Application for Code Signing Certificate

Date: ____/____/20____
(dd/mm/yyyy)

Purpose

Tick one of the below options for which you are submitting the request. Submit a separate form for each purpose:

☐ Request a new certificate

☐ Revoke an existing certificate

Entity Legal Information

Provide the legal information of the Entity/Organization as it exists in the Iraqi authoritative source (such as the Official Gazette of Iraq for government entities and/or *Iraqi Incorporating or Registration Agency)*.

Organization Name (legal name)	
organizationIdentifier[1]	
Address	
City	
State/Province	
Country	Iraq
Phone Number	
Fax Number	
Email Address	

[1] VAT number assigned by the national tax authority. In the case of a government entity with no such identifier, this field is left empty.

Certificate Details

Provide the Subject Distinguished Name details for the requested certificate:

Common Name (CN)	
Organization (O)	
State/ Province (S) (provide either state/ province or locality)	
Locality (L) (provide either state/ province or locality)	
Country (C)	Iraq

Certificate Purpose (description of the planned usage of the certificate)

____

____

____

Revocation Details (fill this section only if "Revoke an existing certificate" purpose is selected)

Certificate Serial Number: ____

Revocation Reason: ____

____

____

Key Pair Generation

☐ Code signing key pair is generated on a FIPS 140-2 level 3, Common Criteria EAL 4+, or equivalent.

Applicant Representative

Applicant Representative Name: ____

☐ I hereby confirm that the information provided herein is accurate, correct, and complete and that the documents submitted along with this application form are genuine

____

Applicant Representative Signature

Official Representative

Official Representative Name: ____

☐ I/We hereby approve this request and confirm that the information provided herein is accurate, correct, and complete and that the documents submitted along with this application form are genuine

____________________________________ __________________________

Official Representative Signature Stamp

Agreement Terms and Conditions

1. Definitions

The following definitions are used throughout this agreement.

"Applicant" means the natural person that has the authority to authorize certificate request originating from an entity. He is the legally authorized official representative of the entity. In the remainder of this document, the words Applicant and Official Representative are used interchangeably.

"Applicant Representative" means a natural person who is either the Applicant or employed by the Applicant: (i) who signs and submits or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant. I n the context of this CPS, the applicant representative is in charge of submitting certificate requests and certificate revocation requests on behalf of the applicant.

"**Certificate**" means an electronic document that uses a digital signature to connect a public key with an identity (person or organization) and, at least, states a name or identifies the issuing certificate authority, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and contains a digital signature of the issuing certificate authority.

"**Certificate Application**" means a request to a CA for the issuance of a Certificate.

"**Certification Authority**" or "CA" means an entity authorized to issue, suspend, or revoke Certificates. For purposes of this Agreement, CA shall mean Technology Source.

"**Certificate Policy**" or "**CP**" means a document, as revised from time to time, representing the set of rules that indicates the applicability of a Certificate issued by Technology Source to a subscriber.

"**Certification Practice Statement**" or "**CPS**" means a document, as revised from time to time, representing a statement of the practices a CA employs in issuing Certificates. Technology Source CPSs are published at Technology Source public repository at the address at https://twokeyok.iq

"**Intellectual Property Rights**" means any and all now known or hereafter existing rights associated with intangible property, including, but not limited to, registered and unregistered, trademarks, trade dress, trade names, corporate names, logos, inventions, patents, patent applications, software, know-how and all other intellectual property and proprietary rights (of every kind and nature throughout the universe and however designated).

"**Public Key Infrastructure**" or "**PKI**" means 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. In the context of this agreement, PKI shall refer to the PKI operated by Technology Source to enable the deployment and use of Certificates issued by the Issuing CAs.

"**Registration Authority**" or “**RA**” means a 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 Agreement, the RA term refers to Technology Source internal RA that is responsible for exposing and fulfilling the certifications services from Technology Source CAs.

"**Relying Party**" A recipient of a certificate who acts in reliance on that certificate/digital signatures verified using that certificate.

"**Repository**" A trustworthy system for storing and retrieving certificates or other information relevant to certificates. Technology Source public repository is accessible at the address at https://twokeyok.iq

"**Services**" mean, collectively, the services offered by Technology Source to Subscribers in delivering digital certificate issuing and revocation services together with the related supporting functions.

"**Subscriber**" means Legal Entity to whom a Certificate is issued and who is legally bound by this Subscriber Agreement.

“**Subject**” means the device, system, unit, or Legal Entity identified in a Certificate as the Subject. In the context of this agreement, Subject populate the certificates issued by Technology Source Issuing CAs depending on the type of certificates.

“Web RA” means the application exposed by TS RA to Applicants.

2. Services Provided by Technology Source

After acceptance of this Agreement and payment of applicable fees, Technology Source shall provide the following services from the time of issuance of the Certificate:

- **Online certificate Status Protocol (OCSP) services and responses and certificate revocation list (CRL)**
  - CRLs for any Certificate containing a CRL Certificate distribution point (CDP extension).
  - OCSP responders for any Certificates containing an OCSP responder URL (AIA extension).
- **Certificates revocation services**
  - Technology Source may revoke a certificate for the circumstances specified in the CPS or if Technology Source receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under this Subscriber Agreement.
- **Key Generation**
  - Technology Source does not generate Key Pairs for publicly trusted SSL certificates.
- **Timestamping Services**
  - Technology Source offers two non-chargeable TSA services to timestamp code and document's digital signatures. Technology Source reserves the right to withdraw the service or charge additional fees for the service depending on the business need.
- **Publishing relevant agreements, policies, and practice statements**
  - Technology Source publishes Information about its CAs Certificates, CRLs and applicable CP & CPS documents on a repository that is publicly accessible at https://twokeyok.iq. Technology Source also publishes other relevant documents, and agreements (e.g., Subscriber, LRA and Relying Party agreements etc.) on the same repository.
- **Helpdesk service to respond to certificate problem requests**
  - Technology Source provides a help desk service to respond to the complaints or suspected Private Key compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates at any time, or any other matter related to Certificates by sending email to Info@techsource.iq

3. Contact Information

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

Technology Source PKI Governance Board
Technology Source,
Baghdad-Four streets- nearby AL-maamon high school
Email: muhanad.ali@techsource.iq
Phone no.: +9647726695600 / +9647842002124

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

4. Subscriber’s Obligations

4.1. Certificate requests

The Subscriber accepts the Terms and Conditions of this Subscriber Agreement and shall adhere to the requirements provided in the corresponding Technology Source CPS.

The Subscriber has the right to submit an application for issuing a Certificate using the processes and systems made available by Technology Source as documented in the provided relevant Subscriber manual.

4.2. Exclusive Control

The Subscriber acknowledges and asserts that they have exclusive control of the domain(s) or IP Address(es) listed in the SubjectAltName(s) for which they are applying for the SSL/TLS certificate.

The Subscriber acknowledges and asserts that they have exclusive control of the e-mail address for which they are applying for a S/MIME certificate.

Regardless of the certificate type, should the Subscriber cease to exclusively own the domain, e-mail address or other identifying information, the Subscriber shall immediately inform Technology Source who will promptly revoke the certificate in accordance with the relevant CPS.

4.3. Data Accuracy

The Subscriber shall provide accurate and complete information when requesting a certificate. The Subscriber shall refrain from submitting to Technology Source any material that contains statements that violate any law or the rights of any party. This includes no misleading information within the Subject:organizationName and the Subject:organizationalUnitName attributes.

4.4. Key Generation and Usage

Trustworthy systems and methods shall be used to generate public-private key pairs.

- A key length and algorithm must be used which is recognized as being fit for purpose for the Digital Signature,
- The Subscriber shall ensure that the Public Key submitted to Technology Source corresponds to the Private Key used,
- The Subscriber shall exercise appropriate and reasonable care to avoid unauthorized use of its Private Key,
- The Subscriber maintains reasonable measures to maintain sole control, keep confidential, and properly always protect the Private Key that corresponds to the Public Key to be included in the requested certificate.
- The Subscriber shall use the provided certificate(s) solely in compliance with all applicable laws and this Subscriber Agreement. Under no circumstances shall a certificate be used for criminal activities such as phishing attacks, fraud, certifying or signing malware etc.

For Code Signing

Subscriber confirms that Subscriber will use one of the following options to generate and protect their Code Signing Certificate Private Keys in a Hardware Crypto Module with a unit design form factor certified as conforming to at least FIPS 140-2 Level 2 or Common Criteria EAL 4+:

- Subscriber uses a Hardware Crypto Module meeting the specified requirement.
- Subscriber uses a cloud-based key generation and protection solution with the following requirements:
  - Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements.
  - Subscription at the level that manages the Private Key must be configured to log all access, operations, and configuration changes on the resources securing the Private Key.
- Subscriber uses a Signing Service which meets the requirements of Section 6.2.7.3 of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates".

At any time during the application and life cycle of the Certificate, Subscriber must be able to, on request of Technology Source, present proof that Key Pair is generated and protected in accordance with these requirements. Failure to provide such evidence might result in revocation of the Certificate.

4.5. Certificate Acceptance

The Subscriber shall not use the certificate until it has reviewed and verified the accuracy of the data incorporated into the certificate.

4.6. Certificate Usage

The Subscriber undertakes to use the Certificates received from Technology Source only for the intended uses as specified by the corresponding CPS.

4.7. Notification and revocation

The Subscriber undertakes to promptly cease using the certificate and its associated Private Key, and promptly request Technology Source to revoke the certificate, if:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key of the certificate's "Subject",
- The Subscriber indicates that the original certificate Signing Request (CSR) was not authorized and does not retroactively grant authorization,
- In relation to code signing, the Subscriber has signed code containing malicious code or serious vulnerabilities,
- The Subscriber has breached a material obligation of the relevant Issuing CA's CPS,
- The Subscriber requests in writing that the CA revoke the certificate,
- The performance of a person's obligations under the CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, another person's information is materially threatened or compromised,
- There has been a modification of the information regarding the "Subject" of the certificate,
- This Subscriber Agreement has been terminated,
- The affiliation between the "Subject" of the certificate with the Subscriber is terminated or has otherwise ended,
- The information within the certificate, other than non - verified "Subscriber Information" contained in the "O" or "OU" field, is incorrect or has changed,
- Termination of use of the Certificate

A Certificate may be revoked for the following reasons. If the situation is that multiple revocation reasons apply, the revocation reason of higher priority (as per the order of the following list) should be indicated:

a) **keyCompromise** (RFC 5280 CRLReason #1): The Subscriber must choose the "keyCompromise" revocation reason when they have reason to believe that the private key of their Certificate has been compromised, e.g., an unauthorized person has had access to the private key of their Certificate.

b) **cessationOfOperation** (RFC 5280 CRLReason #5): The Subscriber should choose the "cessationOfOperation" revocation reason when they no longer own all of the domain names in the Certificate or when they will no longer be using the Certificate because they are discontinuing their website.

c) **affiliationChanged** (RFC 5280 CRLReason #3): The Subscriber should choose the "affiliationChanged" revocation reason when their organization's name or other organizational information in the Certificate has changed.

d) **superseded** (RFC 5280 CRLReason #4): The Subscriber should choose the "superseded" revocation reason when they request a new Certificate to replace their existing Certificate.

e) **No reason provided** or **unspecified** (RFC 5280 CRLReason #0): When the reason codes above do not apply to the revocation request, the Subscriber must not provide a reason other than "unspecified".

4.8. Permission to publish Information

The Subscriber allows Technology Source to publish the serial number of the Subscriber's certificate in connection with the dissemination of CRL and OCSP services.

5. Certificate Transparency

To ensure Certificates function properly throughout their lifecycle, Technology Source may log SSL Certificates with a public Certificate transparency database. Because this will become a requirement for Certificate functionality, Subscriber cannot opt out of this process. Log server information is publicly accessible. Once submitted, information cannot be removed from a log server.

6. Disclaimer of Warranty

Within the limitations of the laws, Technology Source cannot be held liable (except in case of fraud or deliberate abuse) for:

- Profit loss
- Loss of data
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificate or digital signatures.
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the applicant or if it is the result of negligence or with intent to deceive Technology Source, or any person receiving or relying on the certificate.
- Any liability incurred because of the applicant breaking any laws applicable in Iraq, including those related to intellectual property protection, viruses, accessing computer systems, etc.
- The failure to perform if such failure is occasioned by force majeure.

7. Privacy

Technology Source observes personal data privacy rules and privacy rules as specified in relevant CPS documents.

Only limited trusted personnel from Technology Source are permitted to access Subscriber's private information for the purpose of certificate lifecycle management.

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

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

Technology Source will not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. When Technology Source releases private information, Technology Source will ensure through reasonable means that this information is not used for any purpose apart from the requested purposes. All communications channels with Technology Source shall preserve the privacy and confidentiality of any exchanged private information.

8. Term and Termination

This agreement shall terminate at the earliest when:

- The expiry date of any Certificate issued to the subscriber,
- Failure by the Subscriber to perform any of its material obligations under this Subscriber Agreement.

8.1. Effect of termination

Upon termination of this Subscriber Agreement for any reason, Technology Source may revoke the Subscriber's certificate in accordance with the corresponding CPS.

9. Miscellaneous Provisions

9.1. Governing Laws

The laws of the republic of Iraq shall govern the enforceability, construction, interpretation, and validity of the present Agreement.

9.2. Entire Agreement

This Agreement constitutes the entire agreement between the parties and supersedes all prior understandings, oral or written, between the parties.

9.3. Dispute Resolution

All disputes associated with the provisions of the Technology Source services shall be first addressed by the TS PKI GB (i.e., Legal function). If mediation by the TS PKI GB (i.e., Legal function) is not successful, then the dispute will be escalated to the ITPC PMA and eventually adjudicated by the relevant courts of Iraq.

9.4. Severability

If any provision of this Agreement, or the application thereof, shall for any reason and to any extent, be invalid or unenforceable, the remainder of this Agreement and application of such provision to other persons or circumstances shall be interpreted so as best to reasonably effect the intent of the parties hereto.

9.5. Force Majeure

Technology Source shall not be liable for any losses, costs, expenses, liabilities, damages, or claims arising out of or related to delays in performance or from failure to perform its obligations if such failure or delay is due to circumstances beyond Technology Source's reasonable control, including without limitation, acts of any governmental body, war, insurrection, sabotage, embargo, fire, flood, strike or other, interruption of or delay in transportation, unavailability of, interruption or delay in telecommunications or third party services.

Official Representative Name: ______________________________________

☐ I hereby acknowledge that I have read, understand, and agree to the terms and conditions of this subscriber agreement

___________________________________ ___________________________

Official Representative Signature Stamp