Pakistan National PKI

PKI Disclosure Statement

Document Control

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

Change History

Version	Changes Description	
2.0	Final Draft version	Touir Mustapha

Document Approval

Ver. No	Approver (Name/Title)	Signatures
1	PMA	Date:

Table of Contents

1 Introduction

1.1 Overview

The Pakistan National PKI aims to provide digital certification and trust services to government and commercial sectors, enabling individuals and entities within Pakistan to conduct secure electronic transactions.

In this framework, ECAC operates as a trust service provider, delivering trust services to the government sector via a structured hierarchy of Certification Authorities (CAs). Furthermore, ECAC establishes a foundation for additional trust service providers that support both the commercial & Government sectors. This setup provides a resilient framework to support variance in requirements between government and non-government sectors regarding the offering and consumption of certification and other trust services.

The Pakistan National PKI comprises a CA hierarchy of two (2) levels:

(i) **Level 1:** The CAs at this level are positioned at the top of the hierarchy, serving as the trust anchor for Pakistan's National PKI. This level comprises five offline, self-certified CAs responsible for certifying the next layer of Certification Authorities.
Root CAs are:

a. ***Code Signing Root CA:*** Root CA to certify/sign Code Signing Subordinate CAs,
b. ***S/MIME Root CA:*** Root CA to certify email protection Subordinate CAs.
c. ***TLS Root CA:*** Root CA to certify TLS Subordinate CAs.
d. Client Auth Root CA: Root CA to certify Client Auth Subordinate CAs.
e. Timestamp Root CA: Root CA to certify TSA Subordinate CA

(ii) **Level 2:** This level includes ECAC's Subordinate CAs dedicated to serving the government sector, each certified by the corresponding Root CA at the top (Level 1) of the hierarchy as shown in the below figure:

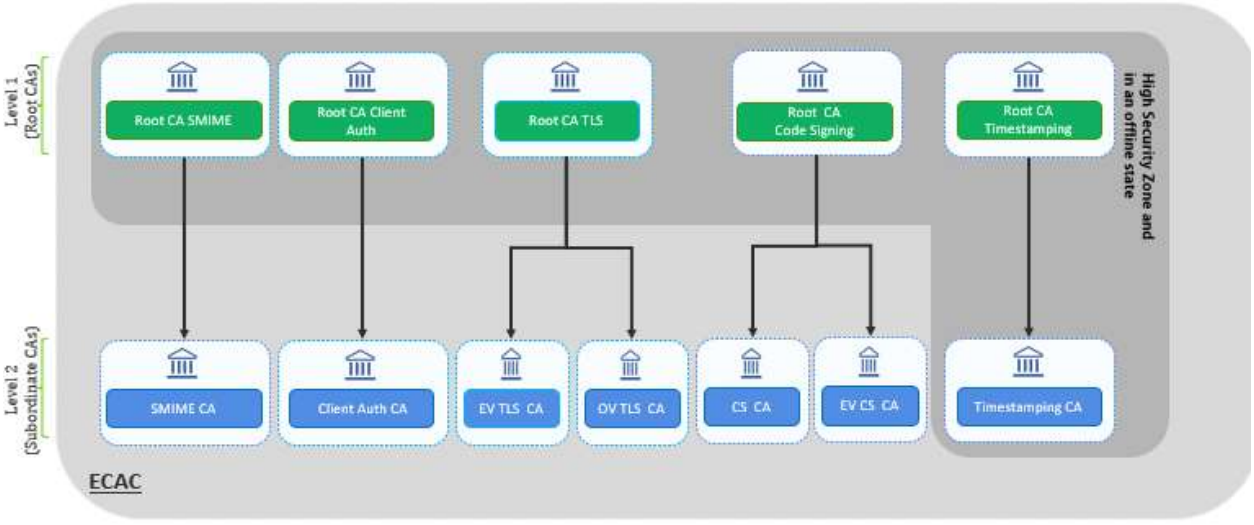

Figure 1 - Pakistan National PKI Government Domain (ECAC)

The ECAC operates as a Trust Service Provider (TSP), delivering its services through a hierarchy of Certification Authorities (CAs) established under the Root CA, as outlined below:

- **Code Signing CA:** Subordinate CA that will issue Non-EV code signing certificates to sign the libraries, exe, msi files etc.
- **EV Code Siging CA:** Subordinate CA that will issue EV code signing certificates to sign the libraries, exe, msi files etc.
- **S/MIME CA:** Subordinate CA that will issue certificates for the email signing and encryption.
- **OV TLS CA:** Subordinate CA that will issue web server TLS organization validation (OV) certificates
- **EV TLS CA:** Subordinate CA that will issue web server TLS extended validation (EV) certificates
- **Client Auth CA:** Subordinate CA that issues certificates to natural persons (government employees or contractors) for authentication and digital signing,
- **Timestamping CA:** Subordinate CA that will issue TSU certificates (i.e., TSU) involved in code signing and document 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 model with government assurance, facilitates adoption, enables interoperability, and enhances user trust.

1.2 Purpose

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

2 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 PDS only when they are addressed to the contact above.

2.1 Certificate Problem Report

ECAC 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:// ecac.pki.gov.pk/repository/Certificate_Problem_Report.html.

Subscribers, relying parties, application software suppliers, and other third parties can report suspected key compromise, certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to any certificates issued by the Subordinate CAs by sending an email to ecac.certification.problem@pki.gov.pk

The ECAC PMA will validate and investigate the request before taking an action. If ECAC deems appropriate, it may forward the revocation reports to law enforcement.

3 Certificate Type, Validation Procedures and Usage

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

The end-user certificates issued by the ECAC's Client Auth CA are:

Certificate types	Description and validation procedure	OID
Qualified signing certificates	This type of certificate is used for producing Qualified (high assurance) digital signatures on documents and electronic transactions. It is issued to individuals acting with professional capacity, who undergo identity verification through in-person meetings with the relevant registration authority or equivalent methods that provide an equivalent level of assurance as physical presence. The individual private keys associated with these certificates are used for local signing purposes.	(local) 1.3.6.1.4.1.59337.3.1.2
Advanced signing certificates	Used to produce Advanced (moderate assurance) digital signatures on documents and e-transactions. Issued to individuals acting with professional capacity and whose identity has been verified with reasonable confidence in the user's identity and does not require the highest level of assurance. The individual private keys associated with these certificates are used for local signing purposes.	(local) 1.3.6.1.4.1.59337.3.1.1

Authentication certificates	Used for authentication of end-users to e-services. These certificates are issued to individuals acting with professional capacity.	1.3.6.1.4.1.59337.3.1.4
eSeal certificates	This certificate is issued to legal person to add an eSeal on a document issued/attested by this legal person. Before issuing this type of certificate, ECAC verifies the legal existence of the applicant (i.e., government entity) using an authoritative data source that provides information on the formation of the organization including its legal name. ECAC also performs a site visit to the applicant's address to validate the applicant's physical address and place of business. The applicant's vetting process also encompasses verification of the applicant's authorized representative based on the organization's record at the authoritative source or a formal communication between the ECAC and the applicant (i.e., legal person).	1.3.6.1.4.1.59337.3.2.1
Signature verification service certificate	Certificate used for signing the signature verification responses returned from the ECAC operated signature verification service. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the ECAC PMA	1.3.6.1.4.1.59337.3.3.2
OCSP certificate	Used by the ECAC Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the ECAC PMA.	N/A

The end-user certificates issued by the ECAC OV TLS CA are:

Certificate types	Description and validation procedure	OID
Organization validated (OV) SSL	Certificate issued for website authentication. Before issuing this type of certificate, ECAC verifies the legal existence of the applicant (i.e., government entity) using an authoritative data source that provides information on the formation of organization including its legal name. ECAC also performs a site visit to the applicant's address to validate the applicant's physical address and place of business. The applicant's vetting process also encompasses verification of the applicant's authorized representative based on the organization's record at the authoritative source or a formal communication between the ECAC and the applicant (i.e., legal person).	1.3.6.1.4.1.59337.3.3.1
OCSP certificate	Used by the ECAC Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the ECAC PMA.	N/A

The end-user certificates issued by the ECAC EV TLS CA are:

Certificate types	Description and validation procedure	OID
Extended validation (EV) SSL	Certificate issued for website authentication. This type of certificate is issued to the applicant who has undergone the most extensive level of vetting and identity background checks to verify that the website, the owner and the business it represents is legitimate and authentic. ECAC applies verifications related to legal, physical, and operational existence according to section 3.2.2 of the CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates.	1.3.6.1.4.1.59337.3.3.5
OCSP certificate	Used by the ECAC Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the ECAC PMA.	N/A

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

Certificate types	Description and validation procedure	OID
Non-EV Code Signing	Used to sign source code/software developed by a legal person (i.e., a government entity). Before issuing this type of certificate, ECAC verifies the legal existence of the applicant (i.e., Legal person) using an authoritative data source that provides information on the formation of organization including its legal name. ECAC also performs a site visit to the applicant's address to validate the applicant's physical address and place of business. The applicant's vetting process also encompasses verification of the applicant's authorized representative based on the organization record at the authoritative source or a formal communication between the ECAC and the applicant (i.e., legal person).	1.3.6.1.4.1.59337.3.2.2
OCSP certificate	Used by the ECAC Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the ECAC PMA	N/A

The end-user certificates issued by the ECAC EV Code Signing CA are:

Certificate types	Description and validation procedure	OID
Non-EV Code Signing	Used to sign source code/software developed by a legal person (i.e., a government entity). This type of certificate is issued to the applicant who has undergone the most extensive level of vetting and identity background checks to verify that the website, the owner and the business it represents is legitimate and authentic. ECAC applies verifications related to legal, physical, and operational existence according to section 3.2.2.2 of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates	1.3.6.1.4.1.59337.3.2.3
OCSP certificate	Used by the ECAC Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the ECAC PMA	N/A

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

Certificate types	Description and validation procedure	OID
S/MIME Sponsor-Validated	Used to digitally sign and encrypt the email communications. This type of certificate is issued only to the natural persons representing a legal person that are identity-vetted through in-person meetings with the relevant registration authority or equivalent methods that provide an equivalent level of assurance as physical presence. ECAC verifies the applicant's control of Mailbox Addresses to be included in the issued certificates.	1.3.6.1.4.1.59337.3.1.3
OCSP certificate	Used by the ECAC Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the ECAC PMA	N/A

The end-user certificates issued by ECAC Timestamping CA are:

Certificate types	Description and validation procedure	OID
DS Timestamp Certificate	Used for signing the timestamps issued by the ECAC-TSA service for the document signatures. The Timestamping CA does not issue certificates to any legal person other than ECAC itself. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the ECAC PMA.	1.3.6.1.4.1.59337.3.3.4
CS Timestamp Certificate	Compliant to CS BR requirements, used for signing the timestamps issued by the ECAC-TSA service for code signing. The Timestamping CA does not issue certificates to any legal person other than ECAC itself. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the ECAC PMA.	1.3.6.1.4.1.59337.3.3.3
OCSP certificate	Used by the ECAC Online Certificate Status Protocol (OCSP) responder to sign the OCSP responses for the certificates issued by this Subordinate CA. This certificate is issued as part of an authorized internal operational ceremony under the supervision of the ECAC PMA.	N/A

4 Reliance Limits

ECAC cannot be held liable for any use of the certificate that does not comply with its Subordinate CAs CPSs available at https://ecac.pki.gov.pk

5 Subscriber's Obligations

It is the responsibility of Subscribers to:

- only use the Key Pairs for the purposes and in the ways allowed by the relevant CPS.
- submit accurate and complete information to the CA during Subject registration at the time of certificate request.
- Exercise reasonable care to avoid unauthorized use of the Subject's Private Key.

- Notify the CA, without any unreasonable delay, if any of the following occurs up to the end of the validity period indicated in the Certificate:
    - the Subject's Private Key has been potentially or proven lost, stolen or compromised.
    - control over the Subject's Private Key has been lost due to potential or actual compromise of activation data (e.g., PIN code) or other reasons.
    - inaccuracy or changes to the Certificate content, as notified to the Subscriber.
- Ensure that if the Subscriber or Subject generates the Subject's Key Pair, only the Subject holds the Private Key
- Ensure that Private Keys are generated within the signature cryptographic device approved by ECAC.

For further information, please refer to the ECAC CPS available at https://ecac.pki.gov.pk

6 Certificate Status checking obligations of the Relying Parties

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

7 Limited Warranty and disclaimer / Limitation of Liability

The liability taken by the ECAC is limited to the correct application of procedures as declared in its CPS; these procedures relate to the issue and management of digital Certificates. Therefore, ECAC is not in any event liable for any loss of profits, indirect and consequential damages, or loss of data, to the extent permitted by applicable law.
ECAC is not liable for any damages resulting from infringements by the Subscriber or the Relying Party on the applicable terms and conditions.
ECAC is not in any event liable for the damages that result from force major events as detailed in the relevant CPS.
ECAC takes commercially reasonable measures to mitigate the effects of force major in due time. Any damage resulting of any delay caused by force major will not be covered by the ECAC.
On the other hand, in cases where ECAC has not issued or managed the EV certificates in compliance with the CA/Browser Forum EV Guidelines, Baseline requirements and the relevant CPS, ECAC's liability to the Subscriber for legally recognized and provable claims for

losses or damages suffered because of the use or reliance on such an EV Certificate shall not exceed $2,000. Likewise, liability to Relying Parties or any other third parties for legally recognized and provable claims for losses or damages suffered because of the use or reliance on such EV Certificate shall not exceed $2,000.

8 Applicable Agreement and CPSs

ECAC agreements and CPSs are available at https://ecac.pki.gov.pk

9 Privacy Policy

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 subscribed 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 ensure 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.

10 Refund Policy

No refund is applicable for any fees charged by ECAC.

11 Applicable Laws, complaints, and dispute resolution

The provision of the ECAC PKI services is compliant to the relevant and applicable laws of the Islamic Republic of Pakistan.
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.

12 TSP and repository licenses, trust marks, and audit

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