Subscriber Agreement

for Legal Person Certificates

Document Control

Approved By	Owner	Version	Date of Approval
PKI Director	ECAC	2.0	11/12/2024
PKI Director	ECAC	2.1	08/12/2025

Change History

Ver. No	Date	Changes Description	Approved By
2.0	11/12/2024	Issued Version	PKI Director
2.1	08/12/2025	Annual review and update. No changes applied.	PKI Director

Table of Contents

1 Definitions 3
2 Service Provided by ECAC 4
3 Contact Information 5
4 Subscriber's Obligations 5
4.1 Certificate Requests 5
4.2 Exclusive Control 6
4.3 Data Accuracy 6
4.4 Key Generation and Usage 6
4.5 Responsiveness 7
4.6 Certificate Acceptance 7
4.7 Certificate Usage 7
4.8 Notification and Revocation 7
4.9 Permission to Publish Information 9
5 Disclaimer of Warranty 9
6 Privacy 9
7 Term and Termination 10
7.1 Effect of Termination 10
8 Miscellaneous Provisions 10
8.1 Governing Laws 10
8.2 Entire Agreement 10
8.3 Dispute Resolution 10
8.4 Severability 10
8.5 Force Majeure 11
9 Signature 11

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.

"**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 ECAC.

"**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 ECAC 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. ECAC CPSs are published at the public repository at the address at https://ecac.pki.gov.pk

"**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 ECAC to enable the deployment and use of Certificates issued by the Subordinate 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 ECAC internal RA that is responsible for exposing and fulfilling the certifications services from ECAC's Subordinate CAs.

"**Relying Party**" Any natural person or Legal Entity that relies on a Valid Certificate.

"**Repository**" A trustworthy system for storing and retrieving certificates or other information relevant to certificates. ECAC's public repository is accessible at the address at https://ecac.pki.gov.pk

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

"**Subscriber**" means the 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 ECAC's Subordinate CAs depending on the type of certificates.

"ECAC Web RA" means the application exposed by the RA system to Applicants.

2 Service Provided by ECAC

After acceptance of this Agreement, ECAC shall provide the following services:

- **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 issuance services**
    - ECAC exposes the Subordinate CAs certificate management functions through a web-based service referred to as the Web RA portal, which is accessible 24/7. Subscribers are enrolled in the Web RA portal to enable them to manage their own certificates.
- **Certificates revocation services**
    - ECAC may revoke a certificate for the circumstances specified in the CPS or if ECAC receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under this Subscriber Agreement.
- **Key generation**
    - ECAC does not generate Key Pairs for publicly trusted SSL certificates.

- **Timestamping Services**
    - ECAC offers a non-chargeable TSA service for timestamping digital signatures on code and documents. ECAC 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**
    - ECAC publishes Information about its Subordinate CAs Certificates, CRLs and applicable CP & CPS documents on a repository that is publicly accessible at https://ecac.pki.gov.pk. ECAC 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**
    - ECAC 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 ecac.certification.problem@pki.gov.pk

3 Contact Information

The following address is where you can get in touch with the ECAC PMA.

Policy Management Authority
Electronic Certification Accreditation Council (ECAC),
5th Floor NTC HQ Building, G-5/2,
Islamabad, Pakistan
Tel: +92 51 9245739
Email: ecac.certification.info@pki.gov.pk

The PMA 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 ECAC's CPS.

The Subscriber has the right to apply for issuing a Certificate using the processes and systems made available by ECAC 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)[1] 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 ECAC 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 ECAC 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 ECAC 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 EV and Non-EV Code Signing

[1] In case of OV SSL certificates

Subscriber confirms that it 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 ECAC, 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 Responsiveness

The Subscriber shall provide the information requested by ECAC in connection with a known or suspected compromise of the Private Key(s). The Subscriber shall respond to ECAC's instructions concerning any Private Key(s) compromise within 24 hours, including during non-business hours.

4.6 Certificate Acceptance

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

4.7 Certificate Usage

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

4.8 Notification and Revocation

The Subscriber undertakes to promptly cease using the certificate and its associated Private Key, and promptly request ECAC 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 either signed code containing malicious components or serious vulnerabilities, or has failed to demonstrate that the code signing Key Pair was generated and protected in compliance with the requirements outlined in Section 4.4
- The Subscriber has breached a material obligation of the relevant Subordinate CA's CPS,
- The Subscriber requests in writing that the Subordinate 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".

4.9 Permission to Publish Information

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

5 Disclaimer of Warranty

Within the limitations of the laws, ECAC 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 ECAC, or any person receiving or relying on the certificate.
- Any liability incurred because of the applicant breaking any laws applicable in the Islamic Republic of Pakistan, including those related to intellectual property protection, viruses, accessing computer systems, etc.
- The failure to perform if such failure is occasioned by force majeure.

6 Privacy

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

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

ECAC 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 ECAC to Subscribers except for information about themselves and only covered by the contractual agreement between the ECAC and the Subscribers.

ECAC will not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. When ECAC releases private information, ECAC will ensue through reasonable means that this information is not used for any purpose

apart from the requested purposes. All communications channels with ECAC shall preserve the privacy and confidentiality of any exchanged private information.

7 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.

7.1 Effect of Termination

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

8 Miscellaneous Provisions

8.1 Governing Laws

The laws of the Islamic Republic of Pakistan shall govern the enforceability, construction, interpretation, and validity of the present Agreement.

8.2 Entire Agreement

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

8.3 Dispute Resolution

All disputes associated with the provisions of the ECAC services, shall be first addressed by the PMA (i.e., Legal function). If mediation by the PMA (i.e., Legal function) is not successful, then the dispute will be adjudicated by the relevant courts of the Islamic Republic of Pakistan.

8.4 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.

8.5 Force Majeure

ECAC 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 ECAC'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.

9 Signature

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