



Iraq National PKI

S/MIME CA

Certificate Practice Statement

Document Control

Sr. No	Version	Changes Description	Responsible
0.1	17/01/2023	Initial version	Touir Mustapha
0.2	23/02/2023	Internal review and update	Ahmad Ibrahim
0.3	18/07/2023	Update in section 3.2.2	Touir Mustapha
0.4	04/12/2023	Adding OIDs values, Contact information, Repository URL 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	02/05/2024	- Update in section 5.4.1 to clarify data that need to be logged as part of "Firewall and Router activities" logging requirements. - Applied changes introduced in S/MIME BRs 1.0.3	Touir Mustapha
1.0	15/07/2024	Updates based on auditor's recommendations following the Point-In-Time audit.	Touir Mustapha Yasir Khan
1.1	16/09/2025	- Annual review - Correction of typographical errors	Technology Source

Document Approval

Ver. No	Approver (Name/Title)	Signatures
1.1	PKI GB Director	
		Date ¹ : 16/09/2025

¹ In light of the last review activity conducted after the Point-in-Time (PIT) date, this review is exceptionally being submitted for Governance Board approval beyond the one-year period specified in section 2.3, in order to address all auditor comments collected during the Period-of-Time audit conducted in August 2025

Table of Contents

1	INTRODUCTION	9
1.1	OVERVIEW	10
1.1.1	TECHNOLOGY SOURCE PKI GOVERNANCE BOARD (TS PKI GB)	12
1.2	DOCUMENT NAME AND IDENTIFICATION.....	12
1.3	PKI PARTICIPANTS	12
1.3.1	CERTIFICATION AUTHORITIES.....	12
1.3.2	REGISTRATION AUTHORITIES	13
1.3.3	SUBSCRIBERS	14
1.3.4	RELYING PARTIES.....	14
1.3.5	OTHER PARTICIPANTS.....	14
1.4	CERTIFICATE USAGE	15
1.4.1	APPROPRIATE CERTIFICATE USES.....	15
1.4.2	PROHIBITED CERTIFICATE USES	15
1.5	POLICY ADMINISTRATION.....	15
1.5.1	ORGANIZATION ADMINISTERING THE DOCUMENT.....	15
1.5.2	CONTACT PERSON	15
1.5.3	PERSON DETERMINING CPS SUITABILITY FOR THE POLICY	16
1.5.4	CPS APPROVAL PROCEDURES.....	16
1.6	DEFINITIONS AND ACRONYMS	16
1.6.1	DEFINITIONS.....	16
1.6.2	ACRONYMS	22
1.6.3	REFERENCES	24
2	PUBLICATION AND REPOSITORY RESPONSIBILITIES	25
2.1	REPOSITORIES	25
2.2	PUBLICATION OF CERTIFICATION INFORMATION.....	25
2.3	TIME OR FREQUENCY OF PUBLICATION	25
2.3.1	CA CERTIFICATES.....	26
2.3.2	CRLS.....	26
2.4	ACCESS CONTROLS ON REPOSITORIES.....	26
3	IDENTIFICATION AND AUTHENTICATION.....	27
3.1	NAMING	27
3.1.1	TYPE OF NAMES.....	27
3.1.2	NEED FOR NAMES TO BE MEANINGFUL	28
3.1.3	ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS.....	28
3.1.4	RULES FOR INTERPRETING VARIOUS NAME FORMS	28

3.1.5	UNIQUENESS OF NAMES	28
3.1.6	RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS	28
3.2	INITIAL IDENTITY VALIDATION	28
3.2.1	METHOD TO PROVE POSSESSION OF PRIVATE KEY.....	28
3.2.2	AUTHENTICATION OF ORGANIZATION	29
3.2.3	VALIDATION OF MAILBOX AUTHORIZATION OR CONTROL.....	30
3.2.4	AUTHENTICATION OF INDIVIDUAL IDENTITY.....	30
3.2.5	NON-VERIFIED SUBSCRIBER INFORMATION	31
3.2.6	VALIDATION OF AUTHORITY	31
3.2.7	CRITERIA FOR INTEROPERATION	31
3.3	INITIAL IDENTITY VALIDATION IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS	31
3.3.1	IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY	31
3.3.2	IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION.....	32
3.4	IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST	32
4	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	33
4.1	CERTIFICATE APPLICATION.....	33
4.1.1	WHO CAN SUBMIT A CERTIFICATE APPLICATION.....	33
4.1.2	ENROLMENT PROCESS AND RESPONSIBILITIES.....	33
4.2	CERTIFICATE APPLICATION PROCESSING	34
4.2.1	PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS.....	34
4.2.2	APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS.....	35
4.2.3	TIME TO PROCESS CERTIFICATE APPLICATIONS.....	36
4.3	CERTIFICATE ISSUANCE	36
4.3.1	CA ACTIONS DURING CERTIFICATE ISSUANCE	36
4.3.2	NOTIFICATION TO SUBSCRIBER BY THE CA OF ISSUANCE OF CERTIFICATE.....	37
4.4	CERTIFICATE ACCEPTANCE	37
4.4.1	CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE.....	37
4.4.2	PUBLICATION OF THE CERTIFICATE BY THE CA.....	37
4.4.3	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES.....	37
4.5	KEY PAIR AND CERTIFICATE USAGE	37
4.5.1	SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE.....	37
4.5.2	RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE.....	38
4.6	CERTIFICATE RENEWAL	38
4.6.1	CIRCUMSTANCE FOR CERTIFICATE RENEWAL	38
4.6.2	WHO MAY REQUEST RENEWAL	38
4.6.3	PROCESSING CERTIFICATE RENEWAL REQUESTS	38
4.6.4	NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER.....	38
4.6.5	CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE	38
4.6.6	PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA	38
4.6.7	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES.....	38
4.7	CERTIFICATE RE-KEY	39

Certificate Practice Statement for the Technology Source S/MIME CA

4.7.1	CIRCUMSTANCE FOR CERTIFICATE RE-KEY.....	39
4.7.2	WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY	39
4.7.3	PROCESSING CERTIFICATE RE-KEYING REQUESTS	39
4.7.4	NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER.....	39
4.7.5	CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE	39
4.7.6	PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA	39
4.7.7	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES.....	39
4.8	CERTIFICATE MODIFICATION	39
4.8.1	CIRCUMSTANCE FOR CERTIFICATE MODIFICATION	39
4.8.2	WHO MAY REQUEST CERTIFICATE MODIFICATION	39
4.8.3	PROCESSING CERTIFICATE MODIFICATION REQUESTS.....	39
4.8.4	NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER.....	40
4.8.5	CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE	40
4.8.6	PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA.....	40
4.8.7	NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES.....	40
4.9	CERTIFICATE REVOCATION AND SUSPENSION.....	40
4.9.1	CIRCUMSTANCES FOR SUBSCRIBER CERTIFICATES REVOCATION	40
4.9.2	WHO CAN REQUEST REVOCATION	42
4.9.3	PROCEDURE FOR REVOCATION REQUEST	42
4.9.4	REVOCATION REQUEST GRACE PERIOD	44
4.9.5	TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST	44
4.9.6	REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES.....	44
4.9.7	CRL ISSUANCE FREQUENCY (IF APPLICABLE)	44
4.9.8	MAXIMUM LATENCY FOR CRLS (IF APPLICABLE).....	44
4.9.9	ON-LINE REVOCATION/STATUS CHECKING AVAILABILITY.....	45
4.9.10	ON-LINE REVOCATION CHECKING REQUIREMENTS	45
4.9.11	OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE	45
4.9.12	SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE	45
4.9.13	CIRCUMSTANCES FOR SUSPENSION	46
4.9.14	WHO CAN REQUEST SUSPENSION	46
4.9.15	PROCEDURE FOR SUSPENSION REQUEST.....	46
4.9.16	LIMITS ON SUSPENSION PERIOD.....	46
4.10	CERTIFICATE STATUS SERVICES	46
4.10.1	OPERATIONAL CHARACTERISTICS.....	46
4.10.2	SERVICE AVAILABILITY	46
4.10.3	OPTIONAL FEATURES.....	47
4.11	END OF SUBSCRIPTION	47
4.12	KEY ESCROW AND RECOVERY	47
4.12.1	KEY ESCROW AND RECOVERY POLICY AND PRACTICES.....	47
4.12.2	SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES.....	47
5	<u>FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS</u>	<u>48</u>

5.1	PHYSICAL SECURITY CONTROLS.....	49
5.1.1	SITE LOCATION AND CONSTRUCTION	49
5.1.2	PHYSICAL ACCESS	49
5.1.3	POWER AND AIR CONDITIONING	49
5.1.4	WATER EXPOSURES	50
5.1.5	FIRE PREVENTION AND PROTECTION	50
5.1.6	MEDIA STORAGE	50
5.1.7	WASTE DISPOSAL	50
5.1.8	OFF-SITE BACKUP	50
5.2	PROCEDURAL CONTROLS.....	51
5.2.1	TRUSTED ROLES	51
5.2.2	NUMBER OF PERSONS REQUIRED PER TASK	52
5.2.3	IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE.....	52
5.2.4	ROLES REQUIRING SEPARATION OF DUTIES	52
5.3	PERSONNEL CONTROLS.....	52
5.3.1	QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS	52
5.3.2	BACKGROUND CHECK PROCEDURES.....	53
5.3.3	TRAINING REQUIREMENTS	53
5.3.4	RETRAINING FREQUENCY AND REQUIREMENTS	53
5.3.5	JOB ROTATION FREQUENCY AND SEQUENCE	54
5.3.6	SANCTIONS FOR UNAUTHORIZED ACTIONS.....	54
5.3.7	INDEPENDENT CONTRACTOR REQUIREMENTS.....	54
5.3.8	DOCUMENTATION SUPPLIED TO PERSONNEL	54
5.4	AUDIT LOGGING PROCEDURES.....	54
5.4.1	TYPES OF EVENTS RECORDED.....	55
5.4.2	FREQUENCY OF PROCESSING LOG	56
5.4.3	RETENTION PERIOD FOR AUDIT LOG	57
5.4.4	PROTECTION OF AUDIT LOG	57
5.4.5	AUDIT LOG BACKUP PROCEDURES	58
5.4.6	AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)	58
5.4.7	NOTIFICATION TO EVENT-CAUSING SUBJECT	58
5.4.8	VULNERABILITY ASSESSMENTS	58
5.5	RECORDS ARCHIVAL.....	59
5.5.1	TYPES OF RECORDS ARCHIVED	59
5.5.2	RETENTION PERIOD FOR ARCHIVE	59
5.5.3	PROTECTION OF ARCHIVE.....	59
5.5.4	ARCHIVE BACKUP PROCEDURES	60
5.5.5	REQUIREMENTS FOR TIMESTAMPING OF RECORDS	60
5.5.6	ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)	60
5.5.7	PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION.....	60
5.6	KEY CHANGEOVER	60
5.7	COMPROMISE AND DISASTER RECOVERY.....	60
5.7.1	INCIDENT AND COMPROMISE HANDLING PROCEDURES	60
5.7.2	COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED	61

5.7.3	ENTITY PRIVATE KEY COMPROMISE PROCEDURES	61
5.7.4	BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER	61
5.8	CA OR RA TERMINATION	62
6	<u>TECHNICAL SECURITY CONTROLS</u>	<u>64</u>
6.1	KEY PAIR GENERATION AND INSTALLATION	64
6.1.1	KEY PAIR GENERATION	64
6.1.2	PRIVATE KEY DELIVERY TO SUBSCRIBER	65
6.1.3	PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER	65
6.1.4	CA PUBLIC KEY DELIVERY TO RELYING PARTIES	65
6.1.5	KEY SIZES	65
6.1.6	PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING	65
6.1.7	KEY USAGE PURPOSES (AS PER X.509 V3 KEY USAGE FIELD)	66
6.2	PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.....	66
6.2.1	CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS	66
6.2.2	PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL	66
6.2.3	PRIVATE KEY ESCROW	66
6.2.4	PRIVATE KEY BACKUP	66
6.2.5	PRIVATE KEY ARCHIVAL	67
6.2.6	PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE	67
6.2.7	PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE	67
6.2.8	METHOD OF ACTIVATING PRIVATE KEY	67
6.2.9	METHOD OF DEACTIVATING PRIVATE KEY	67
6.2.10	METHOD OF DESTROYING PRIVATE KEY	68
6.2.11	CRYPTOGRAPHIC MODULE RATING	68
6.3	OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	68
6.3.1	PUBLIC KEY ARCHIVAL	68
6.3.2	CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS	68
6.4	ACTIVATION DATA	69
6.4.1	ACTIVATION DATA GENERATION AND INSTALLATION	69
6.4.2	ACTIVATION DATA PROTECTION.....	69
6.4.3	OTHER ASPECTS OF ACTIVATION DATA.....	69
6.5	COMPUTER SECURITY CONTROLS	69
6.5.1	SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS.....	69
6.5.2	COMPUTER SECURITY RATING	70
6.6	LIFE CYCLE TECHNICAL CONTROLS	70
6.6.1	SYSTEM DEVELOPMENT CONTROLS	70
6.6.2	SECURITY MANAGEMENT CONTROLS	70
6.6.3	LIFE CYCLE SECURITY CONTROLS	71
6.7	NETWORK SECURITY CONTROLS.....	71
6.8	TIMESTAMPING	71

7	<u>CERTIFICATE, CRL, AND OCSP PROFILES</u>	<u>72</u>
7.1	CERTIFICATE PROFILE	72
7.1.1	VERSION NUMBER(S)	72
7.1.2	CERTIFICATE EXTENSIONS.....	72
7.1.3	ALGORITHM OBJECT IDENTIFIERS	72
7.1.4	NAME FORMS.....	72
7.1.5	NAME CONSTRAINTS.....	73
7.1.6	CERTIFICATE POLICY OBJECT IDENTIFIER	73
7.1.7	USAGE OF POLICY CONSTRAINTS EXTENSION.....	73
7.1.8	POLICY QUALIFIERS SYNTAX AND SEMANTICS	73
7.1.9	PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICIES EXTENSION.....	73
7.1.10	TS S/MIME CA CERTIFICATE PROFILE.....	74
7.1.11	S/MIME CERTIFICATES PROFILE	78
7.2	CRL PROFILE.....	83
7.2.1	VERSION NUMBER(S)	84
7.2.2	CRL AND CRL ENTRY EXTENSIONS	84
7.3	OCSP PROFILE	85
7.3.1	VERSION NUMBER(S)	89
7.3.2	OCSP EXTENSIONS	89
8	<u>COMPLIANCE AUDIT AND OTHER ASSESSMENTS.....</u>	<u>90</u>
8.1	FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT.....	90
8.2	IDENTITY/QUALIFICATIONS OF ASSESSOR	90
8.3	ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY	90
8.4	TOPICS COVERED BY ASSESSMENT	91
8.5	ACTIONS TAKEN AS A RESULT OF DEFICIENCY	91
8.6	COMMUNICATION OF RESULTS	91
8.7	SELF-AUDITS.....	91
9	<u>OTHER BUSINESS AND LEGAL MATTERS</u>	<u>93</u>
9.1	FEES	93
9.1.1	CERTIFICATE ISSUANCE OR RENEWAL FEES	93
9.1.2	CERTIFICATE ACCESS FEES	93
9.1.3	REVOCATION OR STATUS INFORMATION ACCESS FEES	93
9.1.4	FEES FOR OTHER SERVICES.....	93
9.1.5	REFUND POLICY	93
9.2	FINANCIAL RESPONSIBILITY	93
9.2.1	INSURANCE COVERAGE.....	93
9.2.2	OTHER ASSETS	93
9.2.3	INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES	93

9.3	CONFIDENTIALITY OF BUSINESS INFORMATION	93
9.3.1	SCOPE OF CONFIDENTIAL INFORMATION.....	93
9.3.2	INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION	94
9.3.3	RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION.....	94
9.4	PRIVACY OF PERSONAL INFORMATION	94
9.4.1	PRIVACY PLAN	94
9.4.2	INFORMATION TREATED AS PRIVATE.....	95
9.4.3	INFORMATION NOT DEEMED PRIVATE.....	95
9.4.4	RESPONSIBILITY TO PROTECT PRIVATE INFORMATION	95
9.4.5	NOTICE AND CONSENT TO USE PRIVATE INFORMATION	95
9.4.6	DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS	95
9.4.7	OTHER INFORMATION DISCLOSURE CIRCUMSTANCES	95
9.5	INTELLECTUAL PROPERTY RIGHTS	95
9.6	REPRESENTATIONS AND WARRANTIES	96
9.6.1	CA REPRESENTATIONS AND WARRANTIES.....	96
9.6.2	RA REPRESENTATIONS AND WARRANTIES.....	97
9.6.3	SUBSCRIBER REPRESENTATIONS AND WARRANTIES	97
9.6.4	RELYING PARTY REPRESENTATIONS AND WARRANTIES.....	98
9.6.5	REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS.....	98
9.7	DISCLAIMERS OF WARRANTIES	98
9.8	LIMITATIONS OF LIABILITY	99
9.9	INDEMNITIES.....	99
9.10	TERM AND TERMINATION	99
9.10.1	TERM	99
9.10.2	TERMINATION.....	99
9.10.3	EFFECT OF TERMINATION AND SURVIVAL.....	99
9.11	INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS.....	100
9.12	AMENDMENTS	100
9.12.1	PROCEDURE FOR AMENDMENT.....	100
9.12.2	NOTIFICATION MECHANISM AND PERIOD	100
9.12.3	CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED.....	100
9.13	DISPUTE RESOLUTION PROVISIONS.....	100
9.14	GOVERNING LAW	100
9.15	COMPLIANCE WITH APPLICABLE LAW	100
9.16	MISCELLANEOUS PROVISIONS	101
9.16.1	ENTIRE AGREEMENT.....	101
9.16.2	ASSIGNMENT	101
9.16.3	SEVERABILITY.....	101
9.16.4	ENFORCEMENT (ATTORNEYS' FEES AND WAIVER OF RIGHTS)	101
9.16.5	FORCE MAJEURE	101
9.17	OTHER PROVISIONS	101

1 Introduction

The present document is the Certification Practice Statement (CPS) describing the certification practices that apply to Technology Source (hereinafter, TS) S/MIME CA. This CPS complies with the TSP Certificate Policy that is applicable to the provision of certification services offered by 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 S/MIME CA that are established and operated by TS under the Iraq national PKI hierarchy, with regards to the complete lifetime of certificates issued by this CA.

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

- **S/MIME certificates** - certificates issued to natural persons to be used for email signing and encryption.
- **OCSP responder certificate** – certificates for the Online Certificate Status Protocol (OCSP) responder to sign OCSP responses related to certificates issued by the S/MIME CA.

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

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

- Network and Certificate System Security Requirements
- Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates

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

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

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

1.1 Overview

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

Level 0:

The below five (5) Roots Certification Authorities (CA) are established for the different type 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 CAs² 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:

² For S/MIME certificates, only the Iraq S/MIME Root CA is relevant since it signs the S/MIME Subordinate CA certificate of Technology Source. Other Root CAs belongs to the Iraqi PKI but aren't pertinent to S/MIME certificates issuance and are not included in the S/MIME hierarchy as depicted in Figure 1.

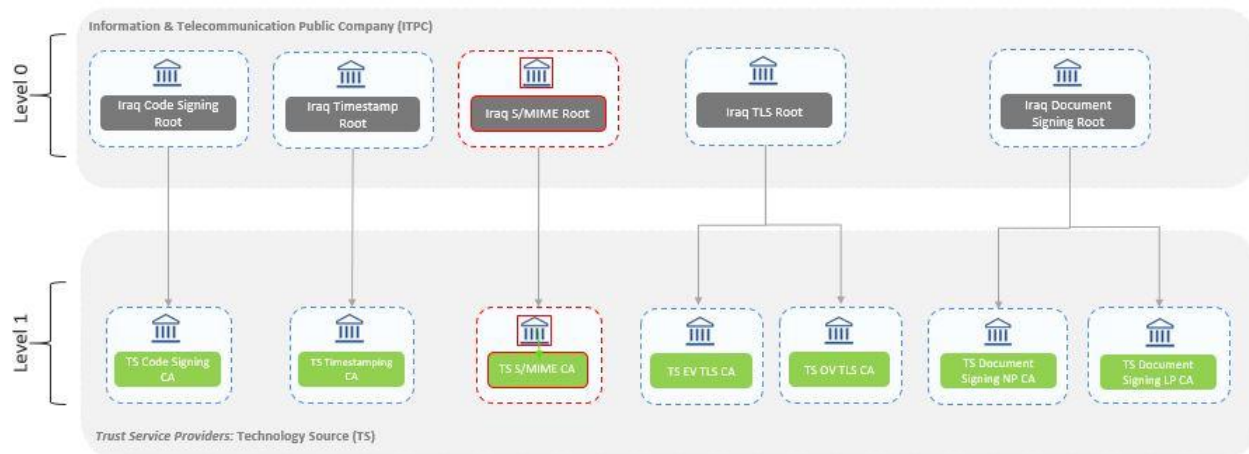


Figure 1 Iraq National PKI hierarchy

Technology Source is the organization to operate the Subordinate CAs and offer related trust services to the Iraq 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 CAs³ for Technology Source as follows:

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

³ For S/MIME certificates, only the TS S/MIME CA is pertinent, as it will issue S/MIME end-entity certificates. Other subordinate CAs belong to the Technology Source PKI but are not relevant for S/MIME certificate issuance and are not part of the S/MIME hierarchy as depicted in Figure 1.

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 this S/mime CA) is referred to as the TS PKI GB. The TS PKI GB comprises the necessary functions including policy, compliance, legal and architecture that are required to provide strategic direction and continuously supervises the TS PKI operations.

The TS PKI GB is particularly responsible for:

- Define and maintain the TS PKI strategy,
- 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 S/MIME CA Certificate Practice Statement**” which is identified by the OID **2.16.368.1.2.1.4** and referenced in related documents as [TS S/MIME CA CPS].

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

1.3 PKI Participants

1.3.1 Certification Authorities

The Technology Source S/MIME 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 S/MIME 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 status of the certificates issued by this CA.

1.3.2 Registration Authorities

1.3.2.1 *Technology Source RA*

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 renewal on behalf of the CA.

Technology Source operates its own RA function and does not rely on Delegated Third Parties for RA functions.

The RA function falls within the PKI operations structure and responsible for identity verification and validation for the Iraqi government and non-government entities wishing to act as a local registration authority to issue Sponsor- validated S/MIME certificates to their own user communities (see section 1.3.2.2).

Technology Source does not delegate the verification of mailbox authorization or control.

1.3.2.2 *Local RAs (LRAs)*

Technology Source provides the ability to Iraqi government and non-government entities aiming to manage certificates lifecycle of their own user communities to act as a local registration authority (LRA) for a certain type of certificates that are issued for natural persons (ie. Sponsor-validated S/MIME certificates).

In this case, the requesting entity enters a contractual relationship (through an LRA agreement) with Technology Source whereby the requesting entity establishes a local registration authority (LRA office) where RA officers belonging to the entity can operate.

The LRA agreement enforces obligations that include 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 technically implements the LRA function through a Web-based application offered for a duly authorized LRA officer(s) operating from designated LRA offices. A dedicated LRA account is issued for each LRA officer to manage certificates limited to the user community belonging to the entity that LRA office belongs to. The LRA officers meet and follow the requirements set forth in Sections 4.2 and 5.3.

1.3.3 Subscribers

Subscribers of the TS S/MIME CA are natural persons identified in association with a legal person (i.e., Iraqi employees) who apply for S/MIME (Sponsor-validated) Certificates from the TS S/MIME CA and agree to be bound by the relevant Subscriber Agreement.

1.3.4 Relying Parties

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

1.3.5 Other Participants

Other Participants include:

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The certificates issued by this CA can be used to:

1. **Certificates for natural persons:**
 - a. **S/MIME:** Used to digitally sign, verify, and encrypt email messages, ensuring they originate from a verified email address.
2. **OCSP responder certificate:** used to sign and verify the Online Certificate Status Protocol (OCSP) responses for certificates issued by the Technology Source S/MIME 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

Technology Source maintains a continuous 24/7 ability to internally respond to any high priority revocation requests and certificate problem reports provides instructions for certificate revocation and certificate problem reporting on a dedicated page in its public repository, accessible at [https://pki.techsource.iq/repository/Certificate Problem Report.html](https://pki.techsource.iq/repository/Certificate_Problem_Report.html).

Subscribers and Relying Parties, Application Software Suppliers, and other third parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud,

compromise, misuse, inappropriate conduct, or any other matter related to Certificates by sending email to certificate.problem@techsource.iq

TS will validate and investigate the revocation request before acting in accordance with section 4.9.

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

1.5.3 Person Determining CPS Suitability for the Policy

Based on the compliance audits' results and recommendations, The TS 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 the CPS.

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

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

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

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

1.6 Definitions and Acronyms

1.6.1 Definitions

Applicant: The natural person that applies for (or seeks renewal of) a Certificate.

Applicant Representative: In the context of this document, the applicant representative is responsible for submitting legal entity's enrolment request as well LRAO management requests to the TS RA. He may be an LRAO himself. 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 government 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.

Legacy Profile: The S/MIME Legacy Generation profiles provide flexibility for existing reasonable S/MIME certificate practices to become auditable under the S/MIME Baseline Requirements. This includes options for Subject DN attributes, extKeyUsage, and other extensions. The Legacy Profiles will be deprecated in a future version of the S/MIME Baseline Requirements.

Mailbox-Validated (MV): Refers to a Certificate Subject that is limited to (optional) subject:emailAddress and/or subject:serialNumber attributes.

Mailbox Address: Also Email Address. From RFC 5321: "A character string that identifies a user to whom mail will be sent or a location into which mail will be deposited."

Mailbox Field: In Subscriber Certificates contains a Mailbox Address of the Subject via rfc822Name or otherName value of type id-on-SmtpUTF8Mailbox in the subjectAltName extension, or in Subordinate CA Certificates via rfc822Name in permittedSubtrees within the nameConstraints extension

Multipurpose Profile: The S/MIME Multipurpose Generation profiles are aligned with the more defined Strict Profiles, but with additional options for extKeyUsage and other extensions. This is intended to allow flexibility for crossover use cases between document signing and secure email.

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

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

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

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

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

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

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

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

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

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

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

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.

Strict Profile: The S/MIME Strict Generation profiles are the long term target profile for S/MIME Certificates with extKeyUsage limited to id-kp-emailProtection, and stricter use of Subject DN attributes and other extensions.

Subject: The Natural Person identified in a Certificate as the Subject. The Subject is either the Subscriber or a mailbox under the control and operation of the Subscriber.

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

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

Subscriber: A natural person 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 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.

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

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

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

1.6.2 Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CCTV	Closed Circuit TV
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CV	Curriculum Vitae
DBA	Doing Business As
DN	Distinguished Name
DNS	Domain Name System
FIPS	Federal Information Processing Standards
EID	Electronic Identity Card
EIDAS	Electronic IDentification, Authentication and trust Services
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IPSEC	Internet Protocol Security

ISO	International Standards Organization
ITPC	Information & Telecommunication Public Company
IT	Information Technology
LRA	Local registration Authority
LRAO	Local registration Authority officer
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

1.6.3 References

This document refers to the following:

- X.509 - The standard of the ITU-T (International Telecommunications Union-T) for Certificates.
- RFC3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Network Security
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates

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. This TS S/MIME 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.

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. In instances where no changes are required, the CPS version number is incremented, and a dated changelog entry is included to document the review.

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

2.3.1 CA Certificates

The Subordinate CA 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

Technology Source S/MIME CA maintains and publishes CRLs as follows:

- CRLs are refreshed no later than every 24 hours, even if no changes have occurred since the last CRL issuance,
- CRLs lifetime are set to 26 hours.

2.4 Access Controls on Repositories

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

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

3 Identification and Authentication

3.1 Naming

3.1.1 Type of names

The Subject names in the TS S/MIME 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.

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

CN	TS SMIME 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.

Sponsor-validated S/MIME certificates for natural persons:

Attribute	Value
GivenName	Individual's authenticated given name
SurName	Individual's authenticated surname
SERIALNUMBER (optional)	unique identifier for everyone as constructed by the RA
CN (optional)	mailbox address
O	The Subject's full legal organization name and/or an Assumed Name. If both are included, the Assumed Name SHALL appear first, followed by the full legal organization name in parentheses
OrganizationIdentifier	Registration Reference for a Legal Entity assigned in accordance with the identified Registration Scheme
Country - "C" (optional)	IQ

S/MIME CA OCSP responder certificate

Attribute	Value
CN	TS SMIME CA G1 OCSP
O	Technology Source;
Country - "C"	IQ

3.1.2 Need for Names to be Meaningful

This CA apply the following rules to ensure the use of meaningful names:

For S/MIME certificates issued to natural persons: S/MIME Certificates include a non-null Subject DN containing the verified information of the entity that sponsored the Certificate issuance and the name of the individual. The rfc822Name includes the email address controlled by the individual requesting the S/MIME Certificate, which may be replicated in the Common Name field.

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 forbidden.

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

For S/MIME certificates issued to natural persons: uniqueness is enforced through the combination of the individual's name and sponsor organization's name.

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

Subscribers may not request Certificates with any content that infringes the intellectual property rights of another entity.

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

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 LRA 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 LRA through CSRs in PKCS#10 format.

3.2.2 Authentication of Organization

Authentication of an organization identity is performed pursuant to current Iraqis legislation through the validation processes specified below, by which the TS RA enrolls the organization and performs initial identity validation of the organization and its representatives.

3.2.2.1 Authentication for Organizations

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 Domain Name(s) (domain portion of an email address) that will be listed in the Certificate by following the procedures of Sec. 3.2.3.

The TS RA ensures that any obtained validation data (regarding authority over mailbox via domain) 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 verifies the authority of the authorized representative and the certificate's requester in accordance with section 3.2.6.

3.2.2.2 Authentication for organizations applying to operate a Local registration authority (LRA)

This scenario applies to organizations wishing to issue and manage natural person certificates. The organization and its authorized representative are verified in accordance

with the process described above (section 3.2.2.1) then the authorized representative signs the LRA agreement. Upon organization's enrolment approval, the TS RA initiates an internal process whereby the organization and its LRAO officers are created on the web RA portal so that they can use their web RA account to perform certificate requests and other certificate management operations.

3.2.3 Validation of Mailbox Authorization or Control

Prior to issuing an S/MIME Certificate, the TS RA verifies that the Applicant has control over all email addresses specified in the certificate's Mailbox fields. This verification is performed by confirming:

- **Email-based mailbox control validation:** The TS RA sends a Random Value to the email address being verified. The Applicant must respond using the same Random Value, thereby proving control of the mailbox.
 - **Validity of the Random Value:** The Random Value is valid for 24 hours from the time of generation. If a response is received after the validity period, the TS RA must initiate a new validation request by generating and sending a new Random Value.

3.2.4 Authentication of Individual Identity

3.2.4.1 *Authentication for Individuals Applying for Natural Person certificates*

This section describes the process followed by an LRAO for verifying the identity of the natural persons as part of the certificate enrolment processes.

The LRAO relies on Authoritative and Supplementary evidence to perform identity verification. The types of supported evidence are listed below:

- **Authoritative Evidence:** The accepted primary evidence is the secure government-issued ID card or passport (including a chip bearing digitally signed information about the holder) which is issued with robust identity proofing, issuance, and management processes.
- **Supplementary Evidence:** Supplementary evidence is evidence used as support for the authoritative evidence (i.e. trusted registers, proof of access in particular a bank account, official document and attestations). Examples are: Human Resource (HR) attestation letters,

The identity verification process is conducted by the LRAO through an in-person meeting with the individual or an equivalent method and includes the following steps:

- a) The LRAO obtains the following individual's identity proofing Supplementary evidence from the entity HR as part of employee induction, from a direct line of business manager or from the individual himself:
- A completed and signed certificate application form.
 - An attestation Letter confirming the affiliation of the individual to the entity and providing details such that full name and date of birth, email address.
 - An email from entity representative to enrol the individual into the Web RA to enable it to benefit from an S/MIME certificate (as per the business need).
- b) The LRAO validates the identity proofing documents through a documented internal process.
- c) The LRAO verifies the link between the claimed identity and the applicant as outlined in a documented internal process.

Upon the initial approval of the individual identity, the LRA initiates a technical procedure through which the individual is enrolled into the Web RA portal with multi-factor authentication credentials that he can use to execute certificate requests and related certificate management operations.

3.2.5 Non-Verified Subscriber Information

Every subscriber information contained within a certificate issued by S/MIME CA is verified by LRAO.

3.2.6 Validation of Authority

The TS RA verifies the authority of the entity official representative as the signatory of the certificate application form (entity registration form) and the LRA agreement. The TS RA also verifies the authority of the LRAO as the person authorized to submit application requests and other certificate managements operations. Refer to sections 3.2.2.2 for further details.

3.2.7 Criteria for Interoperation

No stipulation.

3.3 Initial Identity Validation 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/LRAO checks the existence and validity of the certificate to be rekeyed 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 /LRAO to the subscriber.

3.3.2 Identification and Authentication for Re-Key after Revocation

Identification and authentication for re-keying is performed as in initial registration.

3.4 Identification and Authentication for Revocation Request

The LRAO authenticates the revocation request through one of the following methods:

- Receiving a revocation request from a pre-agreed and a concerned department with the entity (e.g., HR, direct manager of the individual) if the subscriber is terminated or changed role within the entity which would trigger the revocation request. The LRAO would have the internal means to confirm the validity of the revocation request.
- Receiving a revocation request from the subscriber through agreed channels, this may include:
 - A face-to-face visit to the LRAO office, telephone call from the subscriber where the LRAO asks an identity validation questions (e.g., employee ID, name, date of birth etc.),
 - An email from the subscriber using an email address that can be verified by the LRAO or through the web RA portal (user account)

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

Certificate applications can be initiated directly by the applicants themselves through the Web RA portal. The LRAO is authorized to approve and submit the certificate applications. The applicant is responsible for the authenticity of all data submitted as part of the certificate applications. The LRAO ensures subscriber's agreements are ratified by the applicant as part of the certificate request process. The LRAO maintains a blacklist of individuals affiliated to the entity for whom certificate requests will not be accepted.

When the applicant is the LRAO himself, only another LRAO (i.e., someone other than the LRAO identified as the applicant) is authorized to approve and submit the certificate applications.

For OCSP responder certificate: The TS RA and an authorized PKI administrator in trusted role oversee the execution of authorized internal operational ceremonies through which OCSP certificates for the S/MIME CA are issued.

4.1.2 Enrolment Process and Responsibilities

The process is described as following:

- The individual is registered into the Web RA portal.
- The individual authenticates to the Web RA portal (using multi-factor authentication).
- The individual completes a certificate request form.
- A technical process is executed that results in the personalization of the token key pair and CSR generation.
- The individual ratifies the subscriber agreement and submits the certificate request application to the LRAO.
- The LRAO is authorized to review submitted certificate requests. Upon logging into the Web RA portal, the LRAO verifies the application and performs the necessary technical steps to approve the request.
- The LRAO maintains a blacklist of individuals affiliated to the entity for whom certificate request will not be accepted.
- Before submission to the relevant CA, the TS RA performs the Email-based mailbox control validation and CAA (Certification Authority Authorization) verification.

For OSCP 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

The LRAO identifies the Subscriber based on the identifying documents and evidence that the Subscriber presents, In summary:

- a) The LRAO ensures a unique ID is assigned to each certificate application record,
- b) The LRAO 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 a blacklist, the blacklist includes the necessary details to avoid ambiguously in identifying future malicious requests,
- d) The LRAO conduct a blacklist check against his RA's own blacklist. If the applicant is in the blacklist, the certification application is rejected,
- e) The applicant signs or ratifies a dedicated subscriber agreement.
- f) The LRAO identifies the individual as described in section 3.2.4;
- g) The LRAO validates the individual's eligibility for the requested certificate according to the entity's internal processes (e.g., performing this validation through a communication with the individual's direct manager);
- h) The LRAO proceeds with the technical procedures related to approve the requested certificate
- i) Before submission to the relevant CA, the TS RA performs the Email-based mailbox control validation according to Section 3.2.3 and CAA (Certification Authority Authorization) verification according to Section 4.2.2.1.
- j) Upon successful validation, the TS RA proceeds with the technical procedures related to issuing the requested certificate.

Age of Validated Data

The TS RA / LRAO may reuse completed validations and/or supporting evidence performed in accordance with Section 3.2 within the following limits:

- **Validation authority over mailbox via domain:** 398 days prior to issuing the Certificate.
- **Validation of mailbox authorization or control via email:** 30 days prior to issuing certificate.
- **Authentication of organization identity:** 825 days prior to issuing certificate.
- **Authentication of individual identity:** 825 days prior to issuing certificate.

A prior validation is not reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

4.2.2 Approval or Rejection of Certificate Applications

The LRAO approves an application for a certificate only if the following criteria are met:

- Successful identification and authentication of all required Subscriber information according to section 3.2.

The LRAO rejects a certificate application if:

- Identification and authentication of all required Subscriber information according to Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request.

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.

4.2.2.1 Certification authority authorization (CAA)

Prior to issuing an S/MIME certificate, the TS RA officer check the DNS for the existence of a CAA record in accordance with RFC 9495 for each Mailbox Address in the subjectAltName extension of the S/MIME certificate to be issued. Technology Source processes the "issuemail" property tag. Technology Source's CAA issuer domain is "**pki.techsource.iq**".

Certificates passing the CAA check are issued within the Time to Live (TTL) of the CAA record, or 8 hours, whichever is greater.

The RA officer logs all actions related to CAA record checks and processing. Additionally, the RA officer documents any potential certificate issuances that were prevented due to a CAA record, providing sufficient detail to enable feedback to the CA/Browser Forum on the circumstances.

TS RA does not use iodef property tag of the CAA record for communicating with the contact(s) stipulated in the CAA iodef record(s)..

4.2.2.1 *Multi-perspective issuance corroboration*

Technology Source does not require CAA records to be retrieved and processed from additional remote Network Perspectives prior to certificate issuance, as the methods used for validation of Mailbox Authorization or Control do not necessitate such corroboration.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Certificate issuance by the S/MIME CA involves coordinated actions between the Local Registration Authority Officer (LRAO) and the TS RA.

The LRAO is responsible for performing the required identity verification and vetting steps in accordance with Section 4.2.1 of this CPS. This includes validating the certificate request, reviewing subscriber-provided information, and approving the application.

Following LRAO approval, the RA Officer executes the technical steps necessary to complete the validation process, including email-based mailbox control validation and Certification Authority Authorization (CAA) checks when applicable. Upon successful validation, the RA Officer submits the Certificate Signing Request (CSR) to the CA for certificate issuance.

The Certification Authority (CA) will validate the format and structure of the Certificate Signing Request (CSR) and generate a corresponding pre-certificate. The pre-certificate will undergo linting using industry-standard tools to assess its technical conformity and compliance (of each to-be-signed artifact prior to signing it), with applicable standards. Following successful validation, the final certificate will be generated in accordance with the predefined configured certificate template and made available for download from the web RA portal. The CA issues the certificate in “Active” state

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 to establish: (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

For S/MIME certificates issued to natural persons: The subscriber is notified by email that his certificate has been generated. The certificate is made available for download on his Web RA portal account.

For OCSP responder certificate: The designated administrator is notified upon receiving the certificate from TS RA team.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

For S/MIME certificates issued to natural persons: The subscriber downloads the certificate from the web RA portal then validates its content. In case of any discrepancies, the subscriber initiates a discussion with the LRAO which may lead to certificate revocation to issue a corrected certificate.

The certificate is deemed accepted if no complaints are raised by the subscriber to the LRAO within 5 business days of receiving the email notification of certificate generation.

For OCSP responder certificate: Certificate are deployed on the target key store as part of the TS internal operational ceremonies.

4.4.2 Publication of the Certificate by the CA

This CA do not publish end-user certificates apart from sharing it with the subscribers.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No 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 LRAO 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 LRAO 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

Note 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 the TS S/MIME 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 S/MIME certificates.

4.7.2 Who May Request Certification of a New Public Key

As per the initial certificate issuance.

4.7.3 Processing Certificate Re-Keying Requests

As per the initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per the initial certificate issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per the initial certificate issuance.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per the initial certificate issuance.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per the initial certificate issuance.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

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 Subscriber certificates revocation

The Subscriber's Certificate is revoked within 24 hours if one or more of the following occurs:

1. The Subscriber requests such revocation in writing.
2. The Subscriber notifies Technology Source/LRAO that the original Certificate Request was not authorized and does not retroactively grant authorization.
3. Technology Source /LRAO obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise.
4. Technology Source 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>);
5. Technology Source obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate is not relied upon.

Technology Source ensures a certificate revocation is executed within 24 hours and revokes a certificate within 5 days if one or more of the following occurs:

6. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;

7. Technology Source / LRAO obtains evidence that the Certificate was misused;
8. Technology Source /LRAO is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
9. Technology Source / LRAO is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);
10. Technology Source / LRAO is made aware of a material change in the information contained in the Certificate.
11. The Technology Source /LRAO is made aware that the Certificate was not issued in accordance with this CPS.
12. The Technology Source / LRAO determines or is made aware that any of the information appearing in the Certificate is inaccurate.
13. Technology Source's right to issue Certificates under the baseline requirements expires or is revoked or terminated, unless Technology Source has planned to continue maintaining the CRL/OCSP Repository
14. Revocation is required by the CPS; or
15. Technology Source / LRAO is made aware of 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.

4.9.1.1 Circumstances for Subordinate CA revocation

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

1. The revocation is requested in writing;
2. Technology Source notifies the Issuing CA (i.e., Root CA) that the original certificate request was not authorized and does not retroactively grant authorization;
3. Technology Source obtains evidence that the TS SMIME CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;

4. The Issuing CA (i.e., Root CA) obtains evidence that the TS SMIME CA Certificate was misused;
5. The Issuing CA (i.e., Root CA) is made aware that the TS SMIME CA Certificate was not issued in accordance with or that TS SMIME CA has not complied with this document.
6. The Issuing CA (i.e., Root CA) determines that any of the information appearing in the TS SMIME CA Certificate is inaccurate or misleading;
7. TS SMIME CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. TS SMIME CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the (i.e., Root CA) has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's (i.e., Root CA) Certificate Policy and/or Certification Practice Statement.

4.9.2 Who Can Request Revocation

Revocation can be requested by the following:

- The TS RA /LRAO in the cases described in section 4.9.1,
- The Subscriber may submit a revocation request for his own certificate,
- Any relying party or application software supplier possessing evidence of compromise of the subscriber's certificate or its usage to promote malware,
- TS 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.

Only authorized revocation requests are accepted.

4.9.3 Procedure for Revocation Request

Revocation directly by a Subscriber or a Requester:

The subscriber may submit a revocation request through the Web RA portal. Such requests will be processed automatically by the relevant Subordinate CA that issues a new CRL.

Revocation through a LRAO is conducted as follows:

- The LRAO authenticates the revocation request and validates the identity of the subscriber as described in section 3.4.
- The LRAO accesses his account on the web RA portal and issues a direct command to the correspondent CA to revoke the subscriber's certificate.

- The S/MIME CA revokes the certificate, and the certificate status is updated⁴.
- The LRAO notifies via internal communication the concerned departments (e.g. HR, direct line of business) about the completion of the certificate revocation operation.
- If applicable, the LRAO updates its internal blacklist with the details of the subscriber.

Certificate revocation handling following a certificate problem reporting:

Technology Source maintains a continuous 24/7 ability to internally respond to any high priority revocation requests and certificate problem reports provides instructions for certificate revocation and certificate problem reporting on a dedicated page in its public repository, accessible at [https://pki.techsource.iq/repository/Certificate Problem Report.html](https://pki.techsource.iq/repository/Certificate_Problem_Report.html).

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

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.

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

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 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 will be revoked 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. The S/MIME 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 S/MIME CA publishes CRLs at regular intervals. The following rules apply for the CRLs issued by this CA:

- CRLs are refreshed every 24 hours.
- CRLs 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 the S/MIME 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 offers an OCSP responder that conforms to RFC 6960 and whose certificate is signed by this 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 the S/MIME 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:

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

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

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

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements Related to Key Compromise

If TS discovers, or has a reason to believe, that there has been a compromise of the private key of the TS S/MIME CA, TS will immediately declare a disaster and invoke its business continuity plan. TS will also:

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

Parties may use the following methods to demonstrate key compromise:

- 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

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable

4.9.15 Procedure for Suspension Request

Not applicable

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

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

4.10.1 Operational Characteristics

The S/MIME CA publishes its CRLs at the public repository accessible to relying parties.

The S/MIME CA OCSP responder exposes an HTTP interface that is also publicly available to relying parties.

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

4.10.2 Service Availability

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

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

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

4.10.3 Optional Features

No stipulation

4.11 End of Subscription

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

Not supported.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Facility, Management, and Operational Controls

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

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

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

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

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

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

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

5.1 Physical Security Controls

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

5.1.1 Site Location and Construction

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

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

5.1.2 Physical Access

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

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

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

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

5.1.3 Power and Air Conditioning

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

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

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

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

5.1.6 Media Storage

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

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

5.1.7 Waste Disposal

All wastepaper and storage media created within the secure facility 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 S/MIME CA systems are routinely performed to ensure ample recovery data is available to restore the TS S/MIME CA systems when needed.

At least one full backup and several incremental backups of the TS S/MIME 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 procedural controls that apply to the primary facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

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

The following are the trusted roles for the TS S/MIME 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 or more 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 S/MIME CA staff to perform their respective functions.

5.2.4 Roles Requiring Separation of Duties

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

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

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

- Verify the Identity of Such Person: Verification of identity MUST be performed through:
- Personal (physical) presence of such person before trusted persons who perform human resource or security functions, and

- Verification of well-recognized forms of government-issued photo identification; and
- Verify the Trustworthiness of Such Person: Verification of trustworthiness includes background checks, which address at least the following, or their equivalent:
 - Criminal convictions for serious crimes,
 - Misrepresentations by the candidate,
 - Appropriateness of references, and
 - Any clearances as deemed appropriate.

5.3.2 Background Check Procedures

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

5.3.3 Training Requirements

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

The training program encompasses a diverse range of topics and is delivered by a combination of experienced TS S/MIME 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 S/MIME 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 or rotation in staff does not affect the operational effectiveness, continuity, and integrity of the TS S/MIME CA services.

5.3.6 Sanctions for Unauthorized Actions

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

5.3.7 Independent Contractor Requirements

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

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

5.3.8 Documentation Supplied to Personnel

The TS PKI GB 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 S/MIME 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 S/MIME CA systems.

Technology Source records events related to its actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved.

Technology Source makes these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.

At a minimum, each audit record includes the following:

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

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

Following events occurring in relation to the TS S/MIME CA' operations are recorded:

1. TS S/MIME CA key life cycle management 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 Certificates life-cycle management events, including:
 1. Certificate requests, renewal, and re-key requests, and revocation;
 2. All verification activities stipulated in the present CPS.
 3. Approval and rejection of Certificate Requests;
 4. Issuance of Certificates;

3. Security events, including:

1. Successful and unsuccessful PKI system access attempts.
2. PKI and security system actions performed.
3. User management operations.
4. System platform issues (e.g., crashes), hardware failures.
5. Security profile changes.
6. Relevant router and firewall activities (as described in Section 5.4.1.1); and.
7. Entries to and exits from the CA facility,

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

- CA personnel, security profiles rotations/changes.
- All versions of this CPS.
- Minutes of meetings.
- Compliance internal audit reports.
- Current and previous versions of TS S/MIME CA 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 S/MIME CA 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 ensures that the audit logs are maintained and retained for a period not less than 2 years or in accordance with section 5.5.2:

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1(1)) after the later occurrence of:
 1. The destruction of the CA Private Key; or
 2. 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:

1. Backup media are stored locally in the TS Subordinate CAs main site, in a secure location,
2. 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 S/MIME 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 S/MIME 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 S/MIME CAs retains:

- All archived documentation related to the security of CA Systems, certificate management systems (as set forth in Section 5.5.1),
- 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:
 - such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates, or
 - 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 S/MIME 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 TS S/MIME CA key is changed with a frequency that ensures the TS S/MIME CA has a validity period greater than the maximum lifetime of Subscriber certificate after the latest Subscriber certificate issuance.

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

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 Computing Resources, Software, and/or Data are Corrupted

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

The TS 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 Entity Private Key Compromise Procedures

For Subscribers key compromise, see section 4.9.

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

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

5.7.4 Business Continuity Capabilities after a Disaster

In case of a disaster, corrupted servers, software or data, the TS disaster recovery and business continuity plan is triggered to restore the minimum required operational capabilities of the TS S/MIME 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 S/MIME 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 S/MIME 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 S/MIME 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 at the original or a remote site.

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

5.8 CA or RA Termination

The provision of the TS S/MIME 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 S/MIME 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 S/MIME 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 S/MIME CA records to an appropriate custodian,
- Plan to assist (as much as possible) TS's subscribers with a transition to another TSP,
- Revoke all certificates, issued by this CA , that remain unrevoked or unexpired at the end of the notice period, whether the subscribers have requested a revocation.
- Undertake the necessary measures to ensure that discontinuing its operations does not cause disruption to its subscribers and relying parties.
- Arrangements to adequately ensure the ongoing maintenance of its systems and security measures for sensitive and accurate data.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The TS S/MIME CA key pair is generated within the memory of an HSM certified/ validated to FIPS 140-2 Level 3.

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

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

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

6.1.1.2 Subscriber's Key Pair Generation

The subscriber keys are generated according to the below requirements:

- ***S/MIME certificates generated on cryptographic token:*** Subscribers' key pairs generated within the memory of hardware cryptographic devices conforming to FIPS 140 Level 2 and that prevents exportation. Key pairs shall be generated using key generation algorithm and key sizes as specified under sections 6.1.5 and 6.1.6 of this CPS.

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>).

6.1.2 Private Key Delivery to Subscriber

Technology Source does not generate Subscribers' private keys for publicly trusted S/MIME certificates, nor does it perform key escrow, recovery, or backup.

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

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 S/MIME CA public key certificates are published on the TS public repository.

6.1.5 Key Sizes

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

The TS S/MIME CA keys size is 384-bit ECDSA.

6.1.6 Public Key Parameters Generation and Quality Checking

6.1.6.1 TS S/MIME CA

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

6.1.6.2 Subscribers

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

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

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

The TS S/MIME CA staff are assigned to the trusted roles by the TS PKI GB ensuring segregation of duties and enforcing the principles of multi control and split knowledge. Multi-person control of the TS S/MIME CA private keys is achieved using an "m-of-n" split key knowledge scheme. A certain number of persons 'm' (at least two (2)), out of 'n' persons (three (3) persons), the total number of key custodians, need to be concurrently present, together with HSMs administrators to activate or re-activate the Subordinate CA private key.

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

6.2.3 Private Key Escrow

Private keys of the S/MIME CA are not escrowed.

6.2.4 Private Key Backup

The TS S/MIME CA 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 S/MIME CA key generation ceremonies. TS S/MIME CA keys are backed up under the same multi-person control and split knowledge as the primary key. The recovery operation of the backup key is subject to the same multi-person control and split knowledge principles.

The overall TS S/MIME CA key ceremony procedure includes the physical transport of the TS S/MIME 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

This CA does not archive the S/MIME CA 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 private 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 S/MIME 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 their private key according to the obligations articulated in the Subscriber Agreement.

Subscribers plug in their PKI hardware token to the appropriate reader or slot and when asked they provide the PIN associated with the PKI hardware token to activate their private key.

6.2.9 Method of Deactivating Private Key

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

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

6.2.10.2 Subscriber

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

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

See clause 5.5 for archival conditions.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The TS S/MIME CA 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 S/MIME certificate 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.

Subscriber certificates **MUST NOT** have a Validity Period greater than 825 days.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 TS S/MIME CA

The CA 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 protect 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 S/MIME 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. Technology Source system configurations are regularly checked, with a maximum interval of one week between checks.

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

6.6.3 Life Cycle Security Controls

Refer to 6.5.1.

6.7 Network Security Controls

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.

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

6.8 Timestamping

The TS S/MIME CA components are regularly synchronized with a reliable time service. The time-stamping service 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

TS complies with RFC 5280 and Baseline Requirements in all certificates it issues. Subordinate CA and end entity certificates include an Extended Key Usage extension containing the key usage purpose id-kp-emailProtection. The special KeyPurposeId anyExtendedKeyUsage cannot be included in the certificates.

7.1.3 Algorithm Object Identifiers

Certificates are issued by the CA with algorithms indicated by the following OIDs

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

7.1.4 Name Forms

7.1.4.1 Name Encoding

TS 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 S/MIME certificates is specified in the table below. TS issues Certificates where the contents of the Subject DN fields are compliant with their corresponding definitions stated in section 7.1.4 of the Baseline Requirements.

Certificate Type	Subject DN	Subject Name	Alternative
S/MIME	- commonName - organizationName - OrganizationIdentifier - givenName - Surname	rfc822name	

	- SERIALNUMBER - countryName	
--	---	--

7.1.4.3 Subject Information - TS Subordinate CA Certificate

In the TS S/MIME CA; 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

Not applicable.

7.1.6 Certificate Policy Object Identifier

Certificate policy object identifiers are used as per RFC 3739 and RFC 5280.

TS S/MIME CA uses use certificate policy object identifiers that are defined for the Iraq National PKI OID scheme. Refer to the certificate template in section 7.1.10 & 7.1.11 for more details.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

The use of policy qualifiers defined in RFC 5280 is supported. Used policy qualifiers are specified as part of the certificates profiles in Section 7.1.10 and 7.1.11.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.1.10 TS S/MIME CA Certificate Profile

CE² = Critical Extension O/M³: O = Optional M = Mandatory

CO⁴ = 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)

Certificate Practice Statement for the Technology Source S/MIME CA

OrganizationName		M	S	Informatics & Telecommunications Public Company	UTF8 encoded
CommonName		M	S	ITPC SMIME 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 SMIME CA G1	UTF8 encoded
SubjectPublicKeyInfo	False	M	D		
AlgorithmIdentifier		M	D	ECDSA (OID: 1.2.840.10045.2.1)	
				secp384r1 (OID: 1.3.132.0.34)	
SubjectPublicKey		M	D	Value of the key	
Extensions					
Authority Properties					

Certificate Practice Statement for the Technology Source S/MIME CA

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	
AuthorityInfoAccess	False	M	S		
AccessMethod		M	S	<i>Id-ad-2 1 id-ad-ocsp OID i.e., 1.3.6.1.5.5.7.48.1 (ca ocsp)</i>	OCSP Responder field
AccessLocation		M	S	http://ocsp.itpc.gov.iq	OCSP responder URL
AccessMethod		M	S	<i>Id-ad-2 2 id-ad-caIssuers OID i.e., 1.3.6.1.5.5.7.48.2 (ca cert)</i>	CA Issuers field
AccessLocation		M	S	http://pki.itpc.gov.iq/repository/cert/smime_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/smime_root_ca.crl	CARL 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	

Certificate Practice Statement for the Technology Source S/MIME CA

Policy Properties					
certificatePolicies		False	M	S	
	PolicyIdentifier		M	S	2.16.368.1.1.1.1
	policyQualifiers:policyQualifierId		M	S	id-qt 1
	policyQualifiers:qualifier:cPSur i		M	S	https://pki.itpc.gov.iq/repository/cps
certificatePolicies		False	M	S	
	PolicyIdentifier		M	S	2.23.140.1.5.3.3
certificatePolicies		False	M	S	
	PolicyIdentifier		M	S	2.23.140.1.5.4.3
certificatePolicies		False	M	S	
	PolicyIdentifier		M	S	2.23.140.1.5.2.3
certificatePolicies		False	M	S	
	PolicyIdentifier		M	S	2.23.140.1.5.1.3
Extended Key Usage Properties					
extKeyUsage		False	M	S	
	emailProtection		M	S	True
Basic Constraints Properties					
basicConstraints		True	M	S	
	cA		M	S	True
	pathLenConstraint		M	S	0

7.1.11 S/MIME Certificates Profile

CE² = Critical Extension O/M³: O = Optional M = Mandatory

CO⁴ = Content: S = Static, D = Dynamic

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

Certificate Practice Statement for the Technology Source S/MIME CA

					PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Technology Source	UTF8 encoded
CommonName		M	S	TS SMIME 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	
Subject	False				
CountryName		M	S	Country Name	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280). If present shall be "IQ"
OrganizationName		M	D	The Subject's full legal organization name and/or an Assumed Name. If both are included, the Assumed Name SHALL appear first, followed by the full legal organization name in parentheses.	UTF8 encoded
OrganizationIdentifier		M	D	Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme.	a PrintableString or UTF8String

Certificate Practice Statement for the Technology Source S/MIME CA

GivenName		M	D	Given Name of the Subject	UTF8 encoded
Surname		M	D	Surname of Subject	UTF8 encoded
SERIALNUMBER		M	D	an identifier assigned by the CA or RA to identify and/or to disambiguate the Subject	PrintableString encoded
CommonName		M	D	Mailbox address	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA (OID: 1.2.840.113549.1.1.1)	
				Null	
SubjectPublicKey		M	D	Public Key Key length: Key length: 2048 or 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate CA public key	
AuthorityInfoAccess	False	M			
AccessMethod		M	S	<i>Id-ad-2 1 id-ad-ocsp OID i.e., 1.3.6.1.5.5.7.48.1 (ca ocsp)</i>	OCSP Responder field
AccessLocation		M	S	http://ocsp.techsource.iq	OCSP responder URL
AccessMethod		M	S	<i>Id-ad-2 2 id-ad-caIssuers OID i.e., 1.3.6.1.5.5.7.48.2 (ca cert)</i>	CA Issuers field

Certificate Practice Statement for the Technology Source S/MIME CA

	AccessLocation		M	S	http://pki.techsource.iq/repository/certs/smime_ca.p7b	Subordinate CA Certificate/Chain download URL over HTTP
	crldistributionPoints	False	M			
	DistributionPoint		M	S	http://pki.techsource.iq/repository/crlsCRLS/smime_ca.crl	CRL download URL.
	Subject Properties					
	SubjectKeyIdentifier	False	M			
	KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
	Key Usage Properties					
	keyUsage	True	M			
	digitalSignature, keyEncipherment		M	S	True	
	Policy Properties					
	certificatePolicies	False	M			
	PolicyIdentifier		M	S	2.16.368.1.2.1.4	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSur i		M	S	https://pki.techsource.iq/repository/cps	
	certificatePolicies	False	M			
	PolicyIdentifier		M	S	2.23.140.1.5.3.3	Sponsor-validated Strict
	certificatePolicies	False	M			

Certificate Practice Statement for the Technology Source S/MIME CA

	PolicyIdentifier		M	S	2.16.368.1.1.3.1.3	
	Extended Key Usage Properties					
	extKeyUsage	False	M			
	emailProtection		M	S	True	
	Subject Alternative Name Properties					
	subjectAlternativeName	False	M			
	rfc822name		M	D	One or more email addresses of the certificate owner	

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 SMIME CA G1	
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime

Certificate Practice Statement for the Technology Source S/MIME CA

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

7.2.1 Version Number(s)

CAs supports X.509 version 2 CRLs (see 7.2 above)

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

The OCSP profile complies with the requirements of RFC 6960.

CE² = Critical Extension

O/M³: O = Optional M = Mandatory

CO⁴ = 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".

Certificate Practice Statement for the Technology Source S/MIME CA

					PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Technology Source	UTF8 encoded
CommonName		M	S	TS SMIME 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 SMIME CA G1 OCSP	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		M			
Subject Properties					
SubjectKeyIdentifier	False	M			

Certificate Practice Statement for the Technology Source S/MIME CA

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

OCSP response format

The below profile describes OCSP response according to RFC 6960:

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

ArchiveCutoff ⁵	the CA's certificate "notBefore" time and date value	According to RFC 6960 clause 4.4.4. "archive cutoff" date set to the CA's certificate "notBefore" time and date value According to ETSI EN 319 411-2 / CSS-6.3.10-10.
extended-revoked definition	Null	the responder supports the extended definition of the "revoked" status to also include non-issued certificates
signatureAlgorithm	Sha384withRSAEncryption	Signing algorithm
signature		signature value
certs		Certificate corresponding to the private key used to sign the response. Only OCSP responder certificate is included in the OCSP response.

7.3.1 Version Number(s)

As per the OCSP certificate profile, section 7.3.

7.3.2 OCSP Extensions

As per the OCSP certificate profile, section 7.3.

⁵ In the current implementation of the OCSP, the "ArchiveCutoff" extension is included in OCSP responses only for certificates that have expired

8 Compliance Audit and Other Assessments

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

8.1 Frequency or Circumstances of Assessment

Technology Source organizes an external WebTrust 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.

The TS compliance function executes yearly verifications on LRA organizations to verify that personnel (LRAOs) involved in verification duties and related certificate issuance comply with the provisions listed in this CPS.

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

8.2 Identity/Qualifications of Assessor

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

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

8.3 Assessor's Relationship to Assessed Entity

For internal audit, the TS PKI GB has its own audit function that is independent of the TS PKI operations team.

External auditors are independent third-party WebTrust practitioners 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 are audited for compliance to the following standards:

- WebTrust Principles and Criteria for Certification Authorities.
- WebTrust Principles and Criteria for Certification Authorities – Network Security
- WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates

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

8.6 Communication of Results

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

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

8.7 Self-Audits

The TS PKI GB through its compliance function, monitors and strictly controls its adherence to the procedures listed in this CPS document by performing:

- Self-audits on at least a quarterly basis against a randomly selected sample including a minimum of the greater of thirty (30) Certificates or three percent (3%) of the

Certificates issued by S/MIME CA during the period commencing immediately after the previous self-audit sample was taken.

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

TS ensures that the TS S/MIME CA is covered by existing insurance provisions.

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities

Refer to 9.6.1

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

TS considers the following as confidential information:

- 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

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

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

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

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

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

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

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.

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

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

- The communications between the TS RA systems and the subscribers.
- The communications between the TS RA and the TS S/MIME 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

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

No stipulation

9.5 Intellectual Property Rights

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

By issuing a Certificate, the S/MIME 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 S/MIME 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 Mailbox Address:** That, at the time of issuance, the S/MIME CA (i.) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Mailbox Addresses listed in the Certificate's subject field and subjectAltName extension (or 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 CP and/or CPS;
- **Authorization for Certificate:** That, at the time of issuance, the S/MIME 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 S/MIME 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 S/MIME 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 S/MIME 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 S/MIME 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 S/MIME CA will revoke the Certificate for any of the reasons specified in these Requirements

9.6.2 RA Representations and Warranties

TS 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 the S/MIME 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 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 the S/MIME CA,

9.6.4 Relying Party Representations and Warranties

Relying Parties who rely upon the certificates issued under TS:

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

9.6.5 Representations and Warranties of Other Participants

No stipulation

9.7 Disclaimers of Warranties

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

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

9.8 Limitations of Liability

- TS will not incur any liability to Subscribers to the extent that such liability results from their negligence, fraud, or wilful misconduct,
- TS assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under this CPS for any use other than in accordance with this document. The Subscribers will immediately indemnify TS from and against any such liability and costs and claims arising there from,
- TS will not be liable to any party whosoever for any damages suffered whether directly or indirectly because of an uncontrollable disruption of its services,
- 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 TS,
- 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
- TS denies any financial or any other kind of responsibility for damages or impairments resulting from the TS S/MIME CA' operations.

9.9 Indemnities

Note 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 S/MIME CAs' 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 S/MIME CA' services are compliant to relevant and applicable laws of the Republic of Iraq.

9.16 Miscellaneous Provisions

9.16.1 Entire agreement

No stipulation

9.16.2 Assignment

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

9.16.3 Severability

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

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

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

The TS will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS. Any modification to the TS practice enabled under this section will be discontinued if 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

Note Applicable.