Pakistan National PKI

Relying Party Agreement

Document Control

Prepared / Updated By	Reviewed By	Approved By	Owner	Version	Date of Approval
			ECAC	2.0	

Change History

Vr. No	Date	Changes Description	
2.0	11/12/2024	Final Draft Version	Touir Mustapha

Document Approval

Vr. No	Approver (Name/Title)	Signatures
2.0	PMA	Date:

Table of Contents

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.

2 Notice

YOU MUST READ THIS RELYING PARTY AGREEMENT ("AGREEMENT") BEFORE RELYING ON ANY IDENTITY INFORMATION IN A ECAC ISSUED CERTIFICATE, VALIDATING A ECAC ISSUED CERTIFICATE, USING A ECAC DATABASE OF CERTIFICATE REVOCATIONS, OR RELYING ON ANY ECAC CERTIFICATE-RELATED INFORMATION (COLLECTIVELY, " ECAC INFORMATION").

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT SUBMIT A QUERY AND DO NOT DOWNLOAD, ACCESS, OR RELY ON ANY ECAC INFORMATION.

IN CONSIDERATION OF YOUR AGREEMENT TO THESE TERMS, YOU ARE ENTITLED TO USE ECAC INFORMATION AS SET FORTH HEREIN.

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 Scope

This relying party Agreement ("this Agreement") controls the use of information provided by ECAC:

- As a result of a search for a digital certificate,
- The verification of the status of digital signatures created with a private key corresponding to a public key certificate issued by ECAC ("the certificate validation"),
- Information published on ECAC website https://ecac.pki.gov.pk ("repository"),
- Any services advertised or exposed through the ECAC website https://ecac.pki.gov.pk

This Agreement becomes effective between ECAC and the Party ("the Relying Party") when the latter submits a certificate validation query or otherwise uses or relies upon any information provided by ECAC through its repository.

This Agreement does not apply to information provided in or used from demo, free, and test certificates.

5 ECAC Obligations

ECAC shall make every effort to guarantee that the information in its certificates is valid and proper for the Relying Party, acknowledging the trusted position it holds.

ECAC shall take all reasonable steps to ensure the Relying Party that information contained in its records and directories is adequate, i.e., by updating them timely.

6 Relying Party Obligations

The Relying Party acknowledges that they have adequate information to decide whether to rely upon the information provided in certificates issued by ECAC.

The Relying Party shall:

(i) Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension),
(ii) Verify the validity by ensuring that the certificate has not expired,
(iii) Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the RFC 5280,
(iv) Ensure that the certificate has not been revoked by accessing current revocation status information available at the locations specified in the certificate to be relied upon,
(v) Determine that such certificate provides adequate assurances for its intended use,

(vi) Use the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations to be performed, as a condition of relying on a Certificate in connection with each such operation.

Specifically, when relying on a timestamp token, the relying party shall:

1) Verify that the timestamp token (TST) has been correctly signed and that the private key used to sign the timestamp has not been compromised until the time of the verification (refer to ECAC-TSA Policy and practices Statement and the Timestamping CA CPS published at https://ecac.pki.gov.pk for more details)
2) Consider any limitations on the usage of the timestamp indicated by the ECAC-TSA Policy and practices Statement and the Timestamping CA CPS published at https://ecac.pki.gov.pk).
3) In case the verification takes place after expiry of the timestamp certificate, the relying party should consider the following (taken from guidance denoted in Annex D of ETSI EN 319 421):

    a. Verify that the TSU private key is not revoked, and

    b. Verify that the cryptographic hash function and the signing algorithm used in the timestamp token are still considered secure

The Relying Party is solely responsible for deciding whether to rely on the information provided by ECAC.

The Relying Party is solely responsible for all indirect damages suffered as a result of the certificate validation or the use and reliance upon information provided by ECAC through its website.

7 Disclaimer of Warranty

Within the scope of the law of the Islamic Republic of Pakistan, and except in the case of fraud, or deliberate abuse, the ECAC 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 the ECAC with the intention to be included in a certificate,
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificates or digital signatures,
- Wilful misconduct of any third-party participant breaking any applicable laws in the Islamic Republic of Pakistan, 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 ECAC services,

- Any form of misrepresentation of information by relying parties on information contained in ECAC documentation made public on ECAC repository and related to the ECAC services.

Should any of the provisions of this Agreement contradict with the provisions of ECAC CPS documentation, the CPS documentation shall prevail.

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.