TECHNOLOGY SOURCE

SMART.SPEED.SOLUTIONS

# Iraq National PKI

## TLS CA

## Certificate Practice Statement

## Document Control

| Prepared / Updated By | Reviewed By | Approved By | Owner | Version | Date of Approval |
|---|---|---|---|---|---|
| | | | Technology Source | 0,7 | |

## Change History

| Ver. No | Date | Changes Description | |
|---|---|---|---|
| **0.1** | 08/02/2023 | Initial version | Touir Mustapha |
| **0.2** | 23/02/2023 | Internal review and update | Ahmad Ibrahim |
| **0.3** | 05/07/2023 | Update in section 3.2.2.1<br>Update sections 7.1.10.2 & 7.1.10.3.2 to accommodate section 9.2 of the EV guidelines. | Touir Mustapha |
| **0.4** | 29/11/2023 | Removing EV certificate from the scope<br>Adding OIDs values, Contact information, Repository URL<br>Applying Technology Source Template | Touir Mustapha |
| **0.5** | 28/02/2024 | Reviewing and updating based on auditor's feedback on Root CA CP/CPS and TSP CP. | Touir Mustapha, Yasir Khan |
| **0,6** | 28/04/2024 | Update in section 5.4.1 to accommodate section 5.4.1 of the latest BR SSL v 2.0.4 | Touir Mustapha |
| **0,7** | 15/05/2024 | Reviewing and updating based on auditor's feedback on CPSs | Touir Mustapha<br>Yasir Khan |

## Document Approval

| Ver. No | Approver (Name/Title) | Signatures |
|---|---|---|
| 0,7 | PKI GB Director | <br>Date: |

# 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) TLS CA. This CPS complies with the TSP Certificate Policy that is applicable to the provision of certification services offered by 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 TS TLS CA that are established and operated by Technology Source 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 this CA:

- **Web server TLS certificates (OV) -** used for server authentication and session data encryption.
- **OCSP responder certificate** - Used to sign the Online Certificate Status Protocol (OCSP) responses for certificates issued by the TS TLS CA.

This CPS complies with the formal requirements of the Internet Engineering Task Force (IETF) RFC 3647 with regards to format and content. While certain section titles are included according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of this CA. Such sections are denoted as “Not applicable”.  Additional information is presented in subsections of the standard structure where required.

The TS’s PKI GB 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 TLS Server Certificates.
- 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.

This CPS is a public document. 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 section 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) Root Certification Authorities (CAs) are established for the different type of certificates to be issued by the Subordinate CAs. The Informatics & 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:

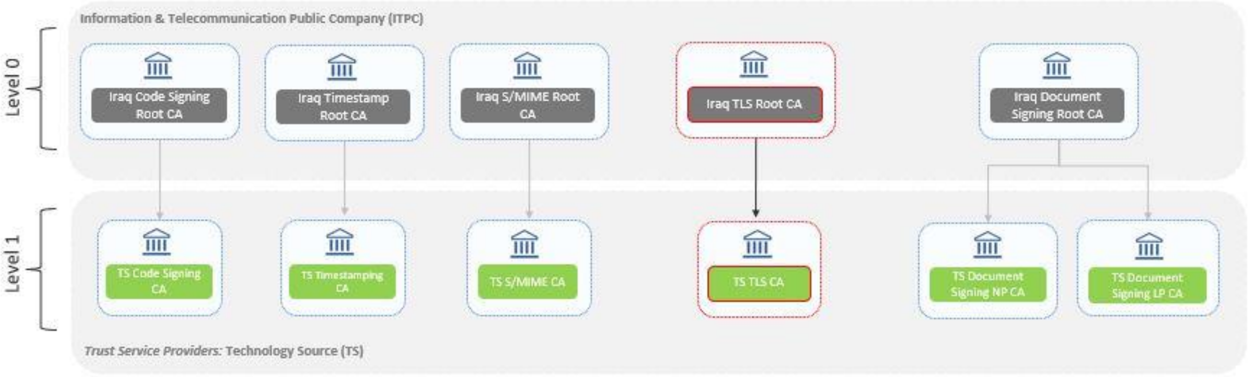
Information & Telecommunication Public Company (ITPC)
Level 0
Iraq Code Signing Root CA
Iraq Timestamp Root CA
Iraq S/MIME Root CA
Iraq TLS Root CA
Iraq Document Signing Root CA
Level 1
TS Code Signing CA
TS Timestamping CA
TS S/MIME CA
TS TLS CA
TS Document Signing NP CA
TS Document Signing LP CA
Trust Service Providers: Technology Source (TS)

*Figure 1 Iraq National PKI hierarchy*

[1] For TLS server certificates, only the Iraq TLS Root CA is relevant since it signs the TLS Subordinate CA certificate of Technology Source. Other Root CAs belongs to the Iraqi PKI but aren't pertinent to TLS server certificates issuance and are not included in the TLS 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 validated (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 (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 Subordinate CAs.

### 1.1.1 Technology Source PKI Governance Board (TS PKI GB)

The Governance board governing the Technology Source PKI (including the TS TLS 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 to:

- Define and maintain the TS PKI strategy,

[2] For TLS server certificates, only the TS TLS CA is pertinent, as it will issue web server TLS organization validated (OV) certificates. Other subordinate CAs belong to the Technology Source PKI but are not relevant for TLS server certificate issuance and are not part of the TLS hierarchy as depicted in Figure 1.

- 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 "**Technology Source TLS CA Certificate Practice Statement**" which is identified by the OID **2.16.368.1.2.1.3** and referenced in related documents as [**TS TLS CA CPS**].

The TS TLS CA includes the above mentioned OID in the CP extension of the certificates it issues to indicate compliance with the current CPS.

## 1.3 PKI Participants

### 1.3.1 Certification Authorities

The TS TLS CA (hereinafter, CA) is owned and operated by Technology Source through its premises in Iraq. This CA has been approved by the ITPC and signed by the Iraq TLS 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, CRL 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 always reflects the current status of the certificates issued by this CA.

### 1.3.2 Registration Authorities

A Registration Authority (RA) is the entity that performs the identification and authentication of certificate applicants for end-user certificates, initiates, or forwards revocation requests, and approves applications for certificate issuance and renewal on behalf of the CA.

Technology Source operates its own Registration Authority (RA) function and does not rely on Delegated Third Parties for RA functions. The RA function primarily processes TLS certification requests for certificates issued to the legal organizations.

The RA function falls within the PKI operations structure. TS RA officers are responsible for identity validation and certificate request management for government and non-government entities according to the procedures outlined in section 4.2.

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 with this CA 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).

Technology Source does not delegate the validation process of domain ownership or control to any third-party RA. This process is performed only by RA officers team of Technology Source.

### 1.3.3 Subscribers

Subscribers encompass Iraqi legal entities, including government entities, non-government entities, and even Technology Source itself, falling under Iraqi jurisdiction. They apply for OV (organization validated) SSL Certificates from the TS TLS CA and commit to adhere to the applicable Subscriber Agreement.

### 1.3.4 Relying Parties

Relying Parties must consistently refer to Technology Source's Certificates Validity Status Service (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 auditor who verifies the requirements set out in section 8.2.

## 1.4 Certificate Usage

### 1.4.1 Appropriate Certificate Uses

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

1) **Web Server TLS certificates**:

    a) **(Organization validated) OV Certificates:** Used for server authentication and session data encryption.

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

### 1.4.2 Prohibited Certificate Uses

Subscribers are authorized to use their certificates for the purposes specified in section 1.4.1 of this CPS. The use of certificates for any other purposes 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-maamon high school**
**Email:** muhanad.ali@techsource.iq
**Phone no.:** +9647726695600 / +9647842002124

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

**Certificate Problem Report**
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 Info@techsource.iq

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

### 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 is approved by the TS PKI GB and 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 this 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.

To maintain credibility and promote trust in this CPS and better correspond to accreditation and legal requirements, the TS PKI GB reviews this CPS at least annually and makes revisions and updates to policies as it sees fit or as required by other circumstances.

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:** The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. In the context of this CPS, this CA issues certificates only to legal entities.

**Applicant Representative:** A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA. In the context of this 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.

**Attestation Letter:** A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information. In the context of this CPS, attestation letters are signed by Human Resource teams of entities.

**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. Section 7 of this CPS provides a list of the certificate profiles defined within it.

**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.

**Onion Domain Name:** A Fully Qualified Domain Name ending with the RFC 7686 ".onion" Special-Use Domain Name. For example, 2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an Onion Domain Name, whereas torproject.org is not an Onion Domain Name.

**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. In the context of this CPS, the RA function is operated by Technology Source.

**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. In the context of this CPS, the Iraqi Incorporating or Registration Agency  is the reliable data source for non-government entities in Iraq and the Iraqi official Gazette is the reliable data source for government entities.

**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.

**Short-lived Subscriber Certificate**: For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).

**Subject:** The entity, or organization defined in the “Subject” field in a Certificate.

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

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

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

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

**Technically Constrained Subordinate CA Certificate:** A Subordinate CA certificate which uses a combination of Extended Key Usage settings and/or 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.

**Top-level Domain:** A top-level domain is the last part of the text in a domain name like .com, .net or .org. In the context of this CPS, the top-level domain is ".IQ".

**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.

**WHOIS:** Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

### 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 | Informatics & Telecommunications 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 |
| TS | Technology Source |
| TLD | top-level domain |
| 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 |

# 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 agreements, PKI disclosure statement, 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 the 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 TLS 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 this CA.

Technology Source hosts test Web pages that allow application developers to test their developed software with Subscriber Certificates. Below are test Web pages for valid, revoked, and expired certificates:

| OV certificates | |
|---|---|
| **Valid certificates:** | https://good.techsource.iq |
| **Revoked certificates:** | https://revoked.techsource.iq |
| **Expired certificates:** | https://expired.techsource.iq |

## 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 Subordinate CAs' operations remain fully aligned to the requirements listed in section 1 of this CPS.
Modified versions of the CPS and agreements (Subscriber and Relying party) are published within five days after the TS PKI GB approval.

### 2.3.1 CA Certificates

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.

Technology Source 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

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

The TS TLS CA is identified in the Issuer's name field of the subscriber certificates as follows:

#### *3.1.1.1 TS TLS CA Certificate*

| | |
|---|---|
| **CN** | TS TLS CA G1 |
| **O** | Technology Source |
| **Country – "C"** | IQ |

Certificates issued by this CA uses Distinguished Names (DN) as specified in Recommendation ITU-T X.500 standards. The tables below specify the DN structures followed for each certificate types supported.

#### *3.1.1.2 Organization Validated (OV) Certificates:*

| Attribute | Value |
|---|---|
| **subjectAltName** | public IP or FQDNs or authenticated domains that are under the control of the Subscriber |
| ***O*** | full registered name of organization to which the certificate is issued |
| **Country – "C"** | IQ |
| **L (optional if S is present, otherwise mandatory)** | which is the city or locality of the organization's place of business. |
| **S (optional if L is present, otherwise mandatory)** | which is the state or province of the organization's place of business. |

#### *3.1.1.3 OCSP certificates:*

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

### 3.1.2 Need for Names to be Meaningful

The Certificates issued pursuant to this CPS are meaningful only if the names that appear in the Certificates can be understood and used by Relying Parties. Distinguished Names (DN) are used to identify both the subject and the issuer of the certificate in a meaningful way. Hence, this CA issues certificates to subscribers (subjects) that demonstrate legitimately ownership and control on the DN, domain names, IP addresses, mentioned in the Subject DN and Subject Alternative Names.

**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

Uniqueness is enforced by the use of registered public DNS name (FQDNs) or public IP addresses. the Subject Alternative Name (SubjectAltName) extension must be used to define the applicable domain and one or more additional domain names for the certificate. The usage of internal domain names and reserved IP addresses is prohibited.

**For OCSP responder certificate:** The OCSP responder unique name is included in the subject DN of issued OCSP certificate.

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

TS RA verifies and authenticates the identity and other attributes of an Applicant prior to inclusion of these attributes in a Certificate. TS RA may refuse to issue a Certificate at its sole discretion if identity validation is not successful.

### 3.2.1 Method to Prove Possession of Private Key

The Applicant provides a digitally signed PKCS#10 CSR to establish that it holds the private key corresponding to the public key to be included in the certificate. The TS RA systems enforce validation of the proof of possession of the private key as part of the certificate request processing. The proof of possession is submitted to the TS RA through CSRs in PKCS#10 format.

### 3.2.2 Authentication of Organization Identity and Domain Identity

#### *3.2.2.1 Identity*

The applicant's organizational identity is verified using reliable authoritative data sources, which are expected to provide details information about the entity including the entity's legal name, address, and Authorized representative's information.

Technology Source rely on the "**Iraqi Official Gazette**" or through other directs means of communication with the entity or jurisdiction governing the entity's legal creation, existence, or recognition for the verification of government entities information and on an approved official communication with the "**Iraqi Incorporating or Registration Agency**" for non-government entities.

Technology Source may require the applicant to submit official entity documentation to confirm the identity of the subject such as corporate charter, government issued tax document, Professional letter (Accountant letter or Legal opinion), or other relevant documents and may conduct a site visit to the entity to verify the entity's address.

Additionally, Technology Source validates the Applicant's right to use the Domain Name(s) that will be listed in the Certificate by following the procedures of Sec. 3.2.2.4.

The TS RA ensures that any obtained validation data will be recollected and validated not more than 398 days after the last performed verifications.

The TS RA verifies the association with the certificate subject by ensuring that the information provided in the application form must exactly match the information to be inserted in the certificate.

**Authority of the applicant**

TS RA verify the authority of the authorized representative and the certificate's requester (applicant representative) in accordance with section 3.2.5.

#### 3.2.2.2 DBA/Tradename

The use of DBA or Tradename in the Subject Identity Information is not supported by this CA.

#### 3.2.2.3 Verification of Country

This CA issues certificates only to organizations established in Iraq. TS RA verifies that the value of the "country" field of the Subject Identity Information is set to "**IQ**".

#### 3.2.2.4 Validation of Domain Authorization or Control

For each domain name to be included in the Certificate Subject, TS RA verifies the Applicant's control of the domain name in accordance with the Baseline Requirements, section 3.2.2.4, and maintains a record of the method used, using one of the following methods for each FQDN.

- Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing a unique Random Value (valid for no more than 30 days from its creation). The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact. (BR Section 3.2.2.4.2)
- Email validation consisting of sending an e-mail with a random, unique value (valid for no more than 30 days from its creation) to an administrative e-mail address associated with the domain name (i.e. admin@organization.iq). This validation may be performed using following e-mail addresses: admin@, administrator@, webmaster@, hostmaster@, postmaster@. (BR Section 3.2.2.4.4)
- Domain Name Service (DNS) change by confirming the presence of a unique random value or request token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character. (BR Section 3.2.2.4.7).

Technology Source don't issue TLS certificates to ".onion" domains.

#### 3.2.2.5 Authentication for an IP Address

Ownership of the IP Address (es) to be added in the certificate is verified through the following methods:

- **Agreed-Upon Change to Website:** Having the Applicant demonstrate control over the requested IP Address (es) by confirming the presence of a Random Value within a file under the "/well-known/pki-validation" directory on an Authorization IP Address that is accessible by the CA via HTTP/HTTPS over an Authorized Port. (BR Section 3.2.2.5.1).

- **Email to IP Address Contact**: Send a random value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the random value. The random value MUST be sent to an email address, fax/SMS number, or postal mail address identified as an IP Address Contact. The random value remains valid for use in a confirming response for no more than 3 days from its creation. (BR Section 3.2.2.5.2).
- **Reverse Address Lookup**: Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name using the supported methods. (BR Section 3.2.2.5.3).

#### *3.2.2.6 Wildcard Domain Validation*

Before issuing a certificate with a wildcard character (*) in the CN or subjectAltName, the following validations apply:

1. Wildcard SSL Certificates include a wildcard asterisk character as the first character in the Common Name (CN) attribute of the Subject field and or in the SubjectAltName extension;
2. The wildcard asterisk character must not fall within the label immediately to the left of a registry-controlled or public suffix;
3. Certificate issuance is accepted only if the applicant proves its rightful control of the entire Domain Namespace. (e.g. TS RA MUST NOT issue "*.co.iq" or "*.local", but MAY issue "*.example.iq" to Example entity).

#### *3.2.2.7 Data Source Accuracy*

Technology Source uses an internal process to check the accuracy of information sources and databases to ensure the data is acceptable. Prior to using any data source as a Reliable Data Source, the source is evaluated for its reliability, accuracy, and resistance to alteration or falsification.

#### *3.2.2.8 CAA Records*

As part of the certificate application processing, the TS RA checks the CAA records for the domains listed in the certificate application according to the procedure in RFC 8659.
The CAA is a special DNS record that a domain owner can configure to specify which CA is allowed to issue a certificate for that domain.

- If the CAA record is undefined or pointing towards the TS TLS CA, the TS RA will proceed with processing the certificate application. Whenever the 'issue' and 'issuewild' tags are present within a CAA record, the TS RA verifies that those tags contain the value "**pki.techsource.iq**" as granting authorization for issuance of the certificate by the TS TLS CA and will ensure that the certificate is issued within the Time to Live (TTL) of the CAA record, or 8 hours, whichever is greater.
- If the CAA record does not point towards the TS CA and points to another third-party CA, the TS RA rejects the certificate application and communicates accordingly with

the applicant representative so that the value "**pki.techsource.iq**" is added in the relevant DNS CAA entries. Since this DNS change may take time to propagate, the TS RA requests the applicant representative to wait few hours before resubmitting his certificate application. The TS RA does not use iodef property tag of the CAA record for communicating with the applicant.

The TS RA logs all actions taken in relation to CAA records checks and processing.

### 3.2.3 Authentication of Individual identity

This CA does not issue certificates to natural persons and issues only certificates for legal entities.

### 3.2.4 Non-Verified Subscriber Information

All fields constituting the subscriber information written in the certificate are verified by TS RA.

### 3.2.5 Validation of Authority

The organization's authorized representative nominates a certificate Requester (Applicant representative) from the organization who submits the certificate management requests with the TS RA. The identity of the Requester is verified by performing the following steps as minimum:

- The TS RA conducts an identity proofing through an in-person identity verification of the Requester against his/her government government-issued ID Card. The actual ID card (not a copy) is presented by the Requester,
- The TS RA uses the proof of employment (Attestation letter) received as part of the certificate application to validate the association between the Requester and the entity,
- The TS RA verifies the authenticity of the certificate application and the authenticity of the attestation letter directly with the entity authorized representative. A reliable method of communication is used involving the usage of the organization email addresses, and when deemed necessary by the TS RA an in-person meeting is organized.

The authorization to request certificates on behalf of the entity is verified based on the signed certificate request form both the Requestor and the authorized representative, that attests the authority of the requestor.

### 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 initial registration, in addition to the below rules:

- The TS RA application checks the existence and validity of the certificate to be re-keyed and that the information used to verify the identity and attributes of the subject is still valid.
- If any of the TS terms and conditions have changed, these will be communicated by the TS RA to the subscriber.

### 3.3.2 Identification and Authentication for Re-Key after revocation

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

## 3.4 Identification and Authentication for Revocation Request

The identification and authentication procedures of revocation requests involves a formal request from the authorized representative of the entity to which the certificate is issued. A revocation procedure is enforced by the TS RA. It encompasses:

- The signature of a revocation request form by an appropriately authorized representative.
- The verification of the identity of the requesters against the information available to the TS RA (provided during the subscriber registration)
- Communication with the entity to provide reasonable assurances that the entity's official representative authorized the revocation operation. Such communication, depending on the circumstances, may include one or more reliable method of communication such as telephone, e-mail or courier service.

**For OCSP responder certificate:** The present CPS does not specify detailed provisions for revoking any of these certificates. Such revocation may be triggered by a compromise or suspected compromise of the related private keys which is considered as a disaster and treated as such in conformance with the TS disaster recovery and business continuity plan.

# 4 Certificate Life-Cycle Operational Requirements

## 4.1 Certificate Application

### 4.1.1 Who Can Submit a Certificate Application

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

Technology Source does not issue Certificates to entities on an internal blacklist[3] of organizations from whom it will not accept certificate requests. This blacklist is queried by the TS RA team whenever it receives any certificate request.

**For OCSP responder certificate:** the TS RA and an authorized PKI administrator in trusted role oversee the execution of an internal operational ceremonies through which these certificates can be issued. They engage TS PKI GB for approving the operational ceremony documentation and for validating the embedded certificate templates and naming conventions against the provisions of this CPS. TS PKI GB authorizes the ceremony and confirms the list of involved trusted role staff.

### 4.1.2 Enrolment Process and Responsibilities

The CAs require each Applicant to submit a Certificate request and application information prior to issuing a Certificate. TS RA authenticates all communication from an Applicant and ensures that the application form is filled and signed as expected.

- The applicant downloads the certificate application form with the subscriber agreement from the public repository.
- The certificate application form is filed and signed by the authorized representative of the entity (likewise, the subscriber agreement must be ratified);
- The relevant technical team from the entity generates a key pair according to the requirements of this CPS then create a Certificate Signing Request (CSR) using the approved certificate fields in the application form (e.g., DN attributes, key size, key type etc.). This CSR is handed over to the authorized certificate requester.
- The requester authenticates to the Web RA portal (using multi-factor authentication credentials set up as part of the registration process outlined in an internal RA process document) and submits the certificate application including:

[3] An internal blacklist in where the TS RA logs previously rejected certificate requests due to suspected or fraudulent usage and revoked certificate requests from entities.

  - Scanned copy of properly filled and signed application form.
  - The information and documents required for identification and authorization of the subject request.
  - Certificate Signing Request (CSR) file.

Two (02) members from the TS RA team are required to issue an TLS certificate:

- The TS RA team reviews and validates the integrity and authenticity of all the submitted documents in addition to vetting the applicant identity as specified in section 3.2.2.
- The TS RA checks the blacklist of organizations from whom it will not accept certificate requests. This blacklist is queried by the TS RA team whenever it receives any certificate request.
- The TS RA team processes the certificate request. Refer to section 4.2.

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

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

**Applicable Requirements for all certificates applications:**

a) A unique ID is assigned to each certificate application record,

b) TS RA records all activities (e-mail communication, phone calls, vetting evidence) along with the certificate application record,

c) Any malicious certificate or revocation request or a request that fails multiple (more than 3) times is added to the TS RA's own blacklist, the blacklist includes the necessary details to avoid ambiguously in identifying future malicious requests,

d) TS RA conducts a blacklist check against its own blacklist. If the applicant is in the blacklist, the certification application is rejected,

**Applicable Requirements for TLS certificates applications:**

e) The TS RA sends to the applicant the necessary information including the documentation required for identity verification and the subscriber agreement once the request is initiated by the applying entity.

f) The Requester fills-in the Organization registration form as follows:

a. Organization Information
    i. Organization’s Legal Name
    ii. Official Address
    iii. Main telephone number

b. Authorized representatives Information:
    i. applicant representative information such as phone, official email address, position.

c. Requester information
    i. Name of and contact information of the Requester (the representative authorized to submit certificate management requests on behalf of the entity).

g) The applicant representative signs and ratifies a dedicated subscriber agreement.

h) An attestation letter issued by the entity HR establish the association between the Requester and the entity,

i) The Requester submits the signed registration form, the attestation letter as well as other validation documentation to TS RA via email,

j) The TS RA performs the following verification for each certificate request without relying on previously performed verifications:

- Validates the organization’s identity as described in section 3.2.2.1
- Validate the entity authorized representative as described in section 3.2.2.1,
- Verify the authorization of certificate Requestor as specified in section 3.2.5,
- Verify the phone number of the organization by making a random call.

If all the above validations are passed, TS RA initiated a process on the Web RA Portal through which the entity and the Requester are registered on the portal based on the collected information. At this point the requester would be able to login to the Web RA Portal and submit certificate requests on behalf of his entity.

Once the certificate request has been submitted, the TS RA can proceed as follows:

k) Verify ownership of the domain names or IP addresses as specified in sections 3.2.2.4 and 3.2.2.5 of this CPS.

l) Verify the subject DN format (from CSR) and ensure that:

- The organization field value matches precisely the name of the entity as it was enrolled by the TS RA;
- A least one FQDN or IP address is included in the certificate's SubjectAltName extension.

m) In case of wildcard certificates, conduct a Wildcard Domain Validation as specified in section 3.2.2.6 of this CPS,

n) Check for valid domain TLD that must be ".IQ" For each domain that is included in the certificate request,

a) Verify the validity of TLD against the IANA published lists of valid TLD and gTLD (https://data.iana.org/TLD/tlds-alpha-by-domain.txt),

b) Check CAA records for the domain as specified in section 3.2.2.8 of this CPS.

**For OCSP responder certificate:** The TS RA and an authorized PKI administrator in trusted role oversee the execution of TS PKI internal operational ceremonies through which any of these certificates can be issued. The TS PKI GB approves the operational ceremony documentation and validates the embedded certificate templates and naming conventions against the provisions of this CPS. The TS PKI GB authorizes then the ceremony and confirms the list of involved trusted role ceremony staff. The ceremony is executed under the supervision of the TS RA that reviews the CSR before its processing by the CA.

### 4.2.2 Approval or Rejection of Certificate Applications

The TS RA approval of the certificate application is subject to:

- Successful identification and authentication of all required Subscriber information according to Section 3.2.2
- Domain/IP ownership verification,
- Proof of association between the requesting organization and the subject to which the certificate will be issued,
- Proof of possession of private key,
- Identification and Authorization of the certificate request.

This CA does not issue publicly trusted SSL certificates to internal server name or reserved IP addresses.

### 4.2.3 Time to Process Certificate Applications

No stipulation.

## 4.3 Certificate Issuance

### 4.3.1 CA Actions During Certificate Issuance

Once all the validation is done as described in section 4.2.1, the TS RA team uses the web RA portal to initiate certificate issuance from this CA based on the CSR received from the applicant.

The CA validates the format and structure of the CSR then generates the certificate in accordance to configured certificate template. The certificate is then made available for download by the Web RA portal. The CA issues the certificate in "**Active**" state so that it is ready for use once deployed on the target key-store.

**For OCSP responder certificate:** The issuance and management of these certificates happen as part of operational ceremonies that are approved by at least two members of the TS PKI GB. These approvals establish the following: (1) authorizing the ceremony execution, (2) approving the list of ceremony attendees involving the TS RA, a member of TS PKI operations management, and designated administrators from the TS PKI operations team, (3) validating embedded certificate templates and naming conventions against the provisions of this CPS.

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

The certificate is made available for download to the subscriber on his Web RA portal account.

## 4.4 Certificate Acceptance

### 4.4.1 Conduct Constituting Certificate Acceptance

The Requester downloads the certificate from the web RA portal then validates its content against the certificate application/CSR. In case of any discrepancies, the Requester initiates a discussion with the TS RA which may lead to certificate revocation to issue a corrected certificate.

The certificate is considered accepted by the organization if no complaints are raised by the Requester to the TS RA within 10 business days of receiving the email notification of certificate generation.

**For OCSP responder certificate**: A certificate is deployed on the target system as part of the overall authorized internal operational ceremony.

### 4.4.2 Publication of the Certificate by the CA

This CA does not publish end-user certificates apart from sharing it with the requester.

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

Not stipulation.

## 4.5 Key Pair and Certificate Usage

### 4.5.1 Subscriber Private Key and Certificate Usage

The subscribers adhere to the following obligations:

- Provide correct and up-to-date information to the TS RA as part of his application,
- Not tampering with a certificate,
- 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 of their private key,
- Notify the TS RA immediately if any details in the certificate become invalid, or because of any compromise, loss, disclosure, or otherwise unauthorized use,
- Not using the certificate outside its validity period, or after it has been revoked.
- No longer use the private key after the validity period of the certificate expires, or when a certificate has been revoked.

Refer to section 9.6.3 of this CPS for complementary details.

### 4.5.2 Relying Party Public Key and Certificate Usage

A party relying on a certificate issued by this CA:

- Uses software that is compliant with X.509 and applicable IETF PKIX standards to validate the certificate signature and validity period,
- Validates the certificate by using the CRL, or the OCSP validity status information service in accordance with the certificate path validation procedure,
- Trusts the certificate only if it has not been revoked and is within the validity period,
- Trusts the certificate only for its intended purpose and in accordance with this CPS.

## 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 of a new certificate to the subscriber with a new public key and validate period while the other information in the certificate may remain same.

Certificate re-key is supported by this CA. The re-key process (including identity validation, certificate issuance and communication to relevant parties) 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 SSL certificates.

### 4.7.2 Who May Request Certification of a New Public Key

As per initial certificate issuance.

### 4.7.3 Processing Certificate Re-Keying Requests

As per initial certificate issuance.

### 4.7.4 Notification of New Certificate Issuance to Subscriber

As per initial certificate issuance.

### 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per initial certificate issuance.

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

As per initial certificate issuance.

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

As per 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

As per initial certificate issuance.

### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable

### 4.8.6 Publication of the Modified Certificate by the CA

As per initial certificate issuance.

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

As per initial certificate issuance.

## 4.9 Certificate Revocation and Suspension

Technology Source provides a continuous ability for subscribers to submit certificate requests. This is available through an online system that is accessible 24 x 7 to authenticated subscribers.
Certificate suspension is prohibited. Only permanent certificate revocation is permitted.

The revocation of subscribers' certificates is handled as per the below subsections.

### 4.9.1 Circumstances for Revocation

This CA does not support revocation of Short-lived subscriber certificates.

With the exception of Short-lived Subscriber Certificates, this CA revokes a certificate within 24 hours and use the corresponding CRLReason if one or more of the following occurs:

1. The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate (CRLReason “unspecified (0)” which results in no reasonCode extension being provided in the CRL);
2. The subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn).
3. The CA obtains reasonable evidence that the subscriber’s private key, corresponding to the public key in the certificate suffered a key compromise (CRLReason #1, keyCompromise).
4. The CA obtains evidence that the validation of domain authorization or control for any FullyQualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).
5. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber’s Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) (CRLReason #1, keyCompromise);

With the exception of Short-lived Subscriber Certificates,  this CA may revoke a certificate within 24 hours and use the corresponding CRL Reason if one or more of the following occurs:

1. Obtaining evidence that the certificate no longer complies with the requirements of sections 6.1.5 and 6.1.6 (CRLReason #4, superseded).
2. Obtaining evidence that the certificate was misused (CRLReason #9, privilegeWithdrawn).
3. Knowing that a subscriber has violated one or more of its material obligations under the subscriber Agreement (CRLReason #9, privilegeWithdrawn).
4. Coming across any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant’s right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation)
5. Knowing that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);

6. Made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn).
7. Discovering that the certificate was issued in a manner not in accordance with the procedures of this CPS and with the Baseline Requirements (CRLReason #4, superseded).
8. Knowing that any of the information contained in the certificate is inaccurate (CRLReason #9, privilegeWithdrawn).
9. This CA right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless this CA has planned to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
10. Revocation is required by this CPS for a reason that is not otherwise required to be specified in this section 4.9.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
11. Discovering that there is a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise);

### 4.9.2 Who Can Request Revocation

Revocation can be requested by the following entities:

- The TS RA in the cases described in section 4.9.1
- The Subscriber may submit a revocation request for his own certificate,
- Technology Source at its own discretion (if for instance a compromise is known for the CA key),
- Subscribers, relying parties, application software suppliers, and other third parties may submit Certificate Problem Reports to notify TS of a suspected reasonable cause to initiate the certificate revocation process.

### 4.9.3 Procedure for Revocation Request

Revocation of certificates is done as follows:

- The TS RA team assigns a unique ID to the revocation request. The TS RA records the submitted documents under the assigned ID,
- The TS RA team authenticates the requester's identity as described in section 3.4;
- The TS RA team validates the certificate information in the revocation request form;
- The TS RA performs any required investigation within the applicable time constraints (as listed in section 4.9.1 of this CPS). This may include any required communication with the certificate subscriber,

- The RA team execute the certificate revocation.
- The CA revokes the certificate and the certificate status is updated[4].
- The TS RA notifies via email the subscriber/the entity requested the revocation of the completion of the certificate revocation operation.
- The TS RA updates his internal blacklist with the details of the revoked certificate, circumstances for revocation and based on this information, potentially change the risk profile of the applicant in the internal blacklist. Such information will be queried by the TS RA prior to processing future certificate requests for the applicant.

**Certificate Revocation handling by TS RA following a Certificate problems reporting:**

Subscribers, relying parties, application software suppliers, and other third parties may submit certificate problem reports via info@techsource.iq

TS discloses instructions related to certificate revocation and certificate problem reporting on a dedicated page part of its public repository.

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

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

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

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

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

### 4.9.4 Revocation Request Grace Period

There is no revocation grace period. Revocation requests are processed by TS RA timely after a decision for revocation is made and in all circumstances within the timeframes listed under section 4.9.1 of this CPS.

### 4.9.5 Time within which CA Must Process the Revocation Request

Certificate revocation requests are processed within 24 hours.

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

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

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

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

### 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. This CA provides revocation status via mechanisms that are embedded in the Certificate i.e. CRL and OCSP.

### 4.9.7 CRL Issuance Frequency (if applicable)

The TS TLS CA publishes CRLs at regular intervals. The following rules apply for the CRLs issued by this CA:

- A new CRL is generated every 24 hours;
- CRL lifetime (i.e., value of the nextUpdate field) is set to 26 hours.

### 4.9.8 Maximum Latency for CRLs (if applicable)

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

### 4.9.9 On-Line Revocation/Status Checking Availability

This CA offer an OCSP responders that conforms to RFC 6960 and whose certificates is signed by the TS TLS CA. 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, as defined by RFC 6960.

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

### 4.9.10 On-Line 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 TLS 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 TLS 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 this CA) then the OCSP responder responds with a "revoked" status as defined by RFC 6960 (section 4.4.8. Extended Revoked Definition).

The TS PKI 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 PKI.

### 4.9.11 Other Forms of Revocation Advertisements Available

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

### 4.9.12 Special Requirements Related to Key Compromise

If Technology Source discovers, or has a reason to believe, that there has been a compromise of the private key of the TS TLS CA , it will immediately declare a disaster and invoke its business continuity plan. Technology Source 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.

Relaying Parties may advise Technology Source of a private key compromise using one of the following methods:

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

### 4.9.13 Circumstances for Suspension

Certificate suspension is not supported by this CA.

### 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

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

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

Revocation entries on a CRL or OCSP responses are not removed until after the expiry date of the revoked certificates.

### 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.

This 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.

This CA maintains a 24X7 ability to respond internally to high-priority certificate problem reports as described in section 4.9.3 of this CPS.

### 4.10.3 Optional Features

No Stipulation.

## 4.11 End of Subscription

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

## 4.12 Key Escrow and Recovery

### 4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow is not supported by this CA.

### 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.

## 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 Technology Source'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 is destroyed before discarding. Paper media is shredded using a crosshatch shredder. The following procedure applies for removable computer media:

- Authorization is granted for the destruction of any removable computer media.
- The media is erased then physically destroyed if no longer required.
- Record of this media destruction is maintained.
- Media is 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 TLS CA systems are routinely performed to ensure ample recovery data is available to restore the TS TLS CA systems when required.

At least one full backup and several incremental backups of the TS TLS CA 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

The TS PKI GB follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the TS PKI staff members, and the satisfactory performance of their duties in the field of PKI governance, operations, and service delivery.

The procedural controls include the following:

### 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 are maintained and reviewed annually.

The following are the trusted roles for the TS TLS 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:** Authorized to conduct the vetting of the certificate requests as part of the certification request processing.
- **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 follows 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 involvement of two persons:

- Physical access to the secure enclave where the TS Subordinate CA 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 IT system credentials for the TS Subordinate CAs 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 TLS CA personnel.

The training program encompasses a diverse range of topics and is delivered by a combination of experienced TS TLS 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 TLS 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 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 in the TS CAs' staff will not affect the operational effectiveness, continuity, and integrity of the CAs' 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, 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 documents all training material and makes it available to the TS PKI staff.

The TS PKI GB also ensures 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 are generated and preserved. These logs are 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 TLS CA operations.

### 5.4.1 Types of Events Recorded

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

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

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

Following events occurring in relation to the TS TLS CA operations are recorded:

1. TS TLS CA certificates and key life cycle events, including:
    1. Key generation, backup, storage, recovery, archival and destruction;
    2. Cryptographic device life-cycle management events.
    3. Certificate requests, renewal, and re-key requests, and revocation;
    4. Approval and rejection of Certificate requests;
    5. Generation of CRLs;
    6. Signing of OCSP responses; and
    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate life-cycle management events, including:
    1. Certificate requests, renewal, and re-key requests, and revocation;
    2. All issued certificates including revoked and expired Certificates;
    3. All verification activities stipulated in this CPS (e.g. date, time, calls, persons communicated with);
    4. Approval and rejection of certificate requests;
    5. Issuance of certificates;
3. Security events, including:
    1. Successful and unsuccessful PKI system access attempts;
    2. PKI and security system actions performed;
    3. Relevant router and firewall activities (as described in Section 5.4.1.1); and
    4. Security profile changes;
    5. System platform issues (e.g. crashes), hardware failures, and other anomalies
    6. Installation, update and removal of software on a Certificate System;
    7. Entries to and exits from the CA facility.

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

1. CA personnel, security profiles rotations/changes.
2. All versions of this CPS.

3. Minutes of meetings.
4. Compliance internal audit reports.
5. Current and previous versions of TS Subordinate CAs configuration and operations manuals.

#### *5.4.1.1 Router and firewall activities logs*

Router and firewall activities logged include:

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

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

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

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

### 5.4.2 Frequency of Processing Log

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 are reviewed by the Monitoring & Compliance team on monthly basis,
- Audit and Security of the online CA systems (Ex. OCSP responder) are 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 are 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 Subordinate CAs operations on yearly basis. Samples of the log review reports and collected audit logs since the last audit cycle is 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 retains 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)) after the later occurrence of:
   a. The destruction of the CA Private Key; or
   b. 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 (2)) after the revocation or expiration of the Subscriber Certificate.
3. Any security event records (as set forth in Section 5.4.1 (3)) 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 Subordinate CAs 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 staff.

### 5.4.5 Audit Log Backup Procedures

The following rules apply for the backup of the TS Subordinate CAs audit log:

- Backup media are stored locally in the TS Subordinate CAs main site, in a secure location,
- A second copy of the audit log data and files are stored in the disaster recovery location 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 is 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 TLS CA  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 is made available to the TS PKI GB and PKI operations management, who is 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 TLS CA' staff.

## 5.5 Records Archival

### 5.5.1 Types of Records Archived

The TS Subordinate CAs archives 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, certificate management systems, and
2. Documentation related to the verification, issuance, and revocation of certificate requests and Certificates.

### 5.5.2 Retention Period for Archive

Archived audit logs, as specified in Section 5.5.1, are retained for a period of at least two (2) years and up to seven (7) years. This retention ensures that records are available for investigating potential security incidents or other events requiring retrospection and examination of past activities.

Additionally, the TS Subordinate CAs retains:

A. All archived documentation related to the security of CA Systems, certificate management systems (as set forth in Section 5.5.1),
B. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of:
   i. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates, or
   ii. the expiration of the Subscriber Certificates relying upon such records and documentation.

### 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 the TS Subordinate CAs. 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 TLS 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 Subordinate CAs archive collection system is internal.

### 5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized and authenticated staff is allowed to access archived material. The TS PKI operations team uses the TS Subordinate CAs 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 CA key is changed at a frequency that ensures the TS Subordinate CA has a validity period greater than the maximum lifetime of Subscriber's certificate after the latest Subscriber certificate issuance.

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

The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in chapter 6.1.4.

To support revocation management of issued certificates, the old CA private keys are maintained until all 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 CA is detected by the TS PKI GB, it performs 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 is followed. Otherwise, the scope of potential damage is 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 Recovery Procedures if Computing Resources, Software, and/or Data are Corrupted

TS implements the necessary measures to ensure full recovery of the TS Subordinate CAs 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 Subordinate CAs 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 Subordinate CAs disaster recovery and business continuity plan is tested at least once a year, including failover scenarios to the disaster recovery location.

### 5.7.3 Recovery Procedures after Key Compromise

For Subscribers key compromise, see section 4.9.

Compromise of the TS TLS CA private key, 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 TLS 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 TLS 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 TLS 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 TLS 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.

## 5.8 CA or RA Termination

The provision of the TS TLS 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 Subordinate CA.

If the TS PKI GB and/or the ITPC PMA determine that termination of the TS TLS CA services is deemed necessary, the TS PKI GB performs a termination plan that has 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 TLS 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 TLS 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 TS TLS CA*

The CA's key pairs are generated and stored within the memory of an HSM certified as meeting the requirements of section 6.2.11.

The TSP CA's Key Generation Ceremonies are video recorded and stored securely for auditing purposes.

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

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 disclosed in this CPS,
5. Performed, during the CA key generation process, all the procedures required by its CA Key Generation Script.

#### *6.1.1.2 Subscriber's Key Pair Generation*

The subscriber keys are generated according to the below requirements:

| Certificate type | Key generation requirements |
|---|---|
| ***OV (Organization-validation)*** | The key pair are generated using the key generation utility provided with the web server software. |

Technology Source reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in 6.1.5 and/or 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. The CA is aware of a demonstrated or proven method that exposes the Private Key to compromise.
4. The CA has previously been made aware that the Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;

5. The CA is aware of a demonstrated or proven method to easily compute the Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

Technology Source will not generate a Key Pair on behalf of a Subscriber, and will not accept a Certificate request using a Key Pair previously generated by the CA.

### 6.1.2 Private Key Delivery to Subscriber

Not applicable. Technology Source do not generate, archive, or deliver the private Key on behalf of the Subscriber.

### 6.1.3 Public Key Delivery to Certificate Issuer

This CA accepts CSRs (i.e., commands for certificate generation) only if these requests have been authenticated in the web RA portal.

### 6.1.4 CA Public Key Delivery to Relying Parties

The TLS CAs public key certificates are published on the TS public repository.

### 6.1.5 Algorithm Type and Key Sizes

Subscriber keys are 2048-bit RSA or 4096-bit RSA (recommended).

The TS TLS CA’s keys size is 384-bit ECDSA.

### 6.1.6 Public Key Parameters Generation and Quality Checking

#### *6.1.6.1 TS TLS CA*

The CAs private and public keys generation is done with state-of-the-art parameter generation. The TS Subordinate CAs HSMs 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*

The RAs use reasonable techniques to validate the suitability of public keys presented by Subscribers. Known weak keys are tested for and rejected as described in the CA/B Forum Baseline Requirements section 6.1.6.

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

The 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 CA's 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 TS Subordinate CAs 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 CA are not escrowed. Dedicated backup and restore procedures of this CA's private key are implemented by the TS PKI GB.

### 6.2.4 Private Key Backup

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

Backup operations are executed as part of the TS Subordinate CAs key generation ceremonies. The TS TLS CAs 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 overall TS TLS CA key ceremony procedure includes the physical transport of the TS TLS CA backup from the primary facility to the DR facility. Dedicated personnel in trusted roles participate in the transport operation, which is escorted by security guards. Provisions stipulated in Section 6.2.2 are also considered during the transportation.

### 6.2.5 Private Key Archival

The TS PKI GB does not archive the CAs' private keys.

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

The CA's key pairs is 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.

At no time the CA's privates key are copied to disk or other media during this operation.

### 6.2.7 Private Key Storage on Cryptographic Module

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

### 6.2.8 Method of Activating Private Key

#### *6.2.8.1 TS TLS CA*

Private keys is activated following the principles of dual control and split knowledge. The activation procedure uses a PIN entry device attached to the CA's HSMs.

#### *6.2.8.2 Subscribers*

Subscribers are responsible for activating and protecting the access to their key pair in accordance with the obligations that are presented in the form of a Subscriber Agreement.

### 6.2.9 Method of Deactivating Private Key

#### *6.2.9.1 TS TLS CA*

Technology Source deactivates CA Private Keys in accordance with the instructions and documentation provided by the manufacturer of the hardware security module.

#### *6.2.9.2 Subscribers*

Subscribers are responsible for deactivating and protecting the access to their key pair in accordance with the obligations that are presented in the form of a Subscriber Agreement.

### 6.2.10 Method of Destroying Private Key

#### *6.2.10.1 TS TLS CA*

Destroying the CA private key outside the context of the end of its lifetime applies to investigation and special authorization from the TS PKI GB. This destruction decision includes the assignment of the personnel.

The CA keys are destroyed through documented procedures involving individuals in trusted roles (at least 3 trusted staff members at the presence of at least one representative of the

PKI GB). These procedures enforces the principle of multi-person control and split knowledge. The procedures also ensures that the CA keys are destroyed by removing permanently from any hardware modules the keys are stored on.

#### *6.2.10.2 Subscribers*

Subscribers are responsible for the destruction of their keys in accordance with the obligations that are presented in the form of a Subscriber Agreement.

The subscribers can delete their keys and certificates using the appropriate vendor's provided software.

### 6.2.11 Cryptographic Module Rating

The CA's 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 CA's certificates are valid for six (6) years, with a key usage period of three (3) years. The maximum permitted duration of validity for Subscriber's certificates is defined in section 7.1.

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.

The maximum duration of a Subscriber end entity certificate is 398 days.

## 6.4 Activation Data

### 6.4.1 Activation Data Generation and Installation

#### *6.4.1.1 TS TLS CA*

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

#### 6.4.1.2 Subscribers

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

### 6.4.2 Activation Data Protection

#### 6.4.2.1 TS TLS CA

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

#### 6.4.2.2 Subscribers

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

### 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 Subordinate CAs internal policy documentation.

In particular, the TS Subordinate CAs 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 Subordinate CAs systems and end-point protection
5. Backup and recovery mechanisms for the TS Subordinate CAs operations.
6. Hardening of TS Subordinate CAs 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 Subordinate CAs operational processes.
9. The TS Subordinate CAs 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 Subordinate CAs 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 Subordinate CAs 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 TS Subordinate CAs is dedicated to performing only CA-related tasks. There is 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 Subordinate CAs systems configuration, modification and upgrades are documented and controlled by the TS PKI operations management.

A vulnerability management process is enforced to ensure that the TS Subordinate CAs equipment is scanned for malicious code on first use and periodically thereafter. The vulnerability management process supports the processing within 96 hours of discovery of critical vulnerabilities not previously met by the TS PKI operations team.

### 6.6.3 Life Cycle Security Controls

Refer to Section 6.6.1 for details.

## 6.7 Network Security Controls

Technology Source 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 is 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 TS Subordinate CAs 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.

## 6.8 Timestamping

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

# 7 Certificate, CRL, and OCSP Profiles

## 7.1 Certificate Profile

### 7.1.1 Version Number(s)

TS Subordinate CAs issue X.509 version 3 certificates as defined in RFC 5280.

### 7.1.2 Certificate Extensions

This CA comply with RFC 5280 and Baseline Requirements in all certificates it issues.

The Subordinate CA and end entity certificates include an Extended Key Usage extension containing key usage purposes id-kp-serverAuth and id-kp-clientAuth.

AnyExtendedKeyUsage KeyPurposeId cannot be included in the certificates.

### 7.1.3 Algorithm Object Identifiers

Certificates are issued by the CA with algorithm indicated by the following OID.

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

### 7.1.4 Name forms

#### *7.1.4.1 Name Encoding*

This CA issues Certificates with name forms compliant to RFC 5280 and section 7.1.4 of the Baseline Requirements.

#### *7.1.4.2 Subject Information - Subscriber Certificates*

The applicable subject information for end-entity TLS Certificates is specified in the table below. This CA issues TLS Certificates where the entries of the Subject Alternative Name Extension and the contents of the Subject DN fields are compliant with their respective definitions stated in section 7.1.4 of the Baseline Requirements. In addition, subject Attributes will not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

| TLS Certificate Type | Subject DN | Subject Alternative Name |
|---|---|---|
| **OV TLS Certificates** | • commonName<br>• organizationName<br>• localityName or stateOrProvinceName | dNSName, iPAddress |

| | | |
|---|---|---|
| | - countryName | |

#### *7.1.4.3 Subject Information – Subordinate CA Certificates*

For TS Subordinate CA certificate, 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.

### 7.1.5 Name Constraints

Technology Source will follow the requirements of section 7.1.5 of the Baseline Requirements for publicly trusted TLS certificates.

### 7.1.6 Certificate Policy Object Identifier

Technology Source uses an OID scheme specified for the Iraqis National PKI Policy. Refer to the following certificate template for more details. The used OIDs are specified as part of the certificate profiles.

Additionally, the following Object Identifiers are also used:

| **End entity certificate policies** | Description |
|---|---|
| **2.23.140.1.2.2** | Reserved Policy for OV TLS Certificates |

### 7.1.7 Usage of Policy Constraints Extension

No stipulation.

### 7.1.8 Policy Qualifiers Syntax and Semantics

The TS Subordinate CA contain a CPS Policy Qualifier that points to the applicable CPS.

### 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

### 7.1.10 TS TLS CA 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 | 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 TLS 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 TLS CA G1 | UTF8 encoded |
| SubjectPublicKeyInfo | False | M | D | | |
| AlgorithmIdentifier | | M | D | ECDSA<br>(OID: 1.2.840.10045.2.1)<br>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/tls_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/tls_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 | |
| Policy Properties | | | | | | |
| certificatePolicies | | False | M | S | | |
| | PolicyIdentifier | | M | S | 2.23.140.1.2.2 | CA/B BR Reserved Certificate Policy for OV TLS Certificates |
| 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 | |
| Extended Key Usage Properties | | | | | | |
| extKeyUsage | | False | M | S | | |
| | clientAuth, serverAuth | | M | S | True | |
| Basic Constraints Properties | | | | | | |
| basicConstraints | | True | M | S | | |
| | cA | | M | S | True | |
| | pathLenConstraint | | M | S | 0 | |

### 7.1.11 Organization Validated (OV) Certificates 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 | The issuing Subordinate CA Signature. | The issuing 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 TLS 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 + **[397]** days | Maximum 397 days validity allowed (Baseline Requirement) |
| Subject | False | | | | |
| CountryName | | M | D | Country Name | Encoded according to “ISO 3166-1-alpha-2 code elements”. PrintableString, size 2 (rfc5280) |
| stateOrProvinceName | | M/O | D | State Or Province | UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present. |
| localityName | | M/O | D | Locality | UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present. |

| | | | | | |
|---|---|---|---|---|---|
| OrganizationName | | M | D | Organization name of the legal entity | UTF8 encoded |
| SubjectPublicKeyInfo | False | M | | | |
| AlgorithmIdentifier | | M | D | RSA<br>(OID: 1.2.840.113549.1.1.1) | |
| SubjectPublicKey | | M | D | Public Key<br>Key length: 2048 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/ts_tls_ca.p7b | Subordinate Issuing CA Certificate/Chain download URL over HTTP |

| | | | | | | |
|---|---|---|---|---|---|---|
| crlDistributionPoints | | False | M | | | |
| | DistributionPoint | | M | S | http://pki.techsource.iq/repository/crls/ts_tls_ca.crl | CRL download URL. |
| Key Usage Properties | | | | | | |
| keyUsage | | True | M | | | |
| | digitalSignature | | M | S | True | RSA |
| Policy Properties | | | | | | |
| certificatePolicies | | False | M | | | |
| | PolicyIdentifier | | M | S | 2.23.140.1.2.2 | CA/B BR Reserved Certificate Policy for OV Certificates |
| certificatePolicies | | False | M | | | |
| | PolicyIdentifier | | M | S | 2.16.368.1.2.1.3 | |
| | policyQualifiers:policyQualifierId | | M | S | id-qt 1 | |
| | policyQualifiers:qualifier:cPSuri | | M | S | https://pki.techsource.iq/repository/cps | |
| certificatePolicies | | False | M | | | |
| | PolicyIdentifier | | M | S | 2.16.368.1.1.3.3.2 | |
| Extended Key Usage Properties | | | | | | |
| extKeyUsage | | False | M | | | |
| | serverAuth, | | M | S | True | |
| | clientAuth | | O | S | True | |
| Subject Alternative Name Properties | | | | | | |
| subjectAlternativeName | | False | M | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | dNSName or<br>iPAddress | | M | D | dNSNames with verified ownership<br>or<br>IPv4 or IPv6 address with verified ownership | Contains either a Fully-Qualified Domain Name or Wildcard Domain Name or<br>Contains an IPAddress |

## 7.2 CRL Profile

CE2 = Critical Extension O/M3: O = Optional M = Mandatory
CO4 = 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 TLS 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 |

### 7.2.1 Version Number(s)

TS TLS CA support 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.

#### *7.2.2.1 reasonCode (OID 2.5.29.21)*

The reasonCode feild may be used for revoked Certificates. The reasonCode indicated must not be unspecified (0) and if reasonCode unspecified (0) is used, the CA will omit the reasonCode entry in the CRL.

This extension must not be marked critical. The most appropriate reason must be selected by the Subscriber or the CA from one the following:

(i) **keyCompromise** (1), Indicates that it is known or suspected that the Subscriber’s Private Key has been compromised.

(ii) **affiliationChanged** (3), Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.

(iii) **superseded** (4), Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with the CAB/Forum Baseline Requirements or this CPS.

(iv) **cessationOfOperation** (5), Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate.

(v) **privilegeWithdrawn** (9), Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

The default revocation reason is **unspecified** (0) which results in no reasonCode being provided in the CRL. The CA will not use reasonCode **certificateHold** (6).

The **priviledgeWithdrawn** (9) reasonCode is not made available to the Subscriber.

If Technology Source obtains evidence of Key Compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise (1) reason, then Technology Source may update the CRL reasonCode to keyCompromise (1).

#### *7.2.2.2 issuingDistributionPoint (OID 2.5.29.28)*

The CRLs do not support the Issuing Distribution Point extension.

## 7.3 OCSP 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 | 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 TLS 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 TLS CA G1 OCSP | UTF8 encoded |
| SubjectPublicKeyInfo | False | M | | | |
| AlgorithmIdentifier | | M | S | RSA | |
| SubjectPublicKey | | M | D | Public Key<br>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 | | | |

### 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.

# 8 Compliance Audit and Other Assessments

## 8.1 Frequency or Circumstances of Assessment

Technology Source organizes 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 for Certification Authorities
- 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 who will not be affiliated directly or indirectly in any way with ITPC or any other person with conflicting interests in this regard.

## 8.4 Topics Covered by Assessment

This CA is audited for compliance with the following standards.

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline -
- WebTrust Principles and Criteria for Certification Authorities – Network Security –

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 TLS 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 overall results of audits are reflected by the TS PKI GB on the TS public repository.

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

External audits reports are published on the TSP public repository.

## 8.7 Self-Audits

Technology Source, through its compliance function, monitors and strictly controls its adherence to the procedures listed in this CPS document and to the latest Baseline Requirements by performing regularly internal audits (on at least a quarterly basis) against a randomly selected samples at least 3 percent of the TLS Certificates issued since the last internal audit.

# 9 Other Business and Legal Matters

## 9.1 Fees

### 9.1.1 Certificate Issuance or Renewal Fees

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

### 9.1.2 Certificate Access Fees

No stipulation

### 9.1.3 Revocation or Status Information Access Fees

No fee will be charged for Certificate revocation or status information access.

### 9.1.4 Fees for Other Services

Technology Source may charge for other services depending on business needs.

### 9.1.5 Refund Policy

No refunds for any charged fees.

## 9.2 Financial Responsibility

### 9.2.1 Insurance Coverage

Technology Source ensures that this 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

Technology Source considers the following as confidential information:

- Subscriber’s personal information that are not part of certificates or CRLs
- Correspondence between and the RA function during the certificate management processing (including the collected subscriber’s data)
- 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 is deemed public. This includes the information published on the TS public repository.

### 9.3.3 Responsibility to Protect Confidential Information

Technology Source 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 TS PKI GB 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.

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

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

All communications channels with the Technology Source preserve the privacy and confidentiality of any exchanged private information. Data encryption is used when electronic communication channels are used with the TS TLS CA systems. This includes:

- The communications between the TS RA systems and the subscribers.
- The communications between the TS RA and the CA systems.
- Sessions to deliver certificates.

### 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

Technology Source 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

Technology Source 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, web sites, the CAs' digital certificates and any other publication whatsoever originating from the PKI, including this CPS.

When Technology Source 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 Technology Source and these suppliers.

## 9.6 Representations and Warranties

### 9.6.1 CA Representations and Warranties

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

- The Subscriber that is a party to the Subscriber Agreement;
- All Application Software Suppliers with whom the Iraqis National Root CA will enter into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier;
- and all 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 TLS CA has complied with the Baseline Requirements and its CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

- **Right to Use Domain Name or IP Address:** That, at the time of issuance, the TS TLS CA **(**i). implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii). Followed the procedure when issuing the Certificate; and (iii). accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- **Authorization for Certificate**: That, at the time of issuance, the TS TLS CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;
- **Accuracy of Information**: That, at the time of issuance, the TS TLS CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;
- **Identity of Applicant**: That, if the Certificate contains Subject Identity Information, the TS TLS CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2 and 11.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;

- **Subscriber Agreement**: That, if the TS TLS CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
- **Status**: That the TS TLS CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates;
- **Revocation**: That the TS TLS CA will revoke the Certificate for any of the reasons specified in these Requirements

### 9.6.2 RA Representations and Warranties

Technology Source warrants that it performs RA functions as per the stipulations specified in this CPS.

### 9.6.3 Subscriber Representations and Warranties

Technology Source implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. A separate Agreement is used for each certificate request. The Subscriber Agreement or Terms of Use contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

- **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to the TS RA, both in the certificate request and as otherwise requested by TS in connection with the issuance of the Certificate(s) to be supplied by this CA
- **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
- **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
- **Use of Certificate:** When natural or legal person certificates are requested, an obligation and warranty to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- **Reporting and Revocation:** An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key

associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;

- **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- **Responsiveness:** An obligation to respond to TS instructions concerning Key Compromise or Certificate misuse within a specified time period.
- **Acknowledgment and Acceptance:** An acknowledgment and acceptance that the TS RA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by this CA, or the Baseline Requirements.

### 9.6.4 Relying Party Representations and Warranties

Relying Parties who rely upon the certificates issued under Technology Source:

- 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, Technology Source 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, delivery, license, performance or non-performance 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 SSL / TLS 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 SSL / TLS CA' services.

## 9.8 Limitations of Liability

- Technology Source will not incur any liability to Subscribers to the extent that such liability results from their negligence, fraud, or wilful misconduct,
- Technology Source 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. The Subscribers will immediately indemnify Technology Source from and against any such liability and costs and claims arising there from,
- Technology Source will not be liable to any party whosoever for any damages suffered whether directly or indirectly because of an uncontrollable disruption of its services,
- Subscribers are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by Technology Source,
- Subscribers to compensate a Relying Party which incurs a loss because of the TSP's breach of Subscriber's agreement.
- Relying Parties bear the consequences of their failure to perform the Relying Party obligations; and
- Technology Source denies any financial or any other kind of responsibility for damages or impairments resulting from the TS TLS 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 remains 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 TLS CA' services, are first addressed by the TS PKI GB legal function. If mediation by the TS PKI GB legal function is not successful, then the dispute is adjudicated by the relevant courts of Iraq.

## 9.14 Governing Law

The laws of the Republic of Iraq governs the enforceability, construction, interpretation, and validity of this CPS.

## 9.15 Compliance with Applicable Law

This CPS and provision of TS TLS 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 Technology Source.

### 9.16.3 Severability

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

In the event of a conflict between the Baseline Requirements and any regulation in Iraq, the Technology Source 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 Technology Source 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 Technology Source 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

Technology Source is not 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

Not applicable.