TECHNOLOGY
SOURCE
SMART.SPEED.SOLUTIONS

Iraq National PKI

PKI Disclosure Statement

Document Control

Prepared / Updated By	Reviewed By	Approved By	Owner	Version	Date of Approval
			Tech Source	1.0	

Change History

Sr. No	Version	Changes Description	
1	0.1	Initial version	Touir Mustapha
2	1.0	Reviewed and updated	Yasir Khan

Document Approval

Ver. No	Approver (Name/Title)	Signatures
1.0	PKI GB Director	Date:

Table of Contents

1 Introduction

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 types of certificates to be issued. The Information & Telecommunication Public Company (ITPC) is responsible for this Root CA layer. As the National PKI governance body, the ITPC is mandated to operate the Policy Management Authority (PMA). ITPC Root CAs are:

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

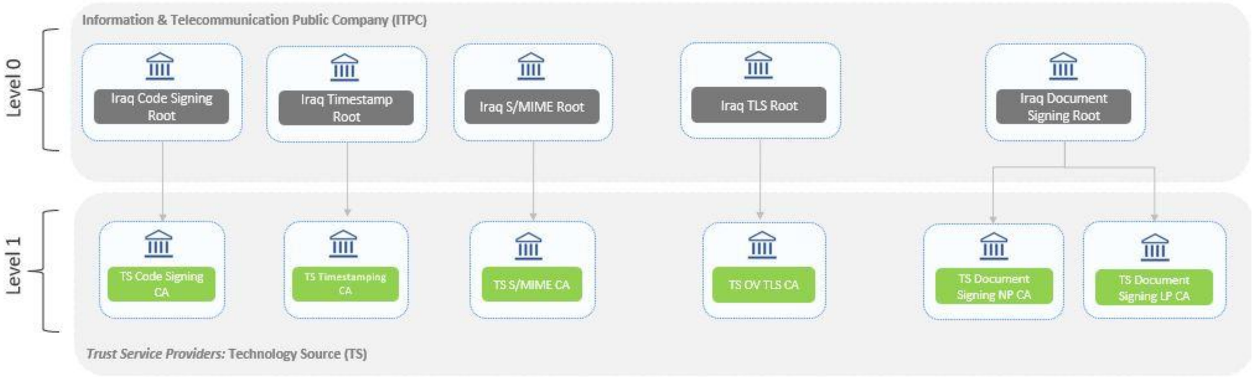
Information & Telecommunication Public Company (ITPC)
Level 0
Iraq Code Signing Root
Iraq Timestamp Root
Iraq S/MIME Root
Iraq TLS Root
Iraq Document Signing Root
Level 1
TS Code Signing CA
TS Timestamping CA
TS S/MIME CA
TS OV TLS CA
TS Document Signing NP CA
TS Document Signing LP CA
Trust Service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

Figure 1- Iraq National PKI hierarchy

Technology Source is the organization to operate the Subordinate CAs and to offer related trust services to the 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 National Root CAs.

ITPC certifies TSP Subordinate CAs for Technology Source as follows:

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

The above use cases are the 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 the adoption, enables interoperability, and enhances the user trust.

1.2 Purpose

The purpose of this document is to summarize in a more readable and understandable format the key points of the Technology Source PKI services for the benefit of Subscribers and Relying Parties. This document does not substitute or replace the Terms and Conditions of the PKI services, nor the Certification Practice Statement (CPS) published on the Technology Source repository.

2 Contact Information

The following address is where you can get in touch with the Technology Source PKI GB:

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 feedback regarding this PDS only when they are addressed to the contact above.

2.1 Certificate Problem Report

Subscribers, 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 certificate revocation requests before taking any action.

3 Certificate Type, Validation Procedures and Usage

Technology Source issues the following types of end-entity certificates as described below:

The end-user certificates issued by the Technology Source Document Signing NP CA are:

Certificate types	Description and validation procedure	OID
Qualified signing certificates	This type of certificate is used for producing Qualified (high assurance) digital signatures on documents and electronic transactions. It is issued to natural persons, including individuals with professional capacity, who undergo identity verification through in-person meetings with the relevant registration authority or equivalent methods that provide an equivalent level of assurance as physical presence. The individual private keys associated with these certificates may be used for both local and remote signing purposes.	(local) 2.16.368.1.1.3.1.2 (remote) 2.16.368.1.1.3.1.5
Advanced signing certificate	Used to produce Advanced (moderate assurance) digital signatures on documents and e-transactions. Issued to natural persons, including individual with professional capacity and whose identity has been verified with reasonable confidence in the user's identity and does not require the highest level of assurance. The individual private keys associated with these certificates may be used for both local and remote signing purposes.	(local) 2.16.368.1.1.3.1.1 (remote) 2.16.368.1.1.3.1.4
OCSP certificate	Used by the Technology Source Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the Technology Source Governance Board (i.e., TS PKI GB).	N/A

The end-user certificates issued by the Technology Source Document Signing LP CA are:

Certificate types	Description and validation procedure	OID
eSeal Certificate	This certificate is issued to legal person to add an eSeal on a document issued/attested by this legal person. Before issuing this type of certificate, Technology Source verifies the legal existence of the applicant (i.e., government or non- government entity) using an authoritative data source that provides information on the formation of the organization including its legal name. Technology Source also performs a site visit to the applicant's address to validate the applicant's physical address and place of business. The applicant's vetting process also encompasses verification of the applicant's authorized representative based on the organization's record at the authoritative source or a formal communication between the Technology Source and the applicant (i.e., legal person).	2.16.368.1.1.3.2.1
Verification response signing certificate	Certificate for signing the signature verification responses returned from the TS operated signature verification service. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the Technology Source Governance Board (i.e., TS PKI GB).	2.16.368.1.1.3.3.3
OCSP certificate	Used by the Technology Source Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the Technology Source Governance Board (i.e., TS PKI GB).	N/A

The end-user certificates issued by the Technology Source SSL/TLS CA are:

Certificate types	Description and validation procedure	OID
Organization validated (OV) SSL	Certificate issued for website authentication. Before issuing this type of certificate, Technology Source verifies the legal existence of the applicant (i.e., government or non- government entity) using an authoritative data source that provides information on the formation of organization including its legal name. Technology Source also performs a site visit to the applicant's address to validate the applicant's physical address and place of business. The applicant's vetting process also encompasses verification of the applicant's authorized representative based on the organization's record at the authoritative source or a formal communication between the Technology Source and the applicant (i.e., legal person).	2.16.368.1.1.3.3.2
OCSP certificate	Used by the Technology Source Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the Technology Source Governance Board (i.e., TS PKI GB).	N/A

The end-user certificates issued by the Technology Source Code Signing CA are:

Certificate types	Description and validation procedure	OID
Code Signing	Used to sign source code/software developed by a legal person (i.e., a government or non- government entity). Before issuing this type of certificate, Technology Source verifies the legal existence of the applicant (i.e., Legal person) using an authoritative data source that provides information on the formation of organization including its legal name. Technology Source also performs a site visit to the applicant's address to validate the applicant's physical address and place of business. The applicant's vetting process also encompasses verification of the applicant's authorized representative based on the organization record at the authoritative source or a formal communication between the Technology Source and the applicant (i.e., legal person).	2.16.368.1.1.3.2.2
OCSP certificate	Used by the Technology Source Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the Technology Source Governance Board (i.e., TS PKI GB).	N/A

The end-user certificates issued by the Technology Source S/MIME CA are:

Certificate types	Description and validation procedure	OID
S/MIME Sponsor-Validated	Used to digitally sign and encrypt the email communications. This type of certificate is issued only to the natural persons representing a legal person that are identity-vetted through in-person meetings with the relevant registration authority or equivalent methods that provide an equivalent level of assurance as physical presence. Technology Source verifies the applicant's control of Mailbox Addresses to be included in the issued certificates.	2.16.368.1.1.3.1.3
OCSP certificate	Used by the Technology Source Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the Technology Source Governance Board (i.e., TS PKI GB).	N/A

The end-user certificates issued by Technology Source Timestamping CA are:

Certificate types	Description and validation procedure	OID
DS Timestamp Certificate	Used for signing the timestamps issued by the TS TSA service for the document signatures. The TS Timestamping CA does not issue certificates to any legal person other than Technology Source itself. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the Technology Source Governance Board (i.e., TS PKI GB).	2.16.368.1.2.1.6.1
CS Timestamp Certificate	Compliant to CS BR requirements, used for signing the timestamps issued by the TS TSA service for code signing. The TS Timestamping CA does not issue certificates to any legal person other than Technology Source itself. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the Technology Source Governance Board (i.e., TS PKI GB).	2.16.368.1.2.1.6.2
OCSP certificate	Used by the Technology Source Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the Technology Source Governance Board (i.e., TS PKI GB).	N/A

4 Reliance Limits

Technology Source cannot be held liable for any use of the certificate that does not comply with its Subordinate CAs CPSs available at https://pki.techsource.iq

5 Subscriber's Obligations

It is the responsibility of Subscribers to:

- only use the Key Pairs for the purposes and in the ways allowed by the relevant CPS.
- submit accurate and complete information to the CA during Subject registration at the time of certificate request.
- Exercise reasonable care to avoid unauthorized use of the Subject's Private Key.
- (for the certificates that require use of a signature creation device) if it generates its Private Key by itself, generate it within a signature creation device approved by the Technology Source.
- notify the CA, without any unreasonable delay, if any of the following occurs up to the end of the validity period indicated in the Certificate:
    - the Subject's Private Key has been potentially or proven lost, stolen or compromised.
    - control over the Subject's Private Key has been lost due to potential or actual compromise of activation data (e.g., PIN code) or other reasons.
    - inaccuracy or changes to the Certificate content, as notified to the Subscriber.
- ensure that if the Subscriber or Subject generates the Subject's Key Pair, only the Subject holds the Private Key
- ensure that Private Keys are generated within the hardware key storage device approved by Technology Source.

For further information, please refer to the Technology Source CPS available at https://pki.techsource.iq

6 Certificate Status checking obligations of the Relying Parties

The "Relying Parties" shall confirm that certificates are not suspended or revoked before relying on the information they contain. Such verification is performed by checking the relevant Subordinate CA's list of revoked certificates (CRL) or by querying the relevant Subordinate CA's OCSP service using the addresses (URLs) from the certificate itself.
The "Relying Parties" shall also take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or the Terms and Conditions.

7 Limited Warranty and disclaimer / Limitation of Liability

The liability taken by the Technology Source is limited to the correct application of procedures as declared in its CPS; these procedures relate to the issue and management of digital Certificates. Therefore, Technology Source is not in any event liable for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by applicable law.

Technology Source is not liable for any damages resulting from infringements by the Subscriber or the Relying Party on the applicable terms and conditions. Technology Source is not in any event liable for the damages that result from force major events as detailed in the relevant CPS. Technology Source takes commercially reasonable measures to mitigate the effects of force major in due time. Any damage resulting of any delay caused by force major will not be covered by the Technology Source.

8 Applicable Agreement and CPSs

Technology Source agreements and CPSs are available at https://pki.techsource.iq

9 Privacy Policy

Technology Source observes personal data privacy rules and privacy rules as specified in relevant CPS documents.
Only limited trusted personnel from Technology Source 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 the Technology Source to Subscribers except for information about themselves and only covered by the contractual agreement between the Technology Source 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, Technology Source will ensure through reasonable means that this information is not used for any purpose apart from the requested purposes. All communications channels with Technology Source shall preserve the privacy and confidentiality of any exchanged private information.

10 Refund Policy

No refund is applicable for any fees charged by Technology Source.

11 Applicable Laws, complaints, and dispute resolution

The provision of the Technology Source PKI services is compliant to the relevant and applicable laws of the Republic of Iraq.
All disputes associated with the provisions of this document and the Technology Source PKI services shall be first addressed by the TS PKI GB. If mediation by the TS PKI GB is not successful, then the dispute will be escalated to the ITPC PMA and eventually adjudicated by the relevant courts of Iraq.

12 TSP and repository licenses, trust marks, and audit

Technology Source ensures that its Subordinate CAs and related services are subject to the regular internal audits. External audits are planned and executed by an independent WebTrust practitioner according to the WebTrust audit scheme. These are organized and applied for the PKI services offered on a yearly basis by Technology Source.