rendered unusable in accordance with Signit's documented key ceremony procedures. Previously issued Time-Stamp Tokens remain verifiable using the corresponding TSU public key certificate and the associated certification path information.

Rekeying activities are performed under dual control by personnel assigned to trusted roles and are formally documented to ensure traceability and auditability.

6.5.5. Life Cycle Management of Signing Cryptographic Hardware

Signit ensures that the lifecycle of cryptographic modules used for Timestamping Unit (TSU) signing operations is securely managed to preserve the confidentiality, integrity, and controlled use of cryptographic keys.

With respect to cryptographic hardware security modules (HSMs) supporting the Signit-TSA Service:

- The integrity of cryptographic modules is verified upon receipt from the manufacturer, including validation of tamper-evident packaging and delivery documentation.

- Cryptographic modules are stored in controlled and physically secured environments prior to installation, ensuring protection against unauthorized access or tampering.

- Installation, initialization, configuration, and operational management of cryptographic modules are performed only by personnel assigned to trusted roles, under dual control and within physically secured facilities.

- Cryptographic modules are operated and maintained in accordance with manufacturer guidance and documented internal procedures to ensure continued correct functioning and security.

- When a cryptographic module is decommissioned, taken out of service, or removed from production use, all TSU private signing keys and sensitive cryptographic material stored within the module are securely destroyed or permanently rendered unusable in accordance with documented key destruction procedures.

Decommissioning and destruction activities are formally documented and performed under controlled conditions to ensure traceability and compliance with applicable regulatory and security requirements.

6.5.6. End of TSU Key Life Cycle

The operational lifetime of a Timestamping Unit (TSU) private key shall not exceed the validity period of its corresponding TSU public key certificate and shall be subject to the defined key usage period specified in the policy and certificate practice statement (CP/CPS).

Upon expiration of the defined signing usage period, the TSU private key shall no longer be used to issue new Time-Stamp Tokens.

Following expiration or revocation of the TSU certificate, and once it has been determined that the associated private key is no longer required for operational, verification, or audit purposes, the TSU private key is securely destroyed within the cryptographic module in accordance with documented key destruction procedures. Destruction ensures that the private key cannot be recovered, reconstructed, or reused.

TSU key lifecycle operations, including key activation, deactivation, and destruction, are:

- Performed by personnel assigned to trusted roles;
- Executed under dual control where required;
- Conducted within secure facilities;
- Logged and formally documented to ensure traceability.

Documented operational procedures ensure that new TSU key pairs are generated, certified, and activated prior to the expiration of an existing TSU key in order to maintain continuity of the Signit-TSA Service without service interruption.

These measures ensure secure and controlled termination of TSU keys while preserving the integrity and reliability of previously issued Time-Stamp Tokens.

6.6. Timestamping

6.6.1. Time-stamp issuance

The Signit Timestamping Authority (Signit-TSA) issues electronic Time-Stamp Tokens (TSTs) in a secure, reliable, and controlled manner. Technical and operational controls are implemented to ensure that TSTs are generated correctly and include accurate, verifiable, and trustworthy time information.

Time-Stamp Tokens are issued in accordance with the time-stamping protocol specified in this document (IETF RFC 3161). Each TST includes, at a minimum:

- A representation (i.e., a hash value) of the data submitted for timestamping, as provided by the requester;
- A unique serial number enabling identification of the specific Time-Stamp Token;
- An identifier of the applicable time-stamping policy (OID);
- The time of issuance, maintained with an accuracy of ±1 second or better relative to Coordinated Universal Time (UTC);
- An electronic signature generated using a TSU private key dedicated exclusively to timestamping operations;
- Identifiers enabling unambiguous determination of the issuing Timestamping Authority (TSA) and Timestamping Unit (TSU);
- Where a nonce is included in the timestamp request, the same nonce value included unchanged in the corresponding TST.

The Signit-TSA ensures that Time-Stamp Tokens are generated only while the corresponding TSU private key remains within its defined operational usage period and the associated TSU certificate is valid. No Time-Stamp Tokens are issued after the TSU private key has been deactivated or retired from service, or after the associated TSU certificate has expired or been revoked.

Audit records relating to timestamp issuance, key usage, and time synchronization are maintained in accordance with documented logging and archival procedures to support verification of the integrity and accuracy of the timestamping service.

6.6.2. Clock Synchronization with UTC

The time used for the issuance of electronic Time-Stamp Tokens by the Signit Timestamping Authority (Signit-TSA) is traceable to Coordinated Universal Time (UTC) and is maintained with an accuracy of ±1 second or better under normal operating conditions.

Signit operates a hybrid infrastructure model. Time synchronization mechanisms are implemented across both:

- Cloud-hosted TSA systems deployed within Oracle Cloud Infrastructure (OCI); and
- Cryptographic components and related infrastructure hosted within Signit-controlled secure facilities.

Systems deployed within Oracle Cloud Infrastructure (OCI) synchronize using the OCI time service, which provides time synchronization for the cloud-hosted components supporting the Signit-TSA Service.

Cryptographic components, including the Timestamping Units (TSUs), synchronize with a trusted government-operated time source that is traceable to Coordinated Universal Time

(UTC). The trusted time used for the generation of Time-Stamp Tokens is derived from this government-operated time source.

Time synchronization mechanisms are configured and monitored to ensure consistent and reliable synchronization across the cloud-hosted and on-premises environments supporting the Signit-TSA Service.

Technical and operational controls are implemented to:

- Monitor clock drift and synchronization status;
- Detect deviations outside defined accuracy thresholds;
- Initiate corrective actions where synchronization deviates from the defined operational thresholds.

If the TSU clock deviates outside the declared accuracy limits, issuance of Time-Stamp Tokens is automatically suspended until correct synchronization is restored.

Leap second adjustments are handled in accordance with established time synchronization procedures and authoritative UTC notifications to ensure continuity and correctness of timestamp issuance.

Audit records relating to time synchronization, monitoring activities, detected deviations, suspension events (if any), and corrective actions are maintained in accordance with documented logging and archival procedures. These records support verification of the accuracy, integrity, and reliability of the Signit-TSA Service.

7. Physical and Environmental Security

The Signit Timestamping Authority (Signit-TSA) operates within a hybrid infrastructure model combining:

- Cryptographic components hosted within Signit-controlled secure on-premises facilities in the Kingdom of Saudi Arabia; and
- Supporting PKI and timestamping application systems hosted within Oracle Cloud Infrastructure (OCI) regions located in the Kingdom of Saudi Arabia.

Signit retains full responsibility and accountability for ensuring that physical and environmental security controls applied to all infrastructure supporting the Signit-TSA Service are adequate, effective, and consistent with this Timestamping Authority Policy and Practice Statement.

7.1. Site Location and Construction

Cryptographic components, including Hardware Security Modules (HSMs) used for TSU key storage and signing operations, are deployed within secure data center facilities located in the Kingdom of Saudi Arabia under Signit operational control.

These facilities are designed to host high-value and sensitive cryptographic infrastructure and implement layered physical protection mechanisms, including:

- Restricted security perimeters;
- Manned guarding and monitoring;
- Intrusion detection systems;
- Continuous CCTV surveillance;
- Controlled secure cages or racks dedicated to Signit equipment.

Supporting timestamping application systems hosted within OCI are deployed in enterprise-grade cloud data centers located in Saudi Arabia. Physical construction and facility controls for cloud environments are managed by the cloud infrastructure provider under internationally recognized certifications (e.g., ISO/IEC 27001, SOC 2 Type II).

7.2. Physical Access

Physical access to Signit-controlled secure facilities hosting cryptographic components is restricted exclusively to authorized personnel assigned to Trusted Roles.

The following controls apply within Signit-controlled environments:

- Multi-layer access control mechanisms (including biometric controls where applicable);
- Dual control requirements for access to inner secure areas hosting HSMs and cryptographic components;
- Logging and periodic review of physical access events;
- Escort requirements for visitors or non-trusted individuals.

For cloud-hosted systems, physical access controls are implemented and managed by the cloud infrastructure provider. Signit maintains logical governance and administrative access control over PKI and TSA systems deployed within the cloud environment.

7.3. Power And Air Conditioning

Within Signit-controlled facilities:

- Power supply is protected by uninterruptible power supply (UPS) systems and backup generators;
- Environmental conditions (temperature and humidity) are maintained within manufacturer-recommended operating ranges for cryptographic and supporting infrastructure.

Cloud-hosted systems rely on the resilience and environmental controls implemented by the infrastructure provider within Saudi-based regions.

Systems are designed to support controlled shutdown procedures in the event of sustained power or environmental failure.

.

7.4. Water Exposures

Signit implements reasonable precautions within its secure facilities to minimize risks associated with water exposure, including infrastructure positioning and environmental monitoring.

For cloud-hosted infrastructure, environmental protection measures are managed by the cloud provider as part of its certified facility operations.

7.5. Fire Prevention and Protection

Signit-controlled facilities implement fire detection and suppression systems in accordance with applicable safety regulations in the Kingdom of Saudi Arabia.

Cloud-hosted systems rely on fire detection and suppression mechanisms implemented by the infrastructure provider within certified Saudi-based facilities.

7.6. Media Storage

Removable media, backup media, and sensitive documentation associated with the Signit-TSA Service are stored within secure facilities under controlled access conditions.

Media containing sensitive or confidential information are:

- Protected against unauthorized access;
- Stored in secure cabinets or controlled areas;
- Replicated and stored at geographically separate disaster recovery locations where required.

For cloud-hosted systems, physical storage protection is managed by the infrastructure provider, while Signit remains responsible for logical access control and data protection.

.

7.7. Waste Disposal

Media and documentation containing sensitive information are securely destroyed prior to disposal using approved destruction methods (e.g., secure wiping, shredding, or physical destruction), depending on media type and sensitivity.

Cryptographic hardware, including HSMs, is decommissioned using controlled procedures ensuring that private keys and sensitive information are permanently destroyed or rendered unrecoverable.

7.8. Off-Site Backup

Critical system data, configuration information, and audit logs supporting the Signit-TSA Service are backed up periodically in accordance with documented backup and disaster recovery procedures.

Backup copies containing sensitive information are:

- Stored in secure locations with equivalent protection measures;
- Geographically separated within the Kingdom of Saudi Arabia;
- Protected against unauthorized access and tampering.

Cloud infrastructure supports secure replication capabilities, while Signit defines and governs backup policies and access controls.

7.9. Operation Security

Operational security controls are implemented to ensure integrity, availability, and resilience of the Signit-TSA Service. These include:

- Security requirements analysis during system design;
- Documented change management procedures;
- Malware protection and system hardening controls;
- Segregation of duties for trusted and administrative roles;
- Secure media handling procedures;
- Vulnerability management processes aligned with documented risk assessment activities.

Vulnerability assessments and penetration testing are performed periodically in accordance with documented security governance processes, covering both cloud-hosted and on-premises environments under Signit operational control.

7.10. Network Security

Signit implements layered network security controls to protect the Signit-TSA Service and supporting systems across both cloud-hosted and on-premises environments.

Network traffic is filtered through managed firewall infrastructure 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 timestamping systems communicate only where strictly necessary.

Communication between systems supporting the Signit-TSA Service is restricted through defined network boundaries. Only approved services, protocols, ports, and communication paths required for secure timestamp issuance and related 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:

- Cloud-hosted timestamping application components;
- On-premises cryptographic infrastructure, including HSM-connected systems; and
- Trusted time synchronization services.

Administrative access to TSA and PKI systems is permitted only through controlled network entry points using authenticated and encrypted connections. Critical components, including TSU signing systems, certificate validation services, HSM-connected systems, and time synchronization infrastructure, operate within restricted and monitored network zones.

Network activity is logged and subject to continuous monitoring to detect unauthorized, anomalous, or malicious behavior. Detected events are handled in accordance with Signit's documented incident management procedures.

These controls collectively support the confidentiality, integrity, and availability of the Signit-TSA Service.

7.11. Incident Management

Signit maintains a documented incident management process to ensure timely detection, response, and containment of security incidents.

The process includes:

- Incident identification and classification;
- Coordinated response and containment actions;
- Internal escalation and management oversight;
- Monitoring and review of TSA audit logs;
- Notification of affected Subscribers where legally required and where impact is identified.

Monitoring activities are performed by personnel assigned to Trusted Roles under controlled access conditions.

7.12. Collection of evidence

All information relevant to the operation of the Signit-TSA Service is recorded and retained to support auditability, evidentiary requirements, and service continuity.

Records include:

- Time-stamp requests received and Time-Stamp Tokens issued;
- Events relating to TSU key lifecycle and certificate management;
- Clock synchronization events and detected deviations;
- Security and environmental events affecting TSA operations.

Records are:

- Maintained with precise time information synchronized with UTC;
- Archived in a secure and integrity-protected manner;
- Retained beyond TSU key expiration where required to support legal or regulatory obligations.

7.13. Business continuity management

Signit maintains documented Business Continuity and Disaster Recovery Plans covering both cloud-hosted systems and on-premises cryptographic components.

If:

- A TSU private key is compromised or suspected to be compromised; or
- Time synchronization accuracy falls outside declared thresholds.

the Signit-TSA Service:

- Immediately suspends affected operations;
- Initiates incident response procedures;
- Performs recovery actions in accordance with documented continuity plans.
- Where revocation of a TSU certificate is required, such revocation is performed in accordance with the applicable Policy and Certification Practice Statement (CP/CPS).

7.14. TSA Termination and Termination Plans

Signit maintains a documented termination plan to minimize disruption in the event of cessation of the Signit-TSA Service.

The termination plan includes:

- Notification to Subscribers and relevant relying parties;
- Controlled revocation of active TSU certificates where required;
- Secure destruction or withdrawal from use of TSU private keys and backup copies;
- Preservation and protection of archived records in accordance with retention requirements.

8. Compliance

The Signit Timestamping Authority (Signit-TSA) operates in accordance with applicable laws and regulations of the Kingdom of Saudi Arabia and follows recognized technical standards and industry best practices applicable to electronic timestamping services.

The Signit-TSA Service is implemented in accordance with IETF RFC 3161 (Time-Stamp Protocol) and related cryptographic and information security standards governing the secure generation and management of digital signatures and cryptographic keys.

Signit maintains documented policies, procedures, and operational controls supporting the timestamping service. These controls are subject to periodic review to ensure continued effectiveness, appropriateness, and alignment with evolving security risks and operational requirements.

Compliance with applicable legal and technical requirements is reviewed at least annually through structured internal governance processes and independent assessments, where appropriate.

Signit maintains documentation and operational evidence necessary to demonstrate conformity with this Timestamping Authority Policy and Practice Statement.

— End of Document —