Iraq National PKI

Timestamping CA

Certificate Practice Statement

Change History

Version	Date	Changes Description	Responsible
0.1	29/01/2023	Initial version.	Touir Mustapha
0.2	23/02/2023	Internal review and update.	Ahmad Ibrahim
0.3	04/12/2023	Adding OIDs values, Contact information, Repository URL. Applying Technology Source Template.	Touir Mustapha
0.4	28/02/2024	Addressing the auditor's feedback.	Touir Mustapha, Yasir Khan
0.5	14/03/2024	Reviewing and updating based on auditor's feedback on Root CA CP/CPS and TSP CP.	Touir Mustapha, Yasir Khan
0.6	02/05/2024	Update in section 5.4.1 to clarify data that need to be logged as part of "Firewall and Router activities" logging requirements.	Touir Mustapha
0.7	15/05/2024	Reviewing and updating based on auditor's feedback on CPSs.	Touir Mustapha Yasir Khan
1.0	15/07/2024	Updates based on auditor's recommendations following the Point-In-Time audit.	Touir Mustapha Yasir Khan
1.1	16/09/2025	Annual review.	Technology Source
1.2	03/06/2026	Amended to change "Subscriber Agreement" to "Subscriber Terms and Conditions of Use".	Technology Source

Document Approval

Version	Approver (Name/Title)	Signature
1.2	**PKI GB Director**	**Date: 03/06/2026**

Table of Contents

1 Introduction

The present document is the Certification Practice Statement (CPS) describing the certification practices that apply to Technology Source (hereinafter, TS) Timestamping Issuing CA. This CPS complies with the TSP Certificate Policy that is applicable to the provision of certification services offered the Trust Services Providers (TSP) issuing publicly trusted certificates to end-entities under the Iraq National PKI Root CAs in the republic of Iraq.

This CPS addresses the technical, procedural, and organizational policies of the Timestamping CA that are established and operated by TS under the Iraq national PKI hierarchy, with regards to the complete lifetime of certificates issued by this CA.

This CPS covers the issuance and controls surrounding the following types of certificates issued by the Timestamping CA:

- **CS TSA certificate –** TSA certificate involved in code signing.
- **DS TSA certificate –** TSA certificate involved in document signing.

This CPS complies with the formal requirements of Internet Engineering Task Force (IETF) [RFC 3647] regarding format and content. While certain clause titles are included according to the structure of [RFC 3647], the topic may not necessarily apply in the implementation of the Timestamping CA. Such clauses are denoted as “clause not applicable”.

This CPS complies with the WebTrust Principles and Criteria for Certification Authorities requirements published at https://www.cpacanada.ca

TS PKI Governance Board is committed to maintain this CPS in conformance with the current versions of the below requirements published at http://www.cabforum.org :

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing.
- Network and Certificate System Security Requirements.

If there is any inconsistency between this document and the requirements above, the above requirements take precedence over this document.

The CPS is public. Wherever confidential information is referenced herein, the text refers to classified documentation that is available to authorized persons only.

Further information with regards to this CPS can be obtained from the TS PKI GB, using contact information provided in clause 1.5.

1.1 Overview

The Iraq National PKI is established under Information & Telecommunication Public Company (ITPC) with multiple root CAs representing national root PKI program. With this National PKI, the Iraqi Government aims to provide a framework to facilitate the establishment of Trust Service Providers (TSP) offering digital certification and trust services to government and non-government entities. The Iraq PKI hierarchy has two levels described as following:

Level 0:

The below five (5) Roots Certification Authorities (CA) are established for the different types of certificates to be issued. The Information & Telecommunication Public Company (ITPC) is responsible for this Root CA layer. As the national PKI governance body, the ITPC is mandated to operate the Policy Management Authority (PMA). ITPC Root CAs[1] are:

- **Iraq Code Signing Root CA:** certifies/signs Code Signing Subordinate CAs.
- **Iraq S/MIME Root CA:** certifies/signs email protection Subordinate CAs.
- **Iraq TLS Root CA:** certifies/signs TLS Subordinate CAs.
- **Iraq Document Signing Root CA**: certifies/signs natural & legal persons document signing Subordinate CAs.
- **Iraq Timestamp Root CA**: certifies/signs Timestamping Subordinate CA.

Level 1: The TS's Subordinate CAs falls at this level within the National PKI hierarchy as shown in the below figure :

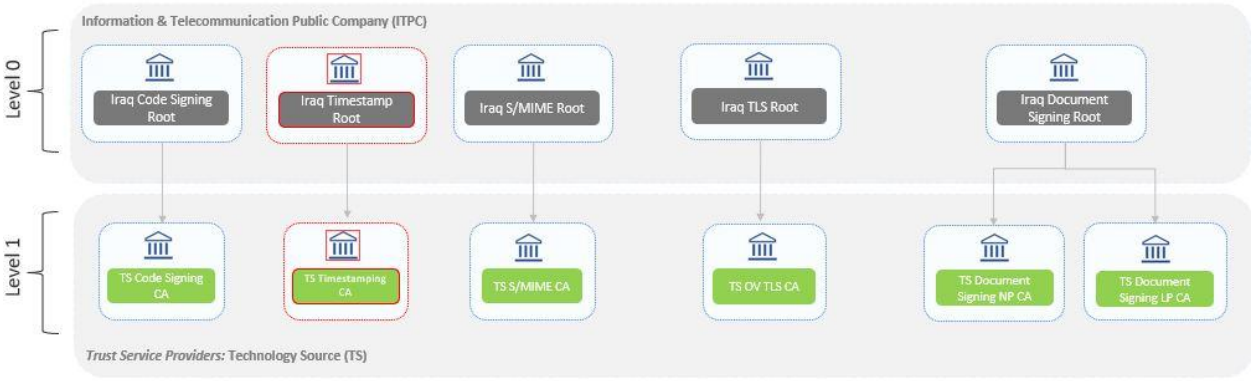

Figure 1 Iraq National PKI hierarchy

[1] For timestamping certificates, only the Iraq Timestamp Root CA is relevant since it signs the Timestamping Subordinate CA certificate of Technology Source. Other Root CAs belongs to the Iraqi PKI but aren't pertinent to timestamping certificates issuance and are not included in the timestamping hierarchy as depicted in Figure 1.

Technology Source is the organization to operate the Subordinate CAs and offer related trust services to the Iraqi government and non-government domains. As such the Technology Source operates as a Trust Services Provider (TSP) offering its services through a hierarchy of Subordinate CAs, implemented under the ITPC Root CAs. ITPC Root CAs certified TSP Subordinate CAs[2] for Technology Source as follows:

- **Technology Source Code Signing CA**: Subordinate CA that issues certificates to sign the software libraries, .jar files, .exe file, .msi files etc.
- **Technology Source S/MIME CA:** Subordinate CA that will issue certificates for email signing and encryption.
- **Technology Source TLS CA:** Subordinate CA that will issue web server TLS organization validation (OV) certificates.
- **Technology Source Document Signing NP CA:** Subordinate CA that will issue document signing certificates to natural persons (citizens and employees).
- **Technology Source Document Signing LP CA:** Subordinate CA that will issue document signing certificates to legal persons (Iraqi non-government and government entities).
- **Technology Source Timestamping CA:** Subordinate CA that will issue TSA certificates involved in document signing and code signing.

The above use cases are key enablers of digital transformation as they represent the corner stone of securing electronic transactions. Supporting these use cases under a unified trust model with government assurance, facilitates adoption, enables interoperability, and enhances user trust.

The TS PKI GB interacts closely with the ITPC PMA to maintain conformity with this CPS in relation to the certification and operations of the TS Timestamping CA.

1.1.1 Technology Source PKI Governance Board (TS PKI GB)

The Governance board governing the Technology Source PKI (including the TS Timestamping CA) is referred to as the TS PKI GB. The TS PKI GB comprises the necessary functions including policy, security, compliance and legal that are required to provide strategic direction and continuously supervises the TS PKI operations.

The TS PKI GB is particularly responsible for:

- Define and maintain the TS PKI strategy,

[2] For timestamping certificates, only the Iraq Timestamp Root CA is relevant since it signs the Timestamping Subordinate CA certificate of Technology Source. Other Root CAs belongs to the Iraqi PKI but aren't pertinent to timestamping certificates issuance and are not included in the timestamping hierarchy as

- Define the TS PKI services and approve its delivery model,
- Define and maintain the TS PKI Policies and Practices,
- Conduct regular supervision activities on the TS PKI operations team,
- Approve PKI budget, and take major commercial decisions,
- Approve major changes on the PKI infrastructure,
- Approve key ceremonies, and allocate internal/external auditors as required,
- Get involved in major incidents, and take decisions as required,
- Lead the resolution of disputes arising out of or related to the activities of the TS PKI,
- Evaluate incidents where key TS PKI staff/personnel did not respect the security and/or operational procedures, including ethics.

1.2 Document Name and Identification

This document is titled "**Certificate Practice Statement for the Technology Source Timestamping CA**" which is identified by the OID **2.16.368.1.2.1.5** and referenced in related documents as [**TS TSA CA CPS**]. This CPS is approved by the TS PKI GB as well as the ITPC PMA for the publication.

The Timestamping CA includes the above mentioned OID in the CP extension of the certificates they issue to indicate compliance with the current requirements.

1.3 PKI Participants

Several parties are involved during the lifecycle management of the digital certificates issued by this CA. This includes:

- The TS Timestamping CA (Certification Authority),
- TS Registration Authorities (RA),
- Subscribers,
- Relying parties.

These participants, collectively called PKI participants, and their roles are described in the following sections.

1.3.1 Certification Authorities

The TS Timestamping CA (hereinafter, CA) are owned and operated by a TS through its premises in Iraq. This CA has been approved by the ITPC and signed by the Iraq Timestamp Root CA, as depicted in Figure 1 (section 1.1).

This CA provides the following certification services:

- **Certificate Generation Service —** it issues end-entity certificates based on the verification conducted by the Registration Authorities.

- **Dissemination Service —** it disseminates OCSP and CA certificates and makes them available to relying parties. This service also makes available any public policy and practice information to Subscribers and relying parties.
- **Revocation Management Service —** it processes requests and reports revocation data for determining the appropriate action to be taken. The results of this service are available through the certificate validity status service.
- **Certificate Validity Status Service —** it provides certificate validity status information to relying parties based upon certificate revocation lists and an OCSP responder service. The status information shall always reflect the status of the certificates issued by this CA.

1.3.2 Registration Authorities

TS operates an RA function serving TS Timestamping CA, mainly to process certification requests for certificate issued to TSA services.

The RA function falls within the PKI operations structure and responsible for identity validation and certificate request management for the government and non-government entities.

TS RA function includes but not limited to:

- Authenticating, approving, or rejecting certificate application and revocation requests,
- Identify subscribers as per the naming conventions defined in this CPS, so that each subscriber is uniquely and unambiguously identified,
- Process certificate issuance and revocation requests based on validated and approved requests,
- Creating and maintaining an audit-log journal that records all significant events related to the RA's operations,
- Providing selective access to audit-log journal records as specified in this CPS,
- Implementing other operational controls as specified in this CPS, Processes, and stores information according to the requirements defined in this CPS (particularly, in section 5).

1.3.3 Subscribers

Subscribers of this CA is Technology Source itself which operate the TS TSA service. For any certificate, the subscriber signs or ratifies a subscriber terms and conditions of use to establish a consent on the terms and conditions of use as set forth by TS.

1.3.4 Relying Parties

Relying Parties must consistently refer to Technology Source's Certificates Validity Status Services (i.e., CRL and OCSP), prior to relying on information featured in said certificate.

1.3.5 Other Participants

Other Participants include:

- The ITPC PMA is the supervision authority responsible for supervising the entire activity of the licensed TSP (i.e., Technology Source). The roles and responsibilities of PMA are described in the ITPC Root CP/CPS published at: https://pki.itpc.gov.iq
- Qualified independent WebTrust auditors who verifies the requirements set out in section 8.2.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The certificates issued by the TS Timestamping CA are:

1. **Certificates for TS TSA service:**

   a) ***TSU Certificates:*** These certificates are issued by the Timestamping Subordinate CA to create and verify electronic time stamps. TSU Certificates issued under this CPS to Technology Source itself are used to provide Time Stamping Service, in accordance with the Time Stamping Policy and Practice Statement, available under https://pki.techsource.iq.

   This CA issues the following TSU certificates:

   a. **DS Timestamp Certificate** – Certificates for signing timestamps used for document signing.

   b. **CS Timestamp Certificate** – Certificates for signing timestamps used for code signing.

2. **OCSP Responder Certificate** – used to sign and verify the Online Certificate Status Protocol (OCSP) responses for certificates issued by this CA.

1.4.2 Prohibited Certificate Uses

The use of certificates for purposes other than those mentioned in section 1.4.1 is strictly prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CPS document is administered by the TS PKI GB according to its operating model and based on as needed interaction with the ITPC PMA.

1.5.2 Contact Person

Requests for information on any inquiry associated with this CPS should be addressed to:

Technology Source PKI Governance Board
Technology Source
Baghdad - Four Streets - Nearby Al-Ma'amon High School
Email: info@techsource.iq
Phone No.: (+964) 784 136 1693

The TS PKI GB accepts comments regarding this CPS only when they are addressed to the contact above.

Certificate Problem Report
Technology Source maintains a continuous 24/7 ability to internally respond to any high priority revocation requests and certificate problem reports provides instructions for certificate revocation and certificate problem reporting on a dedicated page in its public repository, accessible at:

https://pki.techsource.iq/repository/Certificate_Problem_Report.html.

Subscribers and Relying Parties, Application Software Suppliers, and other third parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates by sending email to certificate.problem@techsource.iq

Technology Source will validate and investigate the revocation request before taking an action in accordance with section 4.9.

If Technology Source deems appropriate, it may forward the revocation reports to law enforcement.

1.5.3 Person Determining CPS Suitability for the Policy

Based on the compliance audits' results and recommendations, The TS PKI GB determine the suitability and applicability of this CPS. This CPS shall be approved by the PMA as well, since it must ultimately comply with the provisions of the TSP CP.

1.5.4 CPS Approval Procedures

The TS PKI GB, along with the PMA, formally approves any new version of the CPS.

Dedicated personnel with PKI policy experience from the TS PKI GB review this CPS for the initial draft and subsequent changes to ensure consistency with the best practices implemented and with TSP CP prior to TS PKI GB approval. Amendments may take the form of a document containing an amended version of the CPS or an update notice. Changes made to this CPS will be tracked in the revision table.

The new CPS version will then be submitted to the PMA for ultimate approval, as it must ultimately comply with the provisions of the TSP CP.

Prior to becoming applicable, the updated version of the CPS is announced in the repository as available on: https://pki.techsource.iq

Upon published, the updated version is binding on all Subscribers, including Subscribers and parties relying on Certificates issued under a previous version of the CPS.

1.6 Definitions and Acronyms

1.6.1 Definitions

Applicant: Is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request. In the context of this CPS, the applicant is the Technology Source operating the timestamping service.

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

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

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

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

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

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

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

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

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

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

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

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

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certificate Profile: A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. a Section in a CA's CPS or a certificate template file used by CA software.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control"

under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

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

Cryptographic Token: A USB cryptographic device certified as conformant with FIPS 140 Level 2 or equivalent.

CSPRNG: A random number generator intended for use in cryptographic system.

Delegated Third Party: A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits, but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

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

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

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

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

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

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

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

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

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

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

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

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

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

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

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

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

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

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

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

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

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

Root CA: The top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject: The timestamping service under the control and operation of Technology Source (i.e., Subscriber).

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

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber terms and conditions of use.

Subscriber Terms and Conditions of Use: A consent between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

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

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. In the context of this CPS, Technology Source operates two (02) TSUs for document signing and Code signing.

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

Validation Specialists: Someone who performs the information verification duties specified by these Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

1.6.2 Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CCTV	Closed Circuit TV
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CV	Curriculum Vitae
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
FIPS	Federal Information Processing Standards

EID	Electronic Identity Card
EIDAS	Electronic Identification, Authentication, and Trust Services
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IPSEC	Internet Protocol Security
ISO	International Standards Organization
ITPC	Information & Telecommunication Public Company
IT	Information Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Information Number
PKCS#1	Public Key Cryptography Standards (PKCS) #1
PKCS#7	Cryptographic Message Syntax
PKCS#10	Certification Request Syntax Specification
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RSA	Rivest-Shamir-Adleman (The names of the inventors of the RSA algorithm)
RTO	Recovery Time Objective
SSL	Secure Sockets Layer
TLD	top-level domain
TS	Technology Source

TSA	Timestamping Authority
TLS	Transport Layer Security
TSP	Trust Service Provider
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier, a URL, FTP address, email address, etc.
URL	Universal Resource Locator

1.6.3 References

This document refers to the following:

- X.509 - The standard of the ITU-T (International Telecommunications Union-T) for Certificates.
- RFC3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC3161 - Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Network Security
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.
- ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps.
- ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

2 Publication and Repository Responsibilities

2.1 Repositories

The Technology Source maintains an online repository available 24 × 7 and accessible at: https://pki.techsource.iq

Technology Source is responsible for making available the following information to be published on its repository:

- Current and previous version of Technology Source CPSs;
- Current version of ITPC Root CP/CPS & TSP CP;
- Subscriber, LRA and relying party terms and conditions of use, PDS, TSA CP/PS and TSA disclosure statement.
- The valid self-signed Root CA Certificates, as well as the Technology Source Subordinate CA certificates, OCSP certificates, and certificate revocation lists (CRLs) issued by these Subordinate CAs;
- Time-stamping Unit Certificates (TSU);
- Audit reports.

2.2 Publication of Certification Information

Technology Source is the entity tasked with providing the information for publication, as outlined in section 2.1 of this document.

Technology Source publishes certificate validity status information in frequent intervals as indicated in this CPS.

The provision of the certificate validity status information is a 24/7 available service offered as follows:

- Published CRLs including any changes since the publication of the previous CRL, at regular intervals. The TS Timestamping CA add a pointer (URL) to the relevant CRL to Subscribers' certificates as part of the CDP extension whenever this extension is present,
- An OCSP responder compliant with RFC 6960. The OCSP URL is referenced in the AIA extension of the Subscribers' certificates issued by the TS Timestamping CA.

2.3 Time or Frequency of Publication

The TS PKI GB reviews this CPS at least once annually and makes appropriate changes so that the Issuing CAs' operations remain fully aligned to the requirements listed in section 1 of this CPS. In instances where no changes are required, the CPS version number is incremented, and a dated changelog entry is included to document the review.

Modified versions of the CPS and terms and conditions of use (Subscriber and Relying party) are published within five days (05) after the TS PKI GB approval.

2.3.1 CA Certificate

The Subordinate CAs' and OCSP certificates are published to the public repository once they are issued until they are expired or rekeyed and the new certificates are issued.

2.3.2 CRLs

This CA maintain and publish CRLs as follows:

- A new CRL is generated every 24 hours, even if no changes have occurred since the last CRL issuance.
- CRL lifetime is set to 26 hours.

2.4 Access Controls on Repositories

The information published in the TS public repository is publicly available being guaranteed unrestricted access to read.

TS implements measures regarding logical and physical security to prevent unauthorized persons from adding, erasing, or modifying entries from the repository.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of names

This CA follow the standard X.500 distinguished names that must be unique and meaningful.

The Subject names in the CA certificate comply with the X.500 distinguished names standards. The subject name used is verified and validated by the RA function of the PMA, shall be meaningful, and shall never be reassigned to another entity.

This CA are identified in the Issuer's name field of the subscriber certificates as follows:

CN	TS TSA CA G1
O	Technology Source
Country – "C"	IQ

The certificates issued by this CA contain X.500 Distinguished Names (DN) as follows:

TSA Service Certificate for Document Signing:

Attribute	Value
CN	DS Timestamping
OrganizationID	An identification of the organization different from the organization name
O	Technology Source
Country – "C"	IQ

TSA Service Certificate for Code Signing:

Attribute	Value
CN	CS Timestamping
OrganizationID	An identification of the organization different from the organization name
O	Technology Source
Country – "C"	IQ

Timestamp CA OCSP Responder Certificate:

Attribute	Value
CN	**TS TSA CA G1 OCSP**
O	Technology Source
Country – "C"	IQ

3.1.2 Need for Names to be Meaningful

The TSA issuing CA enforces meaningful names as follow:

For certificates issued to TSA services: Distinguished Names (DN) are used to identify the service in a meaningful way.

For OCSP responder certificate: name is meaningful since it indicates the Subordinate CA's OCSP certificate responder name.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous or pseudonymous subscribers are not permitted.

3.1.4 Rules for Interpreting Various Name Forms

The naming convention used by this CA is based on ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.5 Uniqueness of Names

As per section 3.1.1 of this CPS, this CA enforces uniqueness through unique system common names that guarantees the uniqueness of DNs.

Name uniqueness is not violated when multiple certificates are issued to the same entity.

3.1.6 Recognition, Authentication, and Role of Trademarks

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

This CA have the right to revoke a Certificate upon receipt of a properly authenticated order from TS PKI GB or court of competent jurisdiction requiring the revocation of a Certificate or Certificates containing a Subject name in dispute.

3.2 Initial Identity Validation

The TS Timestamping CA does not issue certificates to any legal person other than Technology Source. The TS RA and TS PKI administrator oversee the issuance of TS TSA service certificates as well as the OCSP responder certificate as part of the authorized internal operational ceremonies under the supervision of TS PK GB.

3.2.1 Method to Prove Possession of Private Key

Not applicable.

3.2.2 Authentication of Organization Identity

Not applicable.

3.2.2.1 DBA/Tradename

Not applicable.

3.2.2.2 Verification of Country

Not applicable.

3.2.3 Authentication of Individual Identity

Not applicable.

3.2.4 Non-Verified Subscriber Information

Not applicable.

3.2.5 Validation of Authority

Not applicable.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Identification and authentication for re-keying is performed as in initial registration (section 3.2).

3.3.2 Identification and Authentication for Re-Key After Revocation

Identification and authentication for re-keying is performed as in initial registration (section 3.2).

3.4 Identification and Authentication for Revocation Request

Identification and authentication for revocation request is performed as in initial registration (section 3.2).

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

The TS Timestamping CA does not issue certificates to any legal person other than Technology Source. The TS RA and TS PKI administrator oversee the issuance of TS TSA

service certificates as well as the OCSP responder certificate as part of the authorized internal operational ceremonies under the supervision of TS PK GB.

4.1.1 Who Can Submit a Certificate Application

Not applicable.

4.1.2 Enrolment Process and Responsibilities

Not applicable.

4.2 Certificate Application Processing

The TS Timestamping CA does not issue certificates to any legal person other than Technology Source. The TS RA and TS PKI administrator oversee the issuance of TS TSA service certificates as well as the OCSP responder certificate as part of the authorized internal operational ceremonies under the supervision of TS PK GB.

4.2.1 Performing Identification and Authentication Functions

Not applicable.

4.2.2 Approval or Rejection of Certificate Applications

Not applicable.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

The TS Timestamping CA does not issue certificates to any legal person other than Technology Source. The TS RA and TS PKI administrator oversee the issuance of TS TSA service certificates as well as the OCSP responder certificate as part of the authorized internal operational ceremonies under the supervision of TS PK GB.

4.3.1 CA Actions During Certificate Issuance

Not applicable.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Not applicable.

4.4 Certificate Acceptance

The TS Timestamping CA does not issue certificates to any legal person other than Technology Source. The TS RA and TS PKI administrator oversee the issuance of TS TSA

service certificates as well as the OCSP responder certificate as part of the authorized internal operational ceremonies under the supervision of TS PKI GB.

4.4.1 Conduct Constituting Certificate Acceptance

Not applicable.

4.4.2 Publication of the Certificate by the CA

Both TSU certificates as well as the OCSP responder certificate are published on the TS public repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Note applicable.

4.5 Key Pair and Certificate Usage

4.5.1 TSA Service Private Key and Certificate Usage

The TS TSA service pledges to use the Certificate in accordance with:

- Only using certificates for legal and authorized purposes in accordance with the common general requirements applicable to the TSP CP and this CPS,
- Protect the private key (and related secrets) from compromise, loss, disclosure, or otherwise from unauthorized use,
- Not using the certificate outside its validity period, or after it has been revoked.
- Avoid using the private key until after the CA has issued the certificate.
- No longer use the private key after the validity period of the certificate expires, or when a certificate has been revoked.

4.5.2 Relying Party Public Key and Certificate Usage

A party relying on a certificate issued by the TS Timestamping CA shall:

- Use software that is compliant with X.509 and applicable IETF PKIX standards to validate the certificate signature and validity period,
- Validate the certificate by using the CRL, or the OCSP validity status information service in accordance with the certificate path validation procedure,
- Trust the certificate only if it has not been revoked and is within the validity period,
- Trust the certificate only for the signing of the RFC 3161 compliant timestamp tokens.

4.6 Certificate Renewal

Not applicable.

4.6.1 Circumstance for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable

4.6.3 Processing Certificate Renewal Requests

Not applicable

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable

4.7 Certificate Re-Key

Certificate Re-key is the process of issuing a new certificate to the subscriber with a new public key and validate period while the other information in the certificate may remain same.
The re-key of the TS TSA certificates is supported by the TS Timestamping CA. The re-key process is like the initial certificate application.

4.7.1 Circumstance for Certificate Re-Key

Certificate re-key may happen while the certificate is still active, after it has expired, or after a revocation. The re-key operation may invalidate any existing active TS TSA certificates.

4.7.2 Who May Request Certification of a New Public Key

As per the initial certificate issuance.

4.7.3 Processing Certificate Re-Keying Requests

As per the initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per the initial certificate issuance.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As per the initial certificate issuance.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per the initial certificate issuance.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per the initial certificate issuance.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

Suspension of a certificate is not allowed by TS Timestamping CA. Only permanent certificate revocation is allowed.

The TS Timestamping CA does not issue certificates to any legal person other than Technology Source. Revocation of TS TSA certificates or OCSP responder certificate may be triggered by a compromise or suspected compromise of the related private keys which shall

be considered by the TS as a disaster and treated as such in conformance with the TS disaster recovery and business continuity plan.

4.9.1 Circumstances for Revocation

4.9.1.1 Circumstances of Subscriber certificates revocation

Not applicable.

4.9.1.2 Circumstances of Subordinate CA revocation

The TS Timestamping CA Certificate will be revoked within seven (7) days if one or more of the following occurred:

1. The revocation is requested in writing;
2. Technology Source notifies the Issuing CA (i.e., Root CA) that the original certificate request was not authorized and does not retroactively grant authorization;
3. Technology Source obtains evidence that the TS Timestamping CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
4. The Issuing CA (i.e., Root CA) obtains evidence that the TS Timestamping CA Certificate was misused;
5. The Issuing CA (i.e., Root CA) is made aware that the TS Timestamping CA Certificate was not issued in accordance with or that TS Timestamping CA has not complied with this document.
6. The Issuing CA (i.e., Root CA) determines that any of the information appearing in the TS Timestamping CA Certificate is inaccurate or misleading;
7. TS Timestamping CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. TS Timestamping CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the (i.e., Root CA) has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's (i.e., Root CA) Certificate Policy and/or Certification Practice Statement.

4.9.2 Who Can Request Revocation

Not applicable.

4.9.3 Procedure for Revocation Request

Not applicable.

4.9.4 Revocation Request Grace Period

Not applicable.

4.9.5 Time within which CA Must Process the Revocation Request

Not applicable.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties are solely responsible for performing revocation checking on all Certificates in the chain before deciding whether to rely on the information in a Certificate. The TS Timestamping CA provides revocation status via mechanisms that are embedded in the TS TSA service certificates i.e. CRL and OCSP.

4.9.7 CRL Issuance Frequency (if applicable)

CRLs shall be issued as per Section 2.3 of this CPS.

4.9.8 Maximum Latency for CRLs (if applicable)

CRLs are issued timely by the TS Timestamping CA as per the CRL issuance frequency listed in section 4.9.7 of this CPS.

4.9.9 Online Revocation/Status Checking Availability

The TS Timestamping CA offers an OCSP responder that conforms to RFC 6960.The OCSP responder avails information immediately to relying party applications based on the CA actions on issued certificates.

The OCSP certificate contains an extension of type id-pkix-ocsp-nocheck, and ocspSigning EKU as defined by RFC 6960.

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

4.9.10 Online Revocation Checking Requirements

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

For the status of Subscriber Certificates:

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

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

The TS Timestamping CA monitors the OCSP responder for requests for "unused" serial numbers as part of its security monitoring procedures and any such case will trigger further investigation by relevant teams from TS operations team.

4.9.11 Other Forms of Revocation Advertisements Available

The TS Timestamping CA only uses OCSP and CRL as methods for publishing certificate revocation information.

4.9.12 Special Requirements Related to Key Compromise

If TS discovers, or has a reason to believe, that there has been a compromise of the private keys of the TS Timestamping CA, TS TSA certificates or OCSP responder certificate, TS will immediately declare a disaster and invoke its business continuity plan. TS will also:

- determine the scope of certificates that must be revoked,
- revoke impacted certificates within 24 hours and publish online CRLs within 30 minutes of creation,
- use reasonable efforts to notify government entities, subscribers and potential relying parties that there has been a key compromise, and
- generate new CA key pair as per TS operational policies and procedures.

4.9.13 Circumstances for Suspension

Not applicable

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure For Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable

4.10 Certificate Status Services

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

4.10.1 Operational Characteristics

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

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

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

4.10.2 Service Availability

The public repository where certificate information and CRLs are published is accessible 24 hours a day and 7 days a week and guarantees an uptime for at least 99.6% over one year period.

The TSA Timestamping CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

No applicable.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Facility, Management, and Operational Controls

This section specifies the physical and procedural security controls implemented by Technology Source within its operations.

The TS PKI GB security management program complies with the CA/Browser Forum's Network and Certificate System Security Requirements, including:

- Physical security and environmental controls,
- System integrity controls, including configuration and change management, patch management, vulnerability management and malware/virus detection/prevention,
- Maintaining an inventory of all assets and manage the assets according to their classification,
- Network security and firewall management, including port restrictions and IP address filtering,
- User management, separate trusted-role assignments, education, awareness, and training, and
- Logical access controls, activity logging and monitoring, and regular user access review to provide individual accountability.

Technology Source's security program includes an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes.

2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that Technology Source has in place to counter such threats.

Based on the Risk Assessment, Technology Source develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan also takes into account available technology and the cost of implementing the specific measures and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical Security Controls

The TS PKI GB ensures that appropriate physical controls are implemented at the TS PKI hosting facilities. Such controls are documented as part of TS's internal policies that are enforced and verified regularly through internal audits performed by the TS PKI GB on the TS PKI operations team.

5.1.1 Site Location and Construction

All critical components of the PKI solution are housed within a highly secure facility operated by the Technology Source. Physical security controls are enforced so that access of unauthorized persons is prevented through four tiers of physical security. When this layered access control is combined with the physical security protection mechanisms such as guards, intrusion sensors and CCTV, it provides robust protection against unauthorized access to the TS PKI systems.

The computing facilities that host the Technology Source CA services are located in Baghdad, Iraq.

5.1.2 Physical Access

The Technology Source CA systems are protected by multi-tiered (four tiers) physical security measures, with access to the lower tiers only possible by first gaining access through the higher tiers. Sensitive CA operational activities related to certificate lifecycle management occur within very restrictive physical tiers. The access control system implemented record the passage of people through each zone (i.e., tier)

Physical security controls include security guard-monitored building access, biometric authentication, and CCTV monitoring, protect the CA systems from unauthorized access, these controls are monitored on a 24x7x365 basis, forming multiple layers of protection for individuals entering and exiting the premises.

Access to the premises is granted upon presentation of the individual's National Citizens ID card, which is verified by the security guard, this includes monitoring and registering pertinent information including the person's identity, time of arrival and departure, and provides a visitor badge. Entry is not allowed unless the persons have been duly authorized by a member of the PKI Board and must be escorted by one from TS's trusted employees.

Further, access to the enclave (cage) where the CA systems are hosted is enabled only if two trusted employees are present to open the enclave's door.

5.1.3 Power and Air Conditioning

The design of the facility hosting the TS PKI provides UPS and backup generators with enough capability to support the PKI systems operations in power failure circumstances. UPS units and stand-by generators are available for the entire facility.

A fully redundant air-conditioning system is installed in the areas hosting the PKI systems. All these systems ensure that the PKI equipment continuously operate within the manufacturers' range of operating temperatures and humidity.

5.1.4 Water Exposures

The TS PKI GB has taken reasonable precautions to minimize the impact of water exposure on the TS PKI hosting facility. These include installing the TS PKI equipment on anti-static floors with moisture detectors.

5.1.5 Fire Prevention and Protection

The TS PKI hosting facility follows leading practices and applicable safety regulations in Iraq, monitored 24x7x365 and equipped with fire and heat detection equipment.

Fire suppression equipment is installed within dedicated areas and automatically activates in the case of fire, and can be manually activated, if necessary.

5.1.6 Media Storage

Electronic, optical, and other storage media are subject to the multi-tiered physical security and are protected from accidental damage (water, fire, electromagnetic interference).

Audit and backup storage media are stored in a secure fire-proof safe and duplicated and stored in the disaster recovery location.

5.1.7 Waste Disposal

All wastepaper and storage media created within the secure facility shall be destroyed before discarding. Paper media shall be shredded using a crosshatch shredder. The following procedure applies for removable computer media:

- Authorization shall be granted for the destruction of any removable computer media.
- The media shall be erased then physically destroyed if no longer required.
- Record of this media destruction shall be maintained.
- Media can then be released for disposal.

Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal.

5.1.8 Off-Site Backup

Full and incremental backups of the TS Timestamping CA systems are routinely performed to ensure ample recovery data is available should the need arise to restore the TS Timestamping CA systems.

At least one full backup and several incremental backups of the TS Timestamping CA's online systems are taken daily in accordance with documented backup policies and procedures followed by the TS PKI operations team.

Backups of the most critical information (e.g., Private Keys), is taken at the end of any key ceremony in accordance with a documented key ceremony script.

Adequate back-up facilities ensure that backup copies are transferred to the disaster recovery location where they are stored with the same physical, technical and procedurals controls that apply to the primary facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

All members of the staff operating the key management operations, administrators, and security officers or any other operations that materially affect such operations are considered as serving in a trusted position (i.e., trusted operatives)

All personnel appointed in a trusted position have their background check before they are allowed to work in such position. The background check shall be maintained and reviewed annually.

The following are the trusted roles for the TS Timestamping CA:

- **PKI Administrator**: Owning the credentials of the CA software. Responsible for configuring and maintaining the CA.
- **PKI Operator:** Authorized to execute the CA operational cycle and is involved in critical operations such as subscribers' certification operations.
- **Security Officer:** Owning credentials that enable configuring the HSMs and PKI policies on the target systems subject to key generation during relevant key ceremony.
- **RA Officer:** Responsible for verifying information that is necessary for certificate issuance and approval of certification requests .
- **M-of-N Custodians:** Owners of the HSM activation data. Custodians of the Subordinate CAs' safes.
- **CA Domain Owner:** Owning the credential that authorizes Subordinate CA HSM backup and restore operations.
- **HSM Auditor:** Owning the credentials for retrieving the HSM audit logs.
- **Data Centre Custodians:** Personnel who has the credentials for opening the PKI datacentre while performing the CA operations.
- **System Administrator:** Authorized to install, configure, troubleshoot, and maintain the supporting operating system and database environment.

- **Network Administrator:** Authorized to install, configure, troubleshoot, and maintain the supporting network equipment.

5.2.2 Number of Persons Required per Task

The TS PKI operations follow rigorous control procedures to ensure the segregation of duties, based on job responsibility, to prevent single trusted personnel to perform sensitive operations.

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

- Physical access to the secure enclave where the TS Timestamping CA's systems are hosted,
- Access to and management of CA cryptographic hardware security module (HSM),
- Validate and authorize the issuance of certificates.
- All operational activities performed by the personnel having trusted roles are logged and maintained in a verifiable and secure audit trail.

5.2.3 Identification and Authentication for each Role

Before exercising the responsibilities of a trusted role:

- The TS PKI GB confirms the identity and history of the employee by carrying out background and security checks.
- When instructed through the internal TS PKI processes, the facility operations team issues an access card to each staff who needs to physically access equipment located in the secure enclave.
- TS PKI dedicated staff (system administrators) issue the necessary ICT system credentials for the TS Timestamping CA staff to perform their respective functions.

5.2.4 Roles Requiring Separation of Duties

The trusted roles listed in section 5.2.1 are established with the appropriate segregation of duties.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

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

- Verify the Identity of Such Person: Verification of identity MUST be performed through:

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

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

The TS PKI GB provides essential technical training for its personnel to effectively carry out their duties. This training is regularly updated and conducted annually for TS Timestamping CA personnel.

The training program encompasses a diverse range of topics and is delivered by a combination of experienced TS Timestamping CA staff and third-party experts specializing in security and PKI. It is meticulously designed to cater to the specific requirements of various trusted roles involved in managing and delivering TS Timestamping CA services. The topics covered in the training are:

- PKI theory and principles
- PKI environmental controls and security policies
- PKI RA processes including vetting and verification procedures.
- PKI operational processes
- PKI products hands-on training
- PKI trusted roles management
- PKI disaster recovery and business continuity procedures

The TS PKI GB maintains comprehensive documentation of all personnel who have undergone training and regularly assesses the satisfaction levels of the trainers. At the end of each training session, examination tests are organized, and certificates are awarded to staff who pass these tests. It is mandatory for all trusted roles, including validation specialists, to pass these examinations before being authorized to operate as trusted role.

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

The TS PKI GB ensures that any change or rotation in staff shall not affect the operational effectiveness, continuity, and integrity of the TSA Issuing CA services.

5.3.6 Sanctions for unauthorized actions

To maintain accountability on the TS PKI staff members, the TS PKI GB sanctions personnel for unauthorized actions, and unauthorized use of authority and unauthorized use of systems, according to the relevant human resources policy and procedures, and the applicable Iraqi law.

5.3.7 Independent contractor requirements

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

- Criminal convictions for serious crimes,
- Misrepresentations by the candidate,
- Appropriateness of references,
- Any clearances as deemed appropriate,
- Privacy protection, and
- Confidentiality conditions.

5.3.8 Documentation supplied to personnel

The TS PKI GB shall document all training material and make it available to the TS PKI staff.

The TS PKI GB shall also ensure that the key operational documentation is made available to the relevant staff members. This includes, at a minimum, this CPS document, security policies, operational guides, and technical documentation relevant to every trusted role.

5.4 Audit Logging Procedures

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

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

officer team and are also subject to review as part of the regular internal audits performed by the TS compliance function on the TS Timestamping CA operations.

5.4.1 Types of Events Recorded

5.4.1.1 Types of events recorded for CAs

Audit logs are generated for all events relating to the security and services of the TS Timestamping CA's systems.

Technology Source records events related to its actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. Technology Source makes these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

At a minimum, each audit record includes the following:

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

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

Following events occurring in relation to the TS Timestamping CA's operations are recorded:

1. TS Timestamping CA key life cycle management events, including:
    - Key generation, backup, storage, recovery, archival and destruction;
    - Cryptographic device life-cycle management events.
    - Certificate requests, renewal, and re-key requests, and revocation;
    - Approval and rejection of Certificate requests;
    - Generation of CRLs;
    - Signing of OCSP responses; and
    - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. TS Timestamping CA and TS Timestamping CA Subscriber Certificates life-cycle management events, including:
    - Certificate requests, re-key requests, and revocation;

- All issued certificates including revoked and expired Certificates;
- Verification activities evidence (e.g., date, time, calls, persons communicated with);
- Acceptance and rejection of certificate requests;
- Issuance of certificates;
- CRL updates (including OCSP entries updates where applicable).
- Signing of OCSP responses.

3. Security events, including:
   - Successful and unsuccessful PKI system access attempts;
   - PKI and security system actions performed;
   - Relevant router and firewall activities (as described in Section 5.4.1.3); and
   - Security profile changes;
   - System platform issues (e.g. crashes), hardware failures, and other anomalies
   - Installation, update and removal of software on a Certificate System;
   - Entries to and exits from the CA facility.

The TS PKI GB also ensures that the following information, not produced by the TS Timestamping CA is maintained (either electronically or manually) by the TS operations team:

- CA personnel, security profiles rotations/changes;
- All versions of this CPS;
- Minutes of meetings;
- Compliance internal audit reports;
- Current and previous versions of TS Timestamping CA configuration and operations manuals.

5.4.1.2 Types of events recorded for Timestamp Authorities

In addition, TS Timestamping CA MUST log the following information and make these records available to its Qualified Auditor as proof of the Timestamp Authority's compliance with these Requirements:

1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
2. History of the timestamp server configuration,
3. Any attempt to delete or modify timestamp logs,

4. Security events, including:
    a. Successful and unsuccessful Timestamp Authority access attempts;
    b. Timestamp Authority actions performed;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies; and
    e. Relevant router and firewall activities (as described in Section 5.4.1.3); and;
5. Revocation of a timestamp certificate
6. Major changes to the timestamp server's time, and
7. System start-up and shutdown

5.4.1.3 Router and firewall activities logs

Router and firewall activities logged include:

1. Successful and unsuccessful login attempts to routers and firewalls; and

2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and

3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and

4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts

5.4.2 Frequency of Processing Log

The TS PKI GB ensures that designated personnel review log files at regular intervals to validate log integrity and ensure timely identification of anomalous events. At a minimum, the following audit log review cycle is implemented by the TS PKI GB:

- Audit and Security logs of the CA applications shall be reviewed by the Monitoring & Compliance team on monthly basis,
- Audit and Security of the online CA systems (Ex. OCSP responder) shall be reviewed by the Monitoring & Compliance team on monthly basis to validate the integrity of the logging processes and to test/confirm the daily monitoring function is being operated properly,
- Physical access logs and the user management on the TS PKI systems shall be reviewed by the Monitoring & Compliance team on quarterly basis to validate the physical and logical access policies,
- The TS PKI GB audit and compliance function executes an internal audit on the TS Timestamping CA operations on yearly basis. Samples of the log review reports and

collected audit logs since the last audit cycle shall be requested by the TS PKI GB as part of this internal audit.

- Evidence of audit log reviews, outcome of the review process, and executed remediation actions are collected and archived.

5.4.3 Retention Period for Audit Log

The TS operations team ensures that the audit logs are maintained and retained for a period not less than 2 years or in accordance with section 5.5.2:

1. CA certificate and key lifecycle management event records (as set forth in Section5.4.1.1 (1)) after the later occurrence of:
    1. The destruction of the CA Private Key; or
       the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 basicConstraints extension with the cA field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1.1 (2)) after the revocation or expiration of the Subscriber Certificate;
3. Timestamp Authority data records (as set forth in Section 5.4.1.2) after the revocation or renewal of the Timestamp Certificate private key;
4. Any security event records (as set forth in Section 5.4.1.1 (3) and for Timestamp Authority security events set forth in section 5.4.1.2 (4)) after the event occurred.

5.4.4 Protection of Audit Log

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

1. The TS Timestamping CA systems generates cryptographically protected audit logs,
2. The security of audits logs is maintained while these logs transit by the backup system and when these logs are archived,
3. The access control policies enforced on the TS PKI systems ensures that read access only is granted to personnel having access to audit logs as part of their operational duties,
4. Only authorized roles can obtain access to systems where audit logs are stored and any attempts to tamper with audit logs can be tracked to the respective TS Timestamping CA staff.

5.4.5 Audit Log Backup Procedures

Incremental backups and full backups are performed periodically. Additionally, the following rules apply for the backups of the TS Timestamping CA audit log:

- Backup media are stored locally in the TS Timestamping CA main site, in a secure location;
- A second copy of the audit log data and files are stored in the disaster recovery site that provides similar physical and environmental security as the main site.

5.4.6 Audit Collection System (Internal vs. External)

Automatic audit processes are initiated at system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, the TS PKI GB determines whether to suspend the relevant CA's operations until the problem is fixed.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

The TS PKI operations conduct an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes,
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that TS has in place to counter such threats.

The TS PKI systems and infrastructure shall be also subject to regular security assessment as follows:

- Within one (1) week of receiving a request from the CA/Browser Forum
- After any system or network changes that the CA determines are significant, and
- at least every three (3) months, on public and private IP addresses identified of TS Timestamping CA's core and supporting PKI system. This regular self-assessment activity is executed by security personnel part of the TS PKI operations team.

On an annual basis, and after infrastructure or application upgrades or modifications that the TS PKI GB determines are significant, the TS PKI GB coordinates a third-party independent vulnerability assessment and penetration testing is conducted on the TS PKI systems.

The outcome of the regular assessments and identified issues shall be made available to the TS PKI GB and PKI operations management, who shall be responsible for organizing and oversee the execution of the remediation's by the respective teams.

Evidence of the vulnerability assessment and penetration testing activities execution are collected and archived by the relevant TS Timestamping CA's staff.

5.5 Records Archival

5.5.1 Types of Records Archived

The TS Timestamping CA shall archive all audit logs (as set forth in Section 5.4.1) in addition to the following:

1. Documentation related to the security of CA systems, and certificate managements Systems, and
2. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

5.5.2 Retention Period for Archive

The TS Timestamping CA retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, as well as all documentation related to the security of the CA system for 7 years after any certificate issuance by the TS Timestamping CA and based on that documentation ceases to be valid.

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

Only one version of each digital archive is maintained in the primary and disaster recovery facilities of this CA. The TS PKI operations team use backup, restore, and archive procedures that document how the archive information is created, transmitted, and stored.

5.5.5 Requirements for Timestamping of Records

All recorded and archived events include the date and time of the event taking place. The time of TS Timestamping CA online systems is synchronized with the time source of a GPS clock. The time-stamping services setup reaches an accuracy of the time of +/-1s or better with respect to UTC.

Further, the PKI operations team enforce a procedure that checks and corrects any clock drift.

5.5.6 Archive Collection System (Internal or External)

The TS Timestamping CA archive collection system is internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized and authenticated staff shall be allowed to access archived material. The TS PKI operations team use the TS Timestamp CA backup, restore, and archive procedures that document how the archive information is created, transmitted, and stored. These procedures also provide information on the archive collection system.

5.6 Key Changeover

To minimize impact of key compromise, the TS Timestamping CA key shall be changed with a frequency that ensures the TS Timestamping CA shall have a validity period greater than the maximum lifetime of Subscriber certificate after the latest Subscriber certificate issuance.

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

To support revocation management of issued certificates, the old CA private keys are maintained until all of the Certificates signed with the Private Key have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If a potential hacking attempt or other form of compromise to the TS Timestamping CA is detected by the TS PKI GB, it shall perform an investigation to determine the nature and the degree of damage:

- If a CA Private key is suspected of compromise, the procedures outlined in the TS's Business continuity and disaster recovery plan shall be followed. Otherwise, the scope of potential damage shall be assessed to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised,
- The TS PKI GB also specifies applicable compromise reporting and relevant communications as part of the Business continuity and disaster recovery plan,

Apart from the circumstance of key compromise, the TS specifies the recovery procedures used when computing resources, software, and/or data are corrupted or suspected of being corrupted.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

TS shall implement the necessary measures to ensure full recovery of the TS Timestamping CA services in case of a disaster, corrupted servers, software, or data. That is subject to the TS PKI GB authorization to trigger incident recovery procedures.

The TS Timestamping CA disaster recovery and business continuity document specifies the circumstances imply triggering of incident recovery procedures that may involve the disaster recovery location if required.

The TS Timestamping CA disaster recovery and business continuity plan is tested at least once a year, including failover scenarios to the disaster recovery location.

5.7.3 Entity Private Key Compromise Procedures

For Subscribers key compromise, see section 4.9.

Compromise of the TS Timestamping CA private key(s), the associated activation data, or the OCSP responder certificate is considered as a mission-critical incident that triggers a process and related procedures, detailed in the TS disaster recovery and business continuity plan.

Considering the criticality of such compromise situation and its impact on Iraq National PKI, the TS PKI GB holds an emergency meeting to take decisions and handles communications as required as part of the Key compromise and CA termination plans. Refer to sections 4.9.1 and 4.9.3 for further details.

5.7.4 Business Continuity Capabilities after a Disaster

In case of a disaster, corrupted servers, software or data, the TS disaster recovery and business continuity plan is triggered to restore the minimum required operational capabilities of the TS Timestamping CA, in a timely fashion. In particular, the plan targets the recovery of the following services, either on the main site, or the disaster recovery location:

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

Failover scenarios to the TS disaster recovery location are made possible considering the TS Timestamping CA backup system that enables the continuous replication of critical data from the main site to the disaster recovery site. That allows a recovery of the TS Timestamping CA critical services at the disaster recovery location within a maximum of twelve (12) hours RTO.

The TS business continuity plan defines the following:

- The conditions for activating the plan,
- Emergency procedures,
- Fallback procedures,
- Resumption procedures,
- A maintenance schedule for the plan;
- Awareness and education requirements;
- The responsibilities of the individuals;

- Recovery time objective (RTO);
- Regular testing of contingency plans.
- The plan to maintain or restore the TS Timestamping CA business operations in a timely manner following interruption to or failure of critical business processes.
- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location.
- What constitutes an acceptable system outage and recovery time.
- How frequently backup copies of essential business information and software are taken.
- The distance of recovery facilities to the main site; and
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either ate the original or a remote site.

Technology Source does not disclose business continuity plans to Subscribers, Relying Parties, or to Application Software Suppliers, but will provide business continuity plan and security plans to the auditors upon request.

5.8 CA or RA Termination

The provision of the TS Timestamping CA services are terminated:

a) Following a TS's Executive Management decision
b) with a justifiable decision of the authority exercising supervision (ITPC)
c) with a final and irrevocable judicial decision
d) upon the liquidation or termination of the operations of TS Timestamping CA.

If the TS PKI GB and/or the ITPC PMA determine that termination of the TS timestamping CA services is deemed necessary, the TS PKI GB shall perform a termination plan that should have been previously agreed with the ITPC PMA.

The TS termination plan covers the below minimum aspects:

- Provide a written notice to the ITPC PMA of its intention to cease operating its CA activities, together with a copy of the TS's termination plan, at least ninety (90) days before:
  - the date when it will cease to the CA related activities,
  - expiry, when applicable, of TS's authorization for providing its CA activities, where TS has no intention to apply for an authorization renewal.
- TS arrangement for the retention of archived logs (as set forth in Section 5.5),
- The TSP arrangement for maintaining the validation status services URLs as mentioned in the certificates that would still be valid for the applicable period after termination,

- Advertisements about TS intention to terminate its TS Timestamping CA activities within at least sixty (60) days before effective termination or the expiry of its authorization, whichever occurring first, in daily newspapers, or by such other mediums and in the manner the ITPC PMA may determine,
- Communications towards relevant parties and for transferring archived TS Timestamping CA records to an appropriate custodian,
- Plan to assist (as much as possible) TS's subscribers with a transition to another TSP,
- Revoke all certificates, issued by this CA, that remain unrevoked or unexpired at the end of the notice period, whether the subscribers have requested a revocation.
- Undertake the necessary measures to ensure that discontinuing its operations does not cause disruption to its subscribers and relying parties.
- Arrangements to adequately ensure the ongoing maintenance of its systems and security measures for sensitive and accurate data.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The TS Timestamping CA key pair is generated within the memory of an HSM certified evaluated to FIPS 140-2 Level 3.

The TS Timestamping CA Key Generation Ceremonies are video recorded and stored securely for auditing purposes.

The TS Timestamping CA Key Generation Ceremonies are witnessed by an internal/external auditor with the aim to produce a report opinion that TS:

1. Documented its CA key generation and protection procedures in compliance with this CPS and the TSP CP,
2. Included appropriate detail in its CA Key Generation Script,
3. Executed in the in presence of a quorum of authorized personnel including representatives from the TS PKI GB,
4. Maintained effective controls to provide reasonable assurance that the CA key pair was generated and protected in conformity with the procedures described in this CPS, the applicable CPS,
5. Performed, during the CA key generation process, all the procedures required by its CA Key Generation Script.

6.1.1.2 Subscribers

Not applicable.

6.1.2 Private Key Delivery to Subscriber

The CA does not generate Subscribers' private keys nor does it perform key escrow, recovery, or backup.

If the CA detects or suspects that the Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA revokes all Certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3 Public Key Delivery to Certificate Issuer

The public key to be certified is transmitted to the CA in the form of CSR, to guarantee the integrity and source of this key.

6.1.4 CA Public Key Delivery to Relying Parties

The CA public key certificates are published on the TS public repository.

6.1.5 Algorithm Type and Key Sizes

6.1.5.1 TS Timestamping CA

The TSA Timestamping CA uses 348-bit ECDSA.

6.1.5.2 Subscribers

Subscriber keys are 3072-bit RSA or 4096-bit RSA (recommended).

6.1.6 Public Key Parameters Generation and Quality Checking

6.1.6.1 TS Timestamping CA

The CA private and public keys generation is done with state-of-the-art parameter generation. The TS Timestamp CA HSM and associated software meet FIPS 186-2 requirements for random generation and primality checks. The TS PKI operations team references the Baseline Requirements Section 6.1.6 on quality checking.

6.1.6.2 Subscribers

Not applicable.

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

Certificates issued by this CA contain a key usage bit string in accordance with [RFC 5280]. Refer to section 7.1 and 7.3 of this CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

For the creation and storage of the TS Timestamping CA private keys, FIPS 140-2 Level 3 certified/compliant hardware security modules are used. The HSMs are stored within the most secure and inner zone of the TS PKI hosting facility.

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

The TS Timestamping CA private keys are continuously controlled by multiple authorized persons, trusted roles in relation to the CA' private keys (and related secrets) management are documented in the TS Timestamping CA KGC procedures, and other internal documentation.

The TS Timestamping CA staff are assigned to the trusted roles by the TS PKI GB ensuring segregation of duties and enforcing the principles of multi control and split knowledge.

Multi-person control of the TS Timestamping CA private keys is achieved using an "m-of-n" split key knowledge scheme. A certain number of persons 'm' (at least two (2)), out of 'n' persons (three (3) persons), the total number of key custodians, need to be concurrently present, together with HSMs administrators to activate or re-activate the CA private key.

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

6.2.3 Private Key Escrow

Private keys of the TS Timestamping CA are not escrowed.

6.2.4 Private Key Backup

The TS Timestamping CA private keys are backed up and held stored safely in exclusive safes maintained in the most inner security zones of the TS Timestamping CA hosting facility.

Backup operations are executed as part of the TS Timestamping CA key generation ceremonies. The TS Timestamping CA keys are backed up under the same multi-person control and split knowledge as the primary key. The recovery operation of the backup key is subject to the same multi-person control and split knowledge principles.

The TS Timestamping CA private keys that are physically transported from the primary facility to the DR one using a dedicated HSM handling and key handling procedure part of the overall TS Timestamping CA key ceremony procedures. Dedicated personnel in trusted roles participate in the transport operation, which is escorted by security guards. Refer to Section 6.2.2 for further details.

6.2.5 Private Key Archival

The TS PKI GB does not archive the CA private keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The TS Timestamping CA key pairs shall only be transferred to another hardware cryptographic token of the same specification as described in 6.2.11 by direct token-to-token copy via trusted path under multi-person control.

6.2.7 Private Key Storage on Cryptographic Module

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

6.2.8 Method of Activating Private Key

CA and TSU Private keys are activated following the principles of dual control and split knowledge. The activation procedure shall use a PIN entry device attached to the hardware security module (i.e., HSMs).

6.2.9 Method of Deactivating Private Key

Private keys for the CA and TSU are deactivated in accordance with the instructions and documentation provided by the manufacturer of the hardware security module.

6.2.10 Method of Destroying Private Key

Destruction of the CA private key, outside the context of its scheduled end-of-life, shall require formal authorization by multiple members of the TS PKI Governance Body (TS PKI GB).

The destruction process follows documented procedures and must involve individuals assigned to trusted roles—a minimum of three trusted staff members, with the presence of at least one representative from the PKI GB. Additionally, the destruction must be witnessed by a qualified auditor.

For TSU private keys, the corresponding private keys are removed from the HSM within 18 months following the issuance of the certificate. The removal of the private key from the HSM is conducted via a key deletion ceremony performed by Technology Source and witnessed and signed off by at least two Trusted Role members.

Technology Source may also perform a key destruction ceremony, ensuring that all copies of the private key—including any backups—are irrevocably and securely destroyed, rendering recovery impossible. This satisfies requirements for total private key elimination.

6.2.11 Cryptographic Module Rating

The TS Timestamping CA cryptographic modules are certified/validated against [FIPS 140-2] Level 3.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

See clause 5.5 for archival conditions.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The TS Timestamping CA certificates are valid for six (06) years, with a key usage period of Three (03) years.

The Subordinate CA private key is not used after the validity period of the associated public key certificate. Additionally, it is not used to sign end-entity certificates after the private key usage period, except for CRLs and OCSP responder certificates for the certificate validity status service.
Each TSU has one active time-stamp signing key active at a time which is generated every 12 months.

6.4 Activation Data

6.4.1 Activation data generation and installation

6.4.1.1 TS Timestamping CA

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

6.4.1.2 Subscribers

Not applicable.

6.4.2 Activation Data Protection

6.4.2.1 TS Timestamping CA

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

6.4.2.2 Subscribers

Not applicable.

6.4.3 Other Aspects of Activation Data

No Stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Technology Source ensures that computer security controls are implemented in compliance with technical standards and vendor security hardening guidelines as a minimum. Implemented computer security controls are documented as part of the TS Timestamping CA internal policy documentation.

In particular, the CA systems and its operations are subject to the following security controls:

1. Separation of duties and dual controls for CA operations
2. Physical and logical access control enforcement
3. Audit of application and security related events
4. Continuous monitoring of the TS Timestamping CA systems and end-point protection
5. Backup and recovery mechanisms for the TS Timestamping CA operations
6. Hardening of TS Timestamping CA servers' operating system according to leading practices and vendor recommendations

7. In-depth network security architecture including perimeter and internal firewalls, web application firewalls, including intrusion detection systems.
8. Proactive patch management as part of the TS Timestamping CA operational processes
9. The TS Timestamping CA systems enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer Security Rating

The technical aspects of computer security are subject to periodic audits.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Purchased hardware or software are to be shipped in a sealed, tamper-proof container, and installed by qualified personnel. Hardware and software updates are to be procured in the same manner as the original equipment. Dedicated trusted personnel are involved to implement the required TS timestamping CA configuration according to documented operational procedures.

Applications are tested, developed, and implemented in accordance with industry leading development and change management practices. No software (or patches), or hardware is deployed on live systems before going through the change and configuration management processes enforced by the TS PKI operations team.

All the TS timestamping CA hardware and software platforms are hardened using industry best practices and vendor recommendations.

6.6.2 Security Management Controls

The hardware and software used to set up the CA shall be dedicated to performing only CA-related tasks. There shall be no other applications, hardware devices, network connections or component software, which are not part of the TS PKI, connected to or installed on CAs' hardware.

A configuration management process is enforced to ensure that TS CAs systems configuration, modification and upgrades are documented and controlled by the TS PKI operations management. Technology Source system configurations are regularly checked, with a maximum interval of one week between checks.

A vulnerability management process is enforced to ensure that the CA equipment is scanned for malicious code on first use and periodically thereafter.

6.6.3 Life Cycle Security Controls

Refer to 6.5.1.

6.7 Network Security Controls

TS implemented strong network security, including managed firewalls and intrusion detection systems. The network is segmented into several zones, based on their functional, logical and physical relationship. Network boundaries are applied to limit the communication between systems (within zones) and communication between zones, with rules that support only the services, protocols, ports, and communications that the CA have identified as necessary to its operations, disabling all accounts, applications, services, protocols, and ports that are not used in the CAs' operations.

Issuing Systems, Certificate Management Systems, and Security Support Systems are protected within a highly Secure network Zone.

Vulnerability scans of networks are conducted at least quarterly, and penetration tests are performed at least annually. Remediation timelines are based on severity: critical vulnerabilities are addressed within 24 hours, high vulnerabilities within 48 hours, while low- and medium-severity issues are resolved within 96 hours. Any exceptions are documented, risk-assessed, and formally recorded.

6.8 Timestamping

The TS Timestamping CA's components are regularly synchronized using a reliable time service. The time-stamping services setup reaches an accuracy of the time of +/-1s or better with respect to UTC.

Technology Source operates a TSA service in support of document signing and Code signing. The TS Timestamping Policy and Practice Statement specifies the policy requirements relating to the operation of TS TSA. It shall be read in conjunction with this CPS. Both documents can be downloaded from https://pki.techsource.iq

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

TS Timestamping CA issues X.509 version 3 certificates as defined in RFC 5280

7.1.2 Certificate Extensions

The TS Timestamping CA issue certificates with X.509 v3 extensions as defined in RFC 5280 in addition to extensions indorsed by the CA/Browser Forum.

The Subordinate CA and TSU (Time Stamp Unit) certificates include a Certificate Policy Extension. TS may use its CA's own policy and/or a number of suitable policy identifiers introduced within the scope of:

- ETSI EN 319 421 (Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Timestamps
- Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

The TSU certificates contain Extended Key Usage Extension which is set critical and include id-kp-timeStamping as KeyPurposeID.

7.1.3 Algorithm object identifiers

Certificates are issued with algorithms indicated by the following OIDs

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

7.1.4 Name Forms

7.1.4.1 Name Encoding

Technology Source issues TSU Certificates with name forms compliant to ETSI EN 319 422 for certificates issued for document signing.

Technology Source issues TSU Certificates with name forms compliant to Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates for certificates issued for code signing.

7.1.4.2 Subject Information - Subscriber Certificates

The applicable subject information for TSU certificates is specified in the table below. Technology Source issues certificates to TSUs where the contents of the Subject DN fields are compliant with their corresponding requirements stated in section 6 of ETSI EN 319 422.

Certificate Type	Subject DN
DS TSU Certificate	• commonName • organizationName • organizationIdentifier • countryName
CS TSU Certificate	• commonName • organizationName • organizationIdentifier • countryName

7.1.5 Subject Information - Root Certificates and Subordinate CA Certificates

For Root CA and Subordinate CA certificates, commonName, organizationName and countryName attributes are present and the combination of these contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.

7.1.6 Name Constraints

No stipulation.

7.1.7 Certificate Policy Object Identifier

TS uses an OID scheme specified for the Iraqis National PKI Policy. Refer to the following certificate template for more details.

Following Object Identifier is also used for Timestamping certificates issued for code signing**:**

End entity certificate policies	
2.23.140.1.4.2	BR CS Reserved OID (TSA)

7.1.8 Usage of Policy Constraints Extension

No stipulation.

7.1.9 Policy Qualifiers Syntax and Semantics

TS Certificates issued to TSUs contain a CPS Policy Qualifier that points to the applicable CPS.

7.1.10 Processing Semantics for The Critical Certificate Policies Extension

No stipulation.

7.1.11 TS Timestamping CA Certificate Profile

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Root CA Signature	Root CA's signature value
TBSCertificate					
Version	False	M	S		
Version		M	S	2	Version 3
SerialNumber	False	M	D		
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M	S		
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer	False	M	S	<Root CA's Subject>	The issuer field is defined as the X.501 type "Name"

CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Informatics & Telecommunications Public Company	UTF8 encoded
CommonName		M	S	ITPC TSA Root CA G1	UTF8 encoded
Validity	False	M	D		Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[72]** Months	Suggested validity for the subordinate certificate is up to 06 years
Subject	False				
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Technology Source	UTF8 encoded
CommonName		M	S	TS TSA CA G1	UTF8 encoded

SubjectPublicKeyInfo		False	M	D		
	AlgorithmIdentifier		M	D	ECDSA (OID: 1.2.840.10045.2.1) secp384r1 (OID: 1.3.132.0.34)	
	SubjectPublicKey		M	D	Value of the key	
Extensions						
Authority Properties						
AuthorityKeyIdentifier		False	M	D		Mandatory in all certificates except for self-signed certificates
	KeyIdentifier		M	D	160-bit SHA-1 Hash of the Root CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess		False	M	S		
	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	http://ocsp.itpc.gov.iq	OCSP responder URL
	AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		M	S	http://pki.itpc.gov.iq /repository/cert/tsa_root_ca.p7b	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M	S		

	DistributionPoint		M	S	http://pki.itpc.gov.iq /repository/crls/tsa_root_ca.crl	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M	D		
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties						
keyUsage		True	M	S		
	keyCertSign, cRLSign		M	S	True	
ExtendedKeyUsage		False	M			
	id-kp-timeStamping		M	S	True	
Policy Properties						
certificatePolicies		False	M	S		
	PolicyIdentifier		M	S	2.23.140.1.4.2	CA/B BR Reserved Certificate Policy for Timestamping
certificatePolicies		False	M	S		
	PolicyIdentifier		M	S	2.16.368.1.1.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	S	https://pki.itpc.gov.iq /repository/cps	
Basic Constraints Properties						
basicConstraints		True	M	S		
	cA		M	S	True	
	pathLenConstraint		M	S	0	

7.1.12 End Entity Certificates

7.1.12.1 TS DS TSU Certificate Profile

CE[2] = Critical Extension O/M[3]: O = Optional M = Mandatory
CO[4] = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Subordinate CA Signature.	Subordinate CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer	False	M		<Subordinate Issuing CA's Subject>	The issuer field is defined as the X.501 type "Name"
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2

					code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Technology Source	UTF8 encoded
CommonName		M	S	TS TSA CA G1	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject	False				
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	Technology Source	UTF8 encoded
OrganizationIdentifier		M	D	An identification of the organization different from the organization name	UTF8 encoded
CommonName		M	D	A name commonly used by the subject to represent itself. It must uniquely identifies the TSU	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA	

	SubjectPublicKey		M	D	Public Key Key length: 3072 or 4096 (RSA)	
Extensions						
Authority Properties						
AuthorityKeyIdentifier		False	M			Mandatory in all certificates except for self-signed certificates
	KeyIdentifier		M	D	160-bit SHA-1 Hash of the subordinate issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess		False	M			
	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	http://ocsp.techsource.iq	OCSP responder URL
	AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		M	S	http://pki.techsource.iq/repository/certs/tsa_ca.p7b	Subordinate Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/tsa_ca.crl	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			

	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties						
keyUsage		True	M			
	nonrepudiation		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.5	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.6	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/tsaps	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.6.1	timestamps issued in support of document signing signature.
Extended Key Usage Properties						
extendedKeyUsage		True	M			
	timeStamping		M	S	True	
Private Key Usage Period		False	M			

	GeneralizedTime		M	D	notBefore notAfter	This extension indicates the period of use of the private key corresponding to the certified public key. A new Key pair will be generated each 12 months

7.1.12.2 TS CS TSU Certificate Profile

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	Subordinate CA Signature.	Subordinate CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer	False	M		<Subordinate Issuing CA's Subject>	The issuer field is defined as the X.501 type "Name"
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Technology Source	UTF8 encoded
CommonName		M	S	TS TSA CA G1	UTF8 encoded

Validity		False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
	NotBefore		M	D	Certificate generation process date/time.	
	NotAfter		M	D	Certificate generation process date/time + **[36]** Months	Suggested validity for the end user certificate is up to 3 years
Subject		False				
CountryName			M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName			M	D	Technology Source	UTF8 encoded
OrganizationIdentifier			M	D	An identification of the organization different from the organization name	UTF8 encoded
CommonName			M	D	A name commonly used by the subject to represent itself. It must uniquely identifies the TSU	UTF8 encoded
SubjectPublicKeyInfo		False	M			
	AlgorithmIdentifier		M	D	RSA	
	SubjectPublicKey		M	D	Public Key Key length: 3072 or 4096 (RSA)	
Extensions						
Authority Properties						
AuthorityKeyIdentifier		False	M			Mandatory in all certificates except for self-signed certificates

	KeyIdentifier		M	D	160-bit SHA-1 Hash of the subordinate issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess		False	M			
	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	http://ocsp.techsource.iq	OCSP responder URL
	AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		M	S	http://pki.techsource.iq/repository/certs/tsa_ca.p7b	Subordinate Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://pki.techsource.iq/repository/crls/tsa_ca.crl	CRL download URL.
Subject Properties						
SubjectKeyIdentifier		False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties						
keyUsage		True	M			
	Digital signature		M	S	True	
Policy Properties						
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.5	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	

	policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/cps	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.6	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	S	https://pki.techsource.iq/repository/tsaps	
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.6.2	timestamps issued in support of code signing signature.
certificatePolicies		False	M			
	PolicyIdentifier		M	S	2.23.140.1.4.2	BR CS Reserved OID (TSA)
Extended Key Usage Properties						
extendedKeyUsage		True	M			
	timeStamping		M	S	True	
Private Key Usage Period		False	M			
	GeneralizedTime		M	D	notBefore notAfter	This extension indicates the period of use of the private key corresponding to the certified public key. A new Key pair will be generated each 12 months

7.2 CRL Profile

CE[2] = Critical Extension O/M[3]: O = Optional M = Mandatory
CO[4] = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
CertificateList		M			
TBSCertificate					
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	The signature of the CA issuing the CRL.	The signature of the authority issuing the CRL.
TbSCertList					
Version	False	M			
Version			S	1	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer	False	M			
CountryName		M	S	IQ	
OrganizationName		M	S	Technology Source	
CommonName		M	S	TS TSA CA G1	
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime

	thisUpdate		M	D	<creation time>	
	NextUpdate		M	D	<Creation time> + [1] day + 2 hours	
RevokedCertificates		False	M			
	CertificateSerialNumber		M	D	Serial of the revoked certificates	
	revocationDate		M	D	Date when revocation was processed by the CA	UTC time of revocation
	crlEntryExtension	False	M			
	reasonCode		M	D	As per BR 7.2.2	Identifies the reason for the certificate revocation
CRLExtensions		False	M			
	AuthorityKeyIdentifier	False	M	D	160-bit SHA-1 hash of the public key of the CA issuing the CRL	
	CRL Number	False	M	D		Sequential CRL Number
	expiredCertsOnCRL	False	M	D		< contains the date on which the CRL starts to keep revocation status information for expired certificates>

7.2.1 Version Number(s)

TS Timestamping CA supports X.509 version 2 CRLs (see 7.2 above)

7.2.2 CRL and CRL Entry Extensions

The profile of the CRL is provided in section 7.2 above.

7.3 OCSP Profile

The OCSP profile complies with the requirements of RFC 6960.

CE[2] = Critical Extension O/M[3]: O = Optional M = Mandatory
CO[4] = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
SignatureValue		M	D	CA's Signature.	CA's Signature.
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.10045.4.3.3	SHA384 with ECDSA Encryption
Issuer	False	M		<Subject of the CA issuing the OCSP Certificate>	The issuer field is defined as the X.501 type "Name"
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements".

					PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Technology Source	UTF8 encoded
CommonName		M	S	TS TSA CA G1	UTF8 encoded
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + [12] months	**Validity period** is 12 months for OCSP Certificates
Subject	False	M			
CountryName		M	S	IQ	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Technology Source	UTF8 encoded
CommonName		M	S	TS TSA CA G1 OCSP	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		M			
Subject Properties					
SubjectKeyIdentifier	False	M			

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

OCSP response format

The below profile describes OCSP response according to RFC 6960:

Field	Value	Comment
responseStatus	"0" Response has valid confirmations	Result of the query. If the value of responseStatus is other than "0", the responseBytes field is not set.
responseBytes		
responseType	id-pkix-ocsp-basic	
BasicOCSPResponse		
tbsResponseData		
version	1	Version of the response format
responderID	C = IQ O = <The full registered name of the subject> CN = <A name commonly used by the subject to represent itself>	Distinguished name of the OCSP responder. The information MUST correspond to the certificate that was used to sign the response.
producedAt		The time at which the OCSP responder signed this response.
responses		
certID		In accordance with RFC 6960
hashAlgorithm	Depending on the hash algorithm used in request	hashAlgorithm is the hash algorithm used to generate the issuerNameHash and issuerKeyHash values. Supported hash algorithms are SHA-1, SHA-256, SHA-384 and SHA-512.
issuerNameHash		Hash of issuer's DN
issuerKeyHash		Hash of issuer's public key
SerialNumber		CertificateSerialNumber
certStatus		Status of the certificate: • Good – certificate issued and has not been revoked. • Revoked – certificate is revoked. • Unknown – the certificate is unrecognized by this OCSP responder.
thisUpdate		The most recent time at which the status being indicated is known by the responder to have been correct.
nextUpdate	• ThisUpdate + 8 hours	The time at or before which newer information will be available about the status of the certificate

ArchiveCutoff[3]	• the CA's certificate "notBefore" time and date value	According to RFC 6960 clause 4.4.4. "archive cutoff" date set to the CA's certificate "notBefore" time and date value According to ETSI EN 319 411-2 / CSS-6.3.10-10.
extended-revoked definition	Null	the responder supports the extended definition of the "revoked" status to also include non-issued certificates
signatureAlgorithm	Sha384withRSAEncryption	Signing algorithm
signature		signature value
certs		Certificate corresponding to the private key used to sign the response. Only OCSP responder certificate is included in the OCSP response.

7.3.1 Version Number(s)

As per the OCSP certificate profile, section 7.3.

7.3.2 OCSP Extensions

As per the OCSP certificate profile, section 7.3.

depicted in Figure 1.
mentation of the OCSP, the ''ArchiveCutoff'' extension is included in OCSP responces only for certificates that have expired

8 Compliance Audit and Other Assessments

The procedures outlined in this CPS are intended to align with the requirements specified in Section 1 and cover all applicable elements of current PKI standards relevant to the industry sectors in which Technology Source operates.

8.1 Frequency or Circumstances of Assessment

Technology Source shall organize an external WebTrust audit to ensure that it meets applicable requirements, standards, procedures, and service levels at least on an annual basis.

Technology Source accepts this auditing of its own practices and procedures and makes the audit report publicly available no later than three months after the end of the audit period. The TS PKI GB and the ITPC PMA evaluate the results of such audits before further implementing them.

In addition, internal audits are conducted according to an audit plan approved by the PMA. Under special circumstances (I.e. a security breach) unplanned audits and assessments may be conducted on request of the PMA.

8.2 Identity/Qualifications of Assessor

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

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

8.3 Assessor's Relationship to Assessed Entity

For internal audit, the TS PKI GB has its own audit function that is independent of the TS PKI operations team. External auditors are independent third party WebTrust practitioners.

8.4 Topics Covered by Assessment

This CA is audited for compliance to the following standards:

- WebTrust Principles and Criteria for Certification Authorities.
- WebTrust Principles and Criteria for Certification Authorities – Network Security.
- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements.

Refer to section 8.1 for the periodicity of the audits. Refer to section 8.2 for the assessor's qualifications.

8.5 Actions Taken as a Result of Deficiency

Issues and findings resulting from the assessment are reported to the TS PKI GB as well as the TS PKI GB.

Regarding compliance audits of TS Timestamping CA operations, any notable exceptions or deficiencies discovered during the audit process prompt a decision on necessary actions. This decision is made by the TS PKI GB with input from the auditor. Should exceptions or deficiencies arise, TS PKI GB assumes responsibility for formulating and executing a corrective action plan. Following implementation of the plan, TS PKI GB initiates an additional audit to ensure that identified deficiencies have been carried out.

8.6 Communication of Results

The internal audit reports are communicated to the TS PKI GB and shall not be disclosed to non-authorized third parties.

Annual WebTrust Audit Reports are made publicly available no later than three (3) months after the end of the audit period. If there is a delay greater than three (3) months, Technology Source will provide an explanatory letter signed by the Qualified Auditor. Technology Source's WebTrust audit reports can be found at:
https://pki.techsource.iq/repository/ar/index.html .

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Not applicable.

9.1.2 Certificate Access Fees

Not applicable.

9.1.3 Revocation or Status Information Access Fees

Not applicable.

9.1.4 Fees for Other Services

Not applicable.

9.1.5 Refund Policy

Not applicable.

9.2 Financial responsibility

9.2.1 Insurance Coverage

Technology Source ensures that the TS Timestamping CA is covered by existing insurance provisions.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

Refer to 9.6.1.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

TS considers the following as confidential information:

- Contractual agreements between TS and its suppliers.
- TS internal documentation (business processes, operational processes…).
- Employees confidential information.

9.3.2 Information not within the Scope of Confidential Information

Any information not defined as confidential by TS shall be deemed public. This includes the information published on the TS public repository.

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Technology Source observes personal data privacy rules and confidentiality rules as specified in the present CPS. The Technology Source implements these provisions through the TS RA.

Refer to section 9.4.2 for the scope of private information and to section 9.4.3 for the items that are not considered as private information.

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

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

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

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

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

9.4.2 Information Treated as Private

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

9.4.3 Information not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

The TS PKI staff, suppliers and contractors handle personal information in strict confidence under TS contractual obligations that at least as protective as the terms specified in Section 9.4.1.

9.4.5 Notice and Consent to Use Private Information

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

No stipulation

9.5 Intellectual Property Rights

Technology Source owns and reserve all intellectual property rights associated with its own databases, websites, the CAs' digital certificates and any other publication whatsoever originating from the PKI, including this CPS.

When TS uses software from third party suppliers, this software remains the intellectual property of the product suppliers, and its usage by TS CAs bound by license agreements between TS and these suppliers.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

By issuing a Certificate, the TS Time Stamping CA makes the certificate warranties listed herein to the Relying Parties who reasonably rely on a Valid Certificate.

Technology Source represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the TS Time Stamping CA has complied with the Baseline Requirements and its CPS in issuing and managing the Certificate.

- **Accuracy of Information:** That, at the time of issuance, TS implemented a procedure for verifying the accuracy of all of the information contained in the Certificate according to this CPS and the Baseline requirements.
- **Status:** That TS maintains a 24 x 7 publicly accessible public repository with current information regarding the status (valid or revoked) of all unexpired Certificates.
- **Revocation:** That TS will revoke the Certificate for any of the reasons specified in these Requirements.
- **Compliance:** The Timestamping CA has complied with the Baseline Requirements for Code Signing and the applicable Certificate Policy and Certification Practice Statement in issuing each TSA Certificate and operating its PKI.

9.6.2 RA Representations and Warranties

Not applicable.

9.6.3 Subscriber Representations and Warranties

Not applicable.

9.6.4 Relying Party Representations and Warranties

Relying Parties who rely upon the certificates issued under TS shall:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension)
- Verify the validity by ensuring that the certificate has not expired.
- Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 version 3 amendment.
- Ensure that the certificate has not been revoked by accessing current revocation status information available at the location specified in the certificate to be relied upon; and
- Determine that such certificate provides adequate assurances for its intended use.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

Within the scope of the law of Iraq, and except in the case of fraud, or deliberate abuse, TS cannot be held liable for:

- The accuracy of any information contained in certificates except as it is warranted by the subscriber that is the party responsible for the ultimate correctness and accuracy of all data transmitted to TS with the intention to be included in a CA certificate,
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificates or digital signatures,
- Willful misconduct of any third-party participant breaking any applicable laws in Iraq, including, but not limited to those related to intellectual property protection, malicious software, and unlawful access to computer systems,
- For any damages suffered whether directly or indirectly because of an uncontrollable disruption of the TS Timestamping CA services,
- Any form of misrepresentation of information by the subscribers or relying parties on information contained in this CPS or any other documentation made public by the TS PKI GB and related to the TS Timestamping CA services.

9.8 Limitations of Liability

- TS assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under this CPS for any use other than in accordance with this document,
- TS will not be liable to any party whosoever for any damages suffered whether directly or indirectly because of an uncontrollable disruption of its services,
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations; and
- TS denies any financial or any other kind of responsibility for damages or impairments resulting from the TS Timestamping CA operations.

9.9 Indemnities

Not applicable.

9.10 Term and Termination

9.10.1 Term

The present CPS is approved by the TS PKI GB and shall remain in force until amendments are published on the TS public repository.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

The TS PKI GB will communicate the conditions and effect of this CPS termination via appropriate mechanisms.

9.11 Individual Notices and Communications with Participants

Notices related to this CPS can be addressed to the TS PKI GB contact address as stated in section 1.5.

9.12 Amendments

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

9.12.1 Procedure for Amendment

Refer to Section 9.12

9.12.2 Notification Mechanism and Period

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

The TS PKI GB coordinates communication in relation to the amendments of this CPS and related effects.

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

9.12.3 Circumstances under which OID Must be Changed

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

9.13 Dispute Resolution Provisions

All disputes associated with the provisions of this CPS and the TS Timestamping CA services, shall be first addressed by the TS PKI GB legal function. If mediation by the TS PKI GB legal function is not successful, then the dispute shall be adjudicated by the relevant courts of Iraq.

9.14 Governing Law

The laws of the republic of Iraq shall govern the enforceability, construction, interpretation, and validity of this CPS.

9.15 Compliance with Applicable Law

This CPS and provision of TS Timestamping CA services are compliant to relevant and applicable laws of the Republic of Iraq.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate rights or duties under this CPS, without the prior written consent of TS.

9.16.3 Severability

If any provision of this CPS is determined to be invalid or unenforceable, the other sections shall remain in effect until this CPS is updated.

In the event of a conflict between the Baseline Requirements and any regulation in Iraq, the TS may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in Iraq.

This applies only to operations or certificate issuances that are subject to that Law. In such event, the TS will immediately (and prior to issuing a certificate under the modified requirement) include in this section a detailed reference to the Law requiring a modification of the Baseline Requirements under this section, and the specific modification to the Baseline Requirements implemented by the TS.

The TS will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS. Any modification to the TS practice enabled under this section will be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CPS and a notice to the CA/Browser Forum, as outlined above, is made within 90 days.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation

9.16.5 Force Majeure

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

9.17 Other Provisions

Note Applicable.