TIMESTAMPING AUTHORITY POLICY AND PRACTICE STATEMENT

Document Classification:

Public

Version Number: 1.0

Issue Date: 08 Feb 2026

Document Reference

Item	Description
Document Title:	Timestamping Authority Policy and Practice Statement
Custodian Department:	sirar's Product Management
Owner:	sirar's Policy Authority
Version Number:	1.0
Document Status:	Final

Document Author:	sirar's Policy Authority	
	PKI Consultant	Signature/Date
Document Reviewer:	Thaar F. AlOtaibi	Thaar alotaibi
	Managed Security Services General Manager	Signature/Date
Approved by:	Aiman H. AlJumoay	Aiman Aljumoay
	Chief Managed Services Officer	Signature/Date

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	08/02/2026	sirar's Policy Authority	- Final incorporating reviews

Document Control

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

The Digitally Signed Copy of this document shall be stored at the sirar's PKI Repository.

Table of Contents

1. INTRODUCTION

1.1 OVERVIEW

The Government of Saudi Arabia has embarked on an ambitious e-transaction program, recognizing that there is a tremendous opportunity to better utilize information technology to improve the quality of care/service, lower the cost of operations, and increase customer satisfaction. To ensure the secure, efficient transmission and exchange of information electronically, the Kingdom of Saudi Arabia has established the "Saudi National PKI" that consists of:

- Shared National PKI Center at National Information Center (NIC-PKIC) hosts and operates the Saudi National Root CA and the Government CA,
- The regulator of Digital Trust Services in the Kingdom of Saudi Arabia being the Digital Government Authority (DGA),
- Commercial Certification Authorities (CAs) owned and operated by Digital Trust Service Providers (DTSPs) that are expressly approved by NIC.

Sirar, a subsidiary of the Saudi Telecommunications Company (STC) is an approved DTSP under the Saudi National PKI. Sirar has established its own PKI infrastructure offering digital trust services designed to enable electronic signature and authentication services for business entities and individuals.

As part of its PKI services, sirar owns and provides a timestamping service branded as the "sirar Timestamping Authority Service", hereinafter "SIRAR-TSA Service". sirar retains overall responsibility and accountability for the governance, compliance, and provision of the SIRAR-TSA Service.

The present document, titled "Timestamping Authority Policy and Practice Statement", describes the policies, controls, and operational practices applicable to the SIRAR-TSA Service and adopted by sirar as the accountable DTSP, in accordance with applicable regulatory and industry requirements.

The timestamping service has been implemented to satisfy, where applicable, the **IETF RFC 3161 – Internet X.509 Public Key Infrastructure Time-Stamp Protocol**.

The structure and content of this document are aligned with recognized policy and security practices for timestamping services.

This document is administered and approved by sirar's PKI Committee and shall be read in conjunction with the sirar Timestamping CA Certification Practice Statement (CPS), which governs the issuance, management, and revocation of TSU certificates. The applicable policy and practice documents are publicly available through the respective repository of sirar.

1.2 SCOPE

This document specifies the policy, security requirements, and operational practices applicable to the sirar Timestamping Authority (SIRAR-TSA) for the issuance of electronic timestamps. It also defines the conditions of use, obligations, and responsibilities of the parties involved in the provision and use of the SIRAR-TSA Service.

sirar provides reliable, standards-based electronic timestamps by operating and controlling a Timestamping Unit (TSU) and by relying on trusted time sources. These timestamps support electronic signatures and electronic seals by establishing that specific data existed at or before

a particular point in time. A document may be signed without being timestamped, and conversely, it may be timestamped without the presence of a signatory's signature, for example, to establish the existence and integrity of electronic data at a specific point in time prior to any formal signing process.

This document may be used by independent parties as a basis for assessing whether the SIRAR-TSA Service is operated in accordance with applicable regulatory and industry requirements, including the relevant regulations and requirements in the Kingdom of Saudi Arabia (KSA).

2. DEFINITION AND ABBREVIATIONS

2.1 DEFINITIONS

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-RTF.460-6.

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

sirar: a subsidiary of the Saudi Telecommunications Company (STC) is an approved DTSP under the Saudi National PKI. Sirar has established its own PKI infrastructure offering digital trust services designed to enable electronic signature and authentication services for business entities and individuals.

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.

Time-stamping service: trust service for issuing time-stamps.

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:

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
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 SIRAR-TSA Service consists of the provision of electronic Time-Stamp Tokens (TSTs) generated using dedicated timestamping systems. The service is provided by sirar, acting as a Timestamping Authority (TSA), to Subscribers and Relying Parties.

The timestamping service is implemented using the IETF RFC 3161 Time-Stamp Protocol over HTTP transport. Each Time-Stamp Token includes a time-stamping policy identifier indicating the policy under which the timestamp was issued.

sirar retains overall responsibility and accountability 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 SIRAR-TSA Service ensures the use of reliable and trusted time sources and the appropriate management and protection of all system components involved in the timestamping process, under sirar's governance and oversight.

3.2 TIME STAMPING AUTHORITY (TSA)

The sirar Timestamping Authority (SIRAR-TSA) is responsible for the provision of the timestamping services described in this document. sirar, acting as a Digital Trust Service Provider (DTSP), is the legal entity that owns the SIRAR-TSA Service and remains fully accountable for its governance, security, and compliance.

sirar ensures that the system clocks used for timestamp issuance are synchronized with Coordinated Universal Time (UTC). The TSU systems synchronize their time through sirar's centralized time distribution infrastructure based on Microsoft Active Directory (AD), which is in turn synchronized with one or more trusted external time sources traceable to UTC. Time synchronization is performed at regular intervals and at least once every twenty-four (24) hours. sirar defines acceptable time accuracy thresholds1 and maintains oversight of time synchronization activities, including the detection, escalation, and handling of any time-related incidents affecting the SIRAR-TSA Service.

3.3 SUBSCRIBER

The Subscriber is the applicant, natural or legal person, to whom the time stamp is provided and who is contracted with sirar.

The Subscriber may be an organization comprising several end-users or an individual end-user. When the Subscriber is an organization, some of the obligations that apply to that organization will have to apply as well to the end-users. In any case, the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organization shall duly notify its end-users.

When the Subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

[1] the maximum allowed deviation between the time stated in the timestamp token and Coordinated Universal Time (UTC)

3.4 TIME-STAMP POLICY AND TSA PRACTICE STATEMENT

A Time-Stamp Policy (TSP) is a formally defined and uniquely identified set of rules that specifies the applicability of Time-Stamp Tokens to a particular community and/or to a defined class of applications with common security requirements.

The TSA Practice Statement (TSA-PS) describes the operational practices, controls, and procedures implemented by the Time-Stamping Authority (TSA) in support of the issuance and management of Time-Stamp Tokens in accordance with the applicable Time-Stamp Policy.

The relationship between the Time-Stamp Policy and the TSA Practice Statement follows the established Certificate Policy (CP) and Certification Practice Statement (CPS) model, whereby the policy defines the applicable requirements and assurance levels, and the practice statement specifies how those requirements are implemented and enforced by the TSA.

4. TIMESTAMP POLICIES

4.1 OVERVIEW

This policy defines a set of rules adhered to by SIRAR-TSA when issuing Timestamps.

SIRAR-TSA signs timestamps using private keys that are specifically reserved for this purpose. The timestamps signature private keys (i.e., TSUs private keys) are stored in a cryptographic device (HSM).

Each TST (Time Stamp Token) shall contain an identifier to the applicable policy and the TSTs shall be issued with an accuracy of ± 1 second of UTC.

The time-stamps shall be requested through Hypertext Transfer Protocol (HTTP), as described by the RFC 3161.

4.2 IDENTIFICATION

The identifier of the Time-Stamp Policy, specified in this document is: 2.16.682.1.101.5000.1.4.1.2.2.1, This OID is referenced in all timestamps issued by the SIRAR-TSA, and this policy is available to all the subscribers and relying parties.

By including this object identifier in the generated time-stamps, sirar claims conformance with this time-stamp policy.

The URL for the SIRAR-TSA service is: https://sirar.com.sa/repository/

4.3 USER COMMUNITY AND APPLICABILITY

The user community for SIRAR-TSA Time-Stamp services includes subscribers and relying parties. Accordingly, Subscribers are also regarded as Relying Parties.

The TSP and TSA-PS are intended to support the issuance of Time-Stamp Tokens that meet the requirements applicable to high-assurance electronic signatures. Notwithstanding the foregoing, SIRAR-TSA Time-Stamp Tokens may be used by any application that requires reliable evidence that a given datum existed prior to a specific point in time.

5. POLICIES AND PRACTICES

5.1 RISK ASSESSMENT

sirar conducts an annual risk assessment covering all systems, processes, and assets supporting the Timestamping Service. This assessment:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Time-Stamp Token data, Time-Stamp Unit (TSU) certificate data, or related certificate management processes,
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Time-Stamp Token operations and TSU certificate management; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that are in place to counter such threats.

The resulting remediation plan incorporates administrative, organizational, technical, and physical measures appropriate to the sensitivity of the timestamping environment. It also considers the availability and cost of applicable technologies, ensuring that the level of security implemented is proportionate to the potential harm from a security breach and the nature of the data and assets being protected.

5.2 TRUST SERVICE PRACTICE STATEMENT

sirar ensures the quality, security, availability, and proper operation of the SIRAR-TSA Service through the implementation of documented policies, procedures, and security controls applicable to the provision of timestamping services.

These policies and controls are subject to regular review. Independent audits may be performed to assess the effectiveness of the implemented controls and trained and authorized personnel periodically verify adherence to the defined policies and procedures to ensure that the timestamping service is operated as intended.

The sirar PKI committee, as the management authority, is responsible for maintaining, approving, and overseeing the policies and practices applicable to the SIRAR-TSA Service, to ensure that the timestamping service is operated as intended.

This Timestamping Authority Policy and Practice Statement, together with other applicable publicly available documents related to the SIRAR-TSA Service, are published in the sirar's repository at: https://sirar.com.sa/repository/.

The Certification Practice Statement (CPS) applicable to the Timestamping CA (TSCA) is published at sirar's repository. That CPS governs certificate issuance (including Time-Stamping Units (TSUs)) and related certificate lifecycle management activities that fall outside the scope of this Time-Stamp Policy and TSA Practice Statement.

Internal or confidential operational documents are disclosed only under strictly controlled conditions. sirar provides appropriate notice of material changes to this Policy in accordance with its policy management procedures.

5.3 TERMS AND CONDITIONS

This section outlines the Terms and Conditions applicable to the use of the SIRAR-TSA services.

These provisions apply to all subscribers and relying parties who interact with or rely upon timestamps issued by SIRAR-TSA.

5.3.1 TRUST SERVICE POLICY APPLIED

The SIRAR-TSA Service is operated in accordance with the Timestamping Authority Policy and Practice Statement (TSA-PPS) defined in this document. This TSA-PPS specifies the policies, controls, and operational practices applicable to the issuance of electronic timestamps by sirar.

Each Time-Stamp Token (TST) issued by the SIRAR-TSA includes a time-stamping policy identifier that uniquely identifies the timestamping policy under which the timestamp was generated. The presence of this policy identifier indicates that the timestamp has been issued in accordance with the requirements defined in this TSA-PPS.

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

5.3.2 TIMESTAMP FORMAT

The SIRAR-TSA service issues Timestamps signed using one of the following digest algorithms:

- SHA-256
- SHA-384
- SHA-512

When submitting a timestamp request, the hash provided by the requester must also be generated using one of the supported algorithms listed above. Requests using unsupported hash functions will be rejected by the SIRAR-TSA.

5.3.3 ACCURACY OF TIME

The SIRAR-TSA Service uses time that is traceable to Coordinated Universal Time (UTC) through trusted external time sources. The Timestamping Unit (TSU) synchronizes its system clock using sirar's internal time distribution infrastructure based on Microsoft Active Directory (AD) time services, which in turn are synchronized with one or more trusted external time sources.

SIRAR-TSA ensures that the time used for timestamp generation achieves an accuracy of ±1 second or better with respect to UTC under normal operating conditions. Time synchronization is monitored on an ongoing basis, and sirar defines acceptable accuracy thresholds and procedures for the detection and handling of time deviations.

If the accuracy of the time source cannot be assured within the defined thresholds, SIRAR-TSA applies appropriate operational controls to prevent the issuance of unreliable timestamps and to manage the incident in accordance with its operational procedures.

5.3.4 LIMITATION OF USE OF THE SERVICE

The use of the service is subject only to the limitations outlined in Section 6.5.

5.3.5 VERIFICATION OF THE TIMESTAMP

5.3.5.1 Verification of timestamp Issuer

TSU certificates and the corresponding certification path are published to allow Relying Parties to enable verification of the origin and authenticity of issued timestamps. Such information is made available through the public repository at https://sirar.com.sa/repository/.

Relying Parties verify the authenticity of a timestamp by validating the digital signature contained within the Time-Stamp Token using the public key included in the TSU certificate, together with the issuing Certification Authority certificates (i.e. sirar's Timestamping CA certificate) forming the trust chain. Successful validation confirms that the timestamp was generated and signed by the TSU operated under the responsibility of the SIRAR-TSA.

5.3.5.2 Verification of timestamp revocation status

The revocation status of the Timestamping Unit (TSU) certificate used to sign a Time-Stamp Token may be verified during and after the certificate's validity period using the Certificate Revocation List (CRL) and/or the Online Certificate Status Protocol (OCSP) services provided by the Timestamping CA.

Information on how to obtain revocation status is identified in the CRL Distribution Point (CDP) and Authority Information Access (AIA) extensions of the TSU signing certificate. Relying Parties may use this information to determine whether the TSU certificate was valid at the time the timestamp was generated.

The management and publication of CRLs and OCSP responses for TSU certificates are the responsibility of the TSCA operated by sirar and are outside the operational scope of the SIRAR-TSA Service.

5.3.6 SERVICE AVAILABILITY

The following measures have been implemented to ensure availability of the service:

- **Redundant setup of IT Systems to avoid single points of failure.**
- **Redundant high-speed internet connections to avoid loss of service.**
- **Use of uninterruptable power supply and power supply redundancies.**

Although these measures ensure service availability, an annual availability of 100% cannot be guaranteed.
The frequency and duration of service interruptions are being monitored to ensure that the total annual unavailability remains within the defined SLA (99.6%). Each disruption event is recorded, and significant or repeated outages trigger incident escalation procedures.

An annual availability target of 99.6% corresponds to a maximum cumulative downtime of approximately 1 day and 11 hours per calendar year.
For informational purposes only, and assuming a 365-day calendar year, 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 informational derivations of the annual availability target and do not represent independent, cumulative, or additional service-level commitments beyond the stated annual availability objective.

5.3.7 SUBSCRIBER OBLIGATIONS

When obtaining a Time-Stamp Token (TST), the Subscriber is responsible for performing appropriate validation checks to confirm that the TST has been correctly generated and signed by the Timestamping Authority. This includes verifying the digital signature on the TST and validating the associated certificate chain in accordance with the procedures described in Section 5.3.5 of this document.

Subscribers rely on certificate status information (e.g., CRLs and OCSP) published by the issuing Certification Authority (i.e., sirar's Timestamping CA) to determine whether the TSU certificate was valid at the time the timestamp was generated. Subscribers are not expected to assess the internal security status of the TSA or the TSU private key beyond the validation mechanisms defined in this document and applicable standards.

Timestamps shall be requested using the HTTP-based Time-Stamp Protocol as specified in IETF RFC 3161.

Subscribers shall use methods, software, or toolkits that are compatible with the SIRAR-TSA Service. Where sirar specifies approved or supported client implementations, Subscribers are expected to use such implementations unless otherwise explicitly authorized in writing by sirar.

5.3.8 RELYING PARTY OBLIGATIONS

The terms and conditions made available to relying parties shall include an obligation on the relying party that, when relying on a time-stamp token, the relying party shall:

1. Verify the authenticity and integrity of the Time-Stamp Token, including validation of the digital signature on the TST and verification of the associated certificate chain, in accordance with the procedures described in Section 5.3.5 of this document,
2. Relying Parties rely on certificate status information (e.g., CRLs and OCSP) provided by the issuing Certification Authority (i.e., sirar's Timestamping CA) to determine whether the TSU certificate was valid at the time the timestamp was generated,
3. Consider any limitations on the usage of the timestamp indicated by this policy,
4. Consider any other precautions prescribed in agreements or elsewhere.

5.3.9 LIMITATION OF USE OF SERVICE

sirar provides timestamping services that may be used, without restriction, in connection with legal or other electronic transactions.

However, to the extent permitted under applicable laws of the Kingdom of Saudi Arabia, sirar shall not be held liable—except in cases of fraud or wilful misconduct—for:

- Loss of profits;
- Loss or corruption of data;
- Any indirect, incidental, consequential, or punitive damages arising from or related to the use, delivery, licensing, performance, or non-performance of timestamping services;
- Any other damages or losses not directly attributable to sirar.

sirar does not assume financial liability for timestamps that are misused or used in a manner inconsistent with the applicable policies or intended purpose of the service.

5.3.10 RETENTION PERIOD

sirar retains all relevant records and data associated with the provision of its timestamping services for a minimum period as defined in the applicable regulatory requirements. Such records include timestamp requests, issued timestamps, and related audit logs necessary to demonstrate the integrity, authenticity, and compliance of the service.

Unless otherwise specified by applicable law or supervisory authority, the retention period shall not be less than 10 years from the date of issuance.

Certification Authority records related to the issuance and management of Timestamping Unit (TSU) certificates are governed separately by the Certification Practice Statement (CPS) maintained by sirar, which is published at: https://sirar.com.sa/repository/

5.3.11 LIMITATION OF LIABILITY

The SIRAR-TSA Service is operated in accordance with this Timestamping Authority Policy and Practice Statement (TSA-PPS), the applicable terms and conditions, and the Certification Practice Statement (CPS) maintained by sirar for the Timestamping CA, where relevant. These documents are publicly available through their respective repositories.

To the maximum extent permitted by applicable law, sirar shall not be liable for any indirect, incidental, consequential, special, or punitive damages arising out of or in connection with the use of, or reliance on, the SIRAR-TSA Service. This limitation includes, without limitation, any liability for:

- loss of profits, revenue, sales, or turnover;
- loss or damage to reputation or goodwill;
- loss of contracts or customers;
- loss of use of, or damage to, software, data, computer systems, or other equipment;
- wasted management time or staff time; or
- losses or liabilities arising under or in connection with any other contracts

Nothing in this section shall exclude or limit sirar’s liability where such exclusion or limitation is not permitted under applicable law, or for losses arising directly from sirar’s material breach of this Timestamping Authority Policy and Practice Statement.

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

5.3.12 Applicable Legal System, Complaint, Dispute Resolution

The laws of the Kimgdom 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 Kimgdom of Saudi Arabia.

5.4 Information Security Policy

Sirar implements and maintains an information security policy applicable to personnel, suppliers, and contractors involved in the operation and support of the SIRAR-TSA Service. The information security policy defines the principles and controls governing the protection of information assets related to the timestamping service.

The information security policy is reviewed at least annually and is additionally reviewed and updated whenever significant changes occur to the operational environment, risk landscape, or applicable regulatory requirements.

5.5 TSA Obligations

5.5.1 General Obligations

SIRAR-TSA ensures conformance with the procedures stated in the present document. An independent auditor verifies the efficiency of procedures on a regular basis.

5.5.2 TSA Obligations toward Subscribers

The SIRAR-TSA assumes the following obligations towards the subscribers of the timestamp service:

1. Ensures that the service is operated using appropriately secured and managed systems and software that are suitable for the provision of trusted timestamping services,
2. To operate in accordance with this Time-stamping Policy, and the other relevant operational policies and procedures,
3. It ensures that the timestamps maintain an accuracy of at least one (1) second relative to UTC,
4. To maintain a competent and experienced team that can ensure the continuity of the Time Stamp Service,
5. To undergo internal and external reviews to assure compliance with relevant legislation and adopted internal policies and procedures,
6. To monitor and control the Time Stamp Service and the whole TSA infrastructure, to prevent or limit any disturbance or unavailability of the service except in the case of planned technical interruptions and loss of time synchronization.

5.6 Information for relying parties

Refer to section 5.3.5.

6. TSA MANAGEMENT AND OPERATIONS

6.1 INTERNAL ORGANIZATION

sirar has established a formal and structured internal organization to manage and operate its Timestamping Authority (TSA) in accordance with applicable regulatory requirements, recognized security practices, and industry best practices.

The internal organization supporting the SIRAR-TSA Service ensures that:

- **Roles and responsibilities** related to timestamping operations are clearly defined, documented, and communicated across all relevant functions, including system administration, security operations, and compliance monitoring.

- **Trusted roles** are assigned to qualified personnel who have undergone appropriate background checks and role-specific training. Such roles include, but are not limited to, TSA operators, system administrators, security officers, and compliance personnel.

- **Separation of duties** is enforced to reduce the risk of unauthorized or erroneous actions, with dual control applied to critical TSA processes where appropriate.

- **Oversight and governance** of the timestamping service are maintained through formal management structures, including the sirar PKI Committee.

- **Security and operational policies and procedures** applicable to the timestamping service are documented, implemented, and periodically reviewed to ensure continued alignment with regulatory, contractual, and operational requirements

An active security management program is maintained applicable to the SIRAR-TSA Service. This program is designed to document, implement, and continually improve sirar's security posture and addresses areas such as risk management, access control, incident response, business continuity, and ongoing security awareness.

This internal organizational framework enables sirar to operate a trusted, resilient, and well-governed timestamping service, supporting the integrity, authenticity, and availability of time-related data in accordance with this Timestamping Authority Policy and Practice Statement.

6.2 PERSONNEL SECURITY

The SIRAR-TSA Service is operated by sirar within a controlled organizational environment supported by personnel security measures aligned with applicable regulatory requirements, recognized security practices, and industry best practices.

sirar ensures that managerial and operational personnel involved in timestamping activities possess the appropriate skills, knowledge, and experience relevant to their assigned roles. This includes competence in areas such as timestamping services, cryptographic operations, trust services, and applicable information security procedures, including risk management and personnel security.

sirar defines Trusted Roles as positions that involve access to, or control over, sensitive systems, cryptographic material, or security-critical functions supporting the SIRAR-TSA Service. Trusted Roles include, but are not limited to:

- TSA operators;
- system and network administrators supporting the TSA service;
- security personnel;
- personnel performing cryptographic or security-sensitive operations; and
- compliance and oversight personnel

For all individuals assigned to Trusted Roles, sirar performs identity verification in accordance with established human resources procedures. This includes verification using government-issued or otherwise well-recognized identification documents and background screening consistent with sirar's internal policies and applicable regulatory requirements.

Before any individual is granted Trusted Role status, the following conditions shall be satisfied:

- Formal approval of the Trusted Role assignment by authorized management.
- Issuance of appropriate physical access means to secure facilities, where applicable.
- Provisioning of electronic credentials granting access only to those TSA systems and functions required for the individual's assigned responsibilities

Access to sensitive systems and cryptographic functions supporting the SIRAR-TSA Service is strictly controlled, monitored, and limited to authorized personnel.

6.3 ASSET MANAGEMENT

sirar maintains a comprehensive, accurate, and up-to-date inventory of information assets relevant to the operation of the SIRAR-TSA Service. Such assets include information, hardware, software, 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 sirar's risk assessment activities. Asset classifications determine the level of protection, handling, and control measures applied throughout the asset lifecycle.

Changes to TSA-related systems, applications, or configurations are managed through documented change management procedures. These procedures ensure that changes are properly reviewed, tested, approved, and authorized prior to implementation, and that potential impacts on the security and availability of the timestamping service are assessed.

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

- Physical devices are delivered, transported, stored, and installed in a controlled and monitored manner to preserve integrity and traceability.
- Replacement activities follow the same security and approval requirements applied to the initial deployment of equipment.
- Only authorized, qualified, and trusted personnel are permitted to perform hardware installation, replacement, or maintenance activities.

6.4 ACCESS CONTROL

sirar ensures that appropriate physical and logical access controls are implemented to protect facilities, systems, hardware, software, and information supporting the SIRAR-TSA Service.

Access to TSA-related systems and information is granted on the basis of least privilege and is restricted to authorized personnel whose access is required for the performance of their assigned duties. Logical access controls include authentication mechanisms, role-based authorization, access logging, and periodic review of access rights. User access privileges are reviewed regularly, and access rights that are no longer required are promptly revoked in accordance with documented procedures.

Sensitive operational activities are performed within highly restricted physical areas. Physical access events are logged and monitored, and additional access controls, including biometric authentication where applicable, are used to enforce individual accountability. Unescorted access by unauthorized personnel is not permitted, and visitors or non-trusted individuals are always accompanied when present within secured areas.

Facilities hosting TSA-related infrastructure are continuously monitored by trained security personnel on a 24x7 basis and are equipped with appropriate normal and emergency lighting to support safe and secure operations. Physical security controls are designed to protect systems and data from unauthorized access, tampering, or compromise, and are implemented within clearly defined security perimeters.

The detailed physical and environmental security controls applicable to the hosting facilities and infrastructure are specified in section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

6.5 CRYPTOGRAPHIC CONTROLS

6.5.1 TSU KEY GENERATION

The generation of the Timestamping Unit (TSU) signing key(s) supporting the SIRAR-TSA Service is performed in a physically secured environment by personnel assigned to trusted roles, operating under dual control. Access to perform TSU key generation activities is strictly limited to authorized personnel whose responsibilities require such access.

TSU signing key generation is carried out within a cryptographic module compliant with FIPS PUB 140-2 Level 3 or equivalent assurance, ensuring protection against key compromise, unauthorized use, and tampering.

The TSU key generation algorithms, key lengths, and signature algorithms used for signing Time-Stamp Tokens are defined in the Timestamping CA CPS.

6.5.2 TSU PRIVATE KEY PROTECTION

SIRAR-TSA ensure that TSU private keys remain confidential and maintain their integrity. These include use of Hardware Security Modules (HSMs) certified to FIPS 140-2 Level 3 to hold and sign with the keys.

When TSU private keys are backed up, they shall be copied, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

The personnel authorized to carry out this function shall be limited to those requiring doing so under SIRAR-TSA practices.

6.5.3 TSU PUBLIC KEY CERTIFICATE

sirar ensures that 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 by the Timestamping CA operated by sirar, in accordance with Timestamping CA CPS.

The TSU certificate, together with the associated certification path information, is published in a publicly repository to enable Relying Parties to perform signature and certificate validation.

sirar remains responsible for ensuring that valid and up-to-date TSU certificate information is made available to Relying Parties for the purposes of timestamp verification.

6.5.4 REKEYING TSU'S KEY

The operation period for TSU key pairs is defined by setting a private key usage period within the TSU's public key certificate. TSTs are signed with sirar's TSU certificates of three (03) years validity. sirar TSU certificates of three (03) years validity are only used to sign TST during a usage period of one (1) year. sirar TSU rekey procedure is executed upon expiry of the usage period (1 year) of the TSU certificate.

6.5.5 LIFE CYCLE MANAGEMENT OF SIGNING CRYPTOGRAPHIC HARDWARE

The SIRAR-TSA assures that:

- The integrity of the cryptographic security modules was not tampered with during transportation from the manufacturer.
- The integrity of the cryptographic security modules was not affected during their storage, prior to their installation.
- They are installed, managed, and operated by trusted personnel /roles using, at least, dual control in a physically secured environment.
- The cryptographic security modules work correctly.
- The private signing keys stored on the cryptographic security modules are destroyed the moment it is taken out of production.

6.5.6 END OF TSU KEY LIFE CYCLE

The validity period of a Time Stamping Unit (TSU) private key shall never exceed the validity of its corresponding public key certificate. Once the private key expires, the TSA will no longer accept any requests to issue timestamps using that key.

Upon expiration, the private key stored within the cryptographic hardware is securely destroyed, ensuring it cannot be recovered or reused. This destruction follows strict operational and technical procedures designed to maintain the security and integrity of the TSA.

Documented operational procedures are maintained to ensure that new TSU key pairs are generated, certified, and activated in a timely manner prior to the expiration of an existing TSU key, to maintain continuity of the SIRAR-TSA Service without interruption.

6.6 TIMESTAMPING

6.6.1 TIME-STAMP ISSUANCE

SIRAR-TSA ensures that electronic timestamps are issued in a secure, reliable, and controlled manner. Technical and operational controls are in place to ensure that Time-Stamp Tokens (TSTs) are generated correctly and include accurate and verifiable time information.

Time-Stamp Tokens are issued in accordance with the time-stamping protocol referenced in this document. Each TST includes, at a minimum:

- A representation (e.g., 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;
- The time of issuance, maintained with an accuracy of ±1 second or better with respect to Coordinated Universal Time (UTC);
- An electronic signature generated using a TSU private key dedicated exclusively to timestamping;
- Identifiers allowing the issuing Timestamping Authority (TSA) and Timestamping Unit (TSU) to be unambiguously determined;
- Where a nonce is included in the timestamp request, the same nonce value is included unchanged in the corresponding TST response.

SIRAR-TSA ensures that audit records related to time synchronization and timestamp issuance are maintained to support verification of the accuracy and integrity of the timestamping service.

The SIRAR-TSA Service issues electronic timestamps only while the corresponding TSU private key is valid. No Time-Stamp Tokens are issued once the TSU private key has reached the end of its validity period or has been otherwise deactivated.

6.6.2 CLOCK SYNCHRONIZATION WITH UTC

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

The system clocks of the Timestamping Unit (TSU) are synchronized using centralized time distribution infrastructure based on Microsoft Active Directory (AD). The AD environment provides a consistent and controlled internal time source for systems supporting the timestamping service. The AD time services are, in turn, synchronized with trusted external time sources to ensure traceability of the time used for timestamp issuance to Coordinated Universal Time (UTC).

Technical measures are implemented to continuously maintain clock synchronization within the declared accuracy bounds. The TSU monitors time drift and synchronization status, and additional synchronization actions are performed where necessary to restore accuracy.

Leap second adjustments are handled in accordance with established time synchronization procedures, based on notifications issued by the relevant authoritative bodies, to ensure continuity and correctness of timestamp issuance.

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

Audit and calibration records related to the operation of the Timestamping Unit (TSU) are maintained in accordance with documented procedures. Records related to time synchronization, monitoring, detected deviations, and corrective actions are retained to support auditability and to enable verification of the accuracy and reliability of the SIRAR-TSA Service. sirar remains responsible for ensuring that such records are available, complete, and protected in accordance with this Timestamping Authority Policy and Practice Statement.

7. PHYSICAL AND ENVIRONMENTAL SECURITY

7.1 SITE LOCATION AND CONSTRUCTION

Refer to section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

7.2 PHYSICAL ACCESS

Refer to section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

7.3 POWER AND AIR CONDITIONING

Refer to section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

7.4 WATER EXPOSURES

Refer to section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

7.5 FIRE PREVENTION AND PROTECTION

The SIRAR-TSA Service's equipment is housed in a facility with appropriate fire suppression and protection systems.

7.6 MEDIA STORAGE

Refer to section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

7.7 WASTE DISPOSAL

Refer to section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

7.8 OFF-SITE BACKUP

Refer to section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

7.9 OPERATION SECURITY

Refer to section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

7.10 NETWORK SECURITY

Refer to section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

7.11 INCIDENT MANAGEMENT

Refer to section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

7.12 COLLECTION OF EVIDENCE

All information relevant to the operation of the SIRAR-TSA Service is recorded and retained for an appropriate period to support auditability, legal evidentiary requirements, and continuity of service, including after the cessation of timestamping activities where applicable.

In particular:

- The confidentiality and integrity of current and archived records relating to the operation of the timestamping service are maintained.
- Records relating to service operation are archived in a complete and confidential manner in accordance with disclosed business practices.
- Records relating to the operation of the service are made available, where required, for the purpose of providing evidence of correct service operation in legal or regulatory proceedings.
- The precise time of significant events related to the timestamping service is recorded, including environmental events, key management events, certificate lifecycle events, and clock synchronization events.
- The time used for recording events in audit logs is continuously synchronized with Coordinated Universal Time (UTC)

Records relating to the operation of the timestamping service are retained for a period extending beyond the expiration of the validity of the relevant TSU signing keys, where necessary to provide legal evidence in response to a court order or other applicable legal requirement.

The following records are maintained with precise time information:

- Time-stamp requests received and Time-Stamp Tokens generated;
- Events related to TSA administration, including certificate management, key management, and clock synchronization;
- Events related to the lifecycle of TSA keys and certificates.

7.13 BUSINESS CONTINUITY MANAGEMENT

Refer to section 5 of the Timestamping CA CPS, which governs the operation of certificate-related systems and facilities.

7.14 TSA TERMINATION AND TERMINATION PLANS

To minimize potential disruptions to subscriber and relaying parties following the cessation of SIRAR-TSA services, SIRAR-TSA maintains an up-to-date termination plan by which its ensure before terminates its services:

- Inform the following of the termination: all subscribers and other entities with which the sirar has agreements or other form of established relations, and other relying parties;
- Where applicable, terminate the authorization of any subcontractors or delegated parties acting on sirar's behalf in relation to the provision of timestamping services.
- If deemed appropriate, transfer obligations (provision of timestamping services) to an identified reliable third party.
- Ensure that the TSU private keys, including backup copies, are destroyed, or withdrawn from use, in a way that the private keys can no longer be retrieved.
- Revoking all non expired TSU certificates.

8. COMPLIANCE

The SIRAR-TSA Service operates in compliance with applicable laws and regulations of the Kingdom of Saudi Arabia and follows recognized technical standards and best practices applicable to electronic timestamping services, including implementation in accordance with IETF RFC 3161; the service is a standalone timestamping service and is not subject to a dedicated WebTrust assurance program, and compliance with applicable legal, regulatory, and technical requirements is reviewed and validated on a yearly basis through independent internal and external reviews, as appropriate.