Pakistan National PKI

ECAC Certification Authorities CP/CPS

Version control

Version	Date	Description / Status	Responsible
V1.0	08/12/2022	Initial version for review & approval	ECAC
V1.1	22/12/2022	Reviewed and updated the Email Addresses, URLs and Object IDs	ECAC
V1.2	28/12/2022	Reviewed and updated the CA Common Name, Subject Name in section 7	ECAC
V1.3	22/02/2023	Updated based on feedback from design authority and WebTrust auditor	ECAC
V1.4	06/07/2023	Corrected certificate and CRL addresses in sections 7. Addressed the findings in point-in-time audit	ECAC

Document Signoff

Version	Date	Responsible	Validated By	Reviewed and Approved By
V1.4	/ /2023	ECAC	ECAC (PMA)	ECAC (PMA)

Table of Contents

1 Introduction

The present Certificate Policy and Certification Practice Statement (hereinafter, CP/CPS) of The Electronic Certification Accreditation Council (ECAC) that applies to:

- Root signing services of the Pakistani National Root Certification Authority (hereinafter, NR-CA),
- CA signing services of the CAs that intermediate Root CAs for the two PKI domains supported under the Pakistani national PKI: (1) Government PKI, (2) Commercial PKI. These CAs are going to be collectively referenced in this document as the NR-CA's intermediate CAs.

This CP/CPS addresses the technical, procedural, and organizational policies and practices of the NR-CA and its intermediate CAs with regard to all services available and during the complete lifetime of certificates issued by these CAs, including the certificates issued by the NR-CA to itself under the form of self-signed certificates.

The provisions of the present CP/CPS regarding practices, level of services, responsibilities and liability bind all parties involved including the NR-CA, its intermediate CAs, subscribers and relying parties.

This CP/CPS complies with the formal requirements of the Internet Engineering Task Force (IETF) RFC 3647 with regards to format and content. While certain section titles are included according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of the PKI services of the NR-CA and its intermediate CAs. Such sections are denoted as "Not applicable".

The CP/CPS complies with the Electronic Transaction Ordinance 2002 (ETO 2002) of Pakistan for Digital Signature and Electronic Certification and ECAC Regulations formulated under ETO 2002.

This CP/CPS complies with the below requirements published at https://www.cpacanada.ca:

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security
- WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities - Code Signing Baseline Requirements

The ECAC's Policy Management Authority (PMA) is committed to maintain this CP/CPS in conformance with the current versions of the below requirements published at http://www.cabforum.org:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Guidelines For The Issuance And Management Of Extended Validation Certificates ("EV Guidelines")

- CA/Browser Forum Baseline Requirements for Code Signing ("Baseline Requirements for Code Signing")

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

Further information with regard to this CP/CPS, the NR-CA and its intermediate CAs can be obtained from the ECAC PMA, using contact information provided in clause 1.5.

1.1 Overview

The Pakistan National PKI comprises two separate PKI hierarchies for each of the Government and Commercial domains, both hierarchies are established under the Pakistan National Root CA (hereinafter, NR-CA). 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 offers certification services to support the following use cases:

- Server Authentication (TLS): certificates used to authenticate the identity of a web server,
- Client Authentication (for both Individuals and Devices): certificates used to authenticate clients during an SSL handshake or sign a random challenge generated by an authentication server,
- Code Signing: certificates used to digitally sign applications, drivers, executables, and software programs,
- Timestamping: certificates used to sign timestamp tokens,
- Document Signing: certificates used to digitally sign documents,
- Email protection: certificates used to digitally sign and encrypt emails.

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.

The Pakistan National PKI comprises a CA hierarchy of three (3) levels:

1. **Level 0:** The NR-CA (offline) is at the top-level of the hierarchy, which sets it as the trust anchor for the Pakistan National PKI. The Root CA certifies a layer of CAs that intermediate Root CA to the two underlying PKI domains: Government PKI and Commercial PKI.
2. **Level 1 (hereinafter, NR-CA's intermediate CAs):**
    - Government Intermediate CAs (offline): multiple intermediate CAs, established separately to provide segregation of the different certificate use cases (e.g., Server Authentication (TLS), Code Signing, Timestamping etc.). The Government Intermediate CAs will be certifying government TSPs according to the Pakistan national PKI accreditation framework.
    - Commercial Intermediate CAs (offline): multiple intermediate CAs, established separately to provide segregation of the different certificate

use cases (e.g., Server Authentication (TLS), Code Signing, Timestamping etc.). The Commercial Intermediate CAs will be certifying Commercial TSPs according to the Pakistan national PKI accreditation framework.

3. **Level 2:** Government and Commercial TSP CAs that are TSP Issuing CAs signed by the corresponding Intermediate CA at level 1 of this PKI hierarchy.

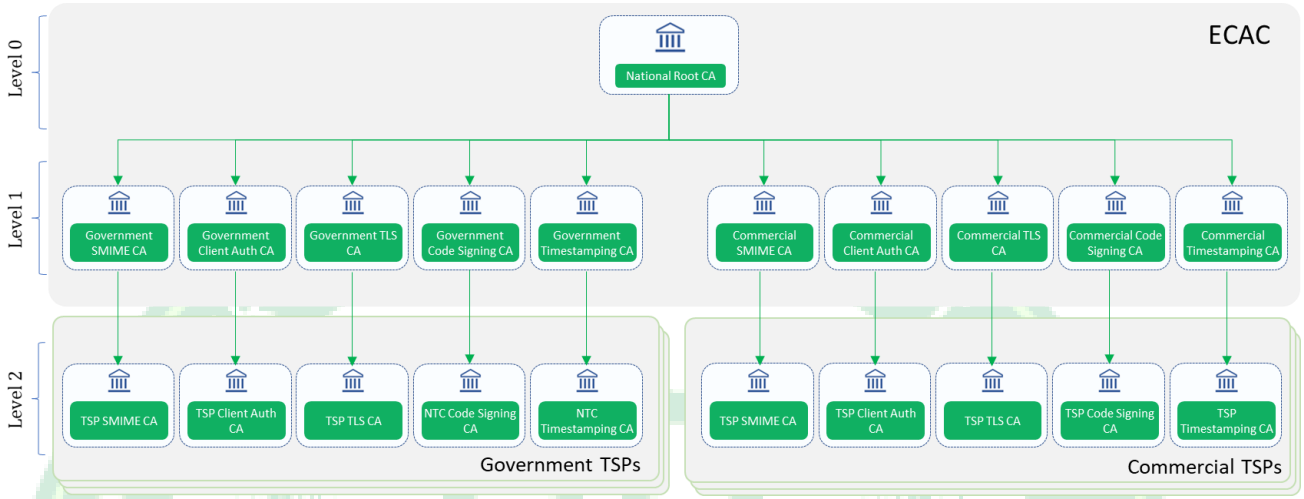

Figure 1 - Pakistan national PKI hierarchy

1.1.1 Overview of ECAC Policy Management Authority (PMA)

The ECAC PMA is the highest-level management body with final authority and responsibility for of the Pakistan national PKI. The ECAC PMA directly supervises the operations of the NR-CA and its intermediate CAs, and overseeing the TSPs in Pakistan through the national TSP accreditation framework.

The ECAC PMA is composed of appointed representatives of the ECAC's senior management, PKI operations management as well as subject matter experts in PKI, compliance, legal and security.

The roles and responsibilities of the ECAC PMA are summarized below:

- **Supervises the operations of the NR-CA and its intermediate CAs:** The ECAC runs the Registration Authority (RA) function as well as the technical operations of the NR-CA and its intermediate CAs under a direct supervision from the ECAC PMA. A coherent reporting structure and communication is defined as part of ECAC's PKI governance and operating model to support and reinforce the ECAC PMA authority towards the PKI operational functions.
- **Develop and Maintain the National PKI Framework**: The ECAC PMA, through its policy function, develops and maintain the National PKI framework including:
  - The PKI governance framework (Superior CAs CP, CPS in addition to other national PKI policies and procedures)
  - TSP accreditation framework: licensing model, supervision processes, accreditation scheme, etc.
- **Managing International Recognition:** Pursuant to the broad and public purpose of digital certificates, the ECAC PMA's seeks global recognition of the Pakistan national PKI based on the well-know WebTrust accreditation. With this

accreditation, the Pakistan national PKI (NR-CA) would be eligible for enrollment into the "commercial" root programs (e.g., browsers and operating systems).

- **Driving PKI Promotion in Pakistan:** The ECAC PMA contributes to awareness programs, collaboration working groups, and supporting taskforces.
- **Contributing to PKI Laws and Decrees:** The ECAC PMA contributes to improving the local laws and decrees in relation to PKI and Trust Services leveraging its practical experience with TSPs as well as its exposure to international regularity authorities, service providers and "commercial" root-signing programs.
- **Oversees the TSPs in Pakistan:** The ECAC PMA manages the licensing of Commercial and Government TSPs under the national TSP accreditation framework. It accordingly approves, maintain, and publishes the list of approved TSPs/TS under the national TSP accreditation framework. The ECAC PMA will also look for establishing mutual recognition with other jurisdictions (e.g., EU) for the TSPs and the services listed in the National Trust List.

1.2 Document Name and Identification

This document is the "ECAC Certification Authorities CP/CPS" by the ECAC Pakistan, and it was approved by the ECAC Policy Management Authority (PMA) for the publication. This CP/CPS document is published at https://ecac.pki.gov.pk

The ECAC CAs will use the OID **1.3.6.1.4.1.59337.1.1** to identify this document.

1.3 PKI Participants

Several parties make up the participants of the NR-CA and its intermediate CAs. The parties mentioned hereunder including the NR-CA, the NR-CA's intermediate CAs, subscribers and relying parties are collectively called PKI participants.

1.3.1 Certification Authorities

The ECAC's PKI comprises the Pakistani NR-CA, as well as the following intermediate CAs that issue Certificates in accordance with this CP/CPS:

- Government SMIME CA
- Government Client Auth CA
- Government TLS CA
- Government Code Signing CA
- Government Timestamping CA
- Commercial SMIME CA
- Commercial Client Auth CA
- Commercial TLS CA
- Commercial Code Signing CA
- Commercial Timestamping CA

The ECAC's CAs offers the supports the below PKI services:

1. Certificate lifecycle management
   1.1. Subscriber registration
   1.2. Certificate issuance
   1.3. Certificate rekeying

1.4. Certificate distribution (where applicable)
1.5. Certificate revocation

2. Publishes certificate revocation information in the form of a Certificate Revocation List (CRL) distribution point and Online Certificate Status Protocol (OCSP) responder.

The ECAC operates a secure facility to deliver the above services by itself. The ECAC has the business ownership and final responsibility in providing the certification services of the above mentioned CAs.
According to its ultimate purpose, The ECAC's PKI issues CA certificates to the Government and Commercial TSPs operating in Pakistan under the national TSP accreditation framework. The TSPs are expected to operate their own CAs in accordance with their respective CA Agreements with the ECAC and to be bound by the terms of this CP/CPS. The TSPs CAs will also have their own CP/CPS documents that are developed by the TSPs and approved by the ECAC PMA.
The ECAC has the business ownership and final responsibility of overseeing the TSPs according to the national TSP accreditation framework.

1.3.2 Registration Authorities

The ECAC PMA bears the responsibility of operating an RA function for the NR-CA as well as its intermediate CAs. This RA is tasked to request the issuance and the revocation of CA certificates under this CP/CPS from the CAs operating under this CP/CPS.

When a subscriber requests for the creation of a Subordinate CAs and Issuing CA certificate under the NR-CA or any of its intermediate CAs, it is the RA function that validates the request and decide whether or not to request the creation of the CA certificate. The ECAC does not delegate the execution of Section 3.2 requirements to any third party. All registration procedures are directly executed by the RA personnel that are appointed and directly supervised by the ECAC PMA.

ECAC's personnel involved in the issuance of the Subordinate CAs and Issuing CAs must meet and follow the requirements set forth in Sections 4.2 and 5.3.

1.3.3 Subscribers

For NR-CA: Subscribers are:

- Government SMIME CA
- Government Client Auth CA
- Government TLS CA
- Government Code Signing CA
- Government Timestamping CA
- Commercial SMIME CA
- Commercial Client Auth CA
- Commercial TLS CA
- Commercial Code Signing CA
- Commercial Timestamping CA

For the NR-CA's intermediate CAs: Subscribers are the TSPs' CAs (Subordinate CAs and Issuing CAs) certified by the intermediate CAs, that are issuing certificates to a subsidiary subordinate CAs issuing certificates or to end-entities.

All the above subscribers are:

• Identified in the Subject field of their certificate, issued by the ECAC's PKI;

• controlling the private key corresponding to the public key that is listed in their certificate.

1.3.4 Relying Parties

Relying parties are entities, including natural or legal persons that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a subscriber's certificate.

To verify the validity of a digital certificate issued by the ECAC's PKI they receive, relying parties must always verify such a certificate against the ECAC Certificate Validation Service(e.g. OCSP or CRL) prior to relying on information featured in such a received certificate.

1.3.5 Other Participants

None.

1.4 Certificate Usage

Certain limitations apply to the usage of certificates issued by the ECAC CAs that includes those stated in the below subsections.

1.4.1 Appropriate Certificate Uses

For certificate issued to the NR-CA itself: it is a special class of self-signed certificate that being the trust anchor of the Pakistan PKI. The NR-CA certificate can be used for:

- Sign certificates for the Government and Commercial Intermediate CAs,
- Sign CRLs containing the list of subscribers' revoked certificates and of NR-CA revoked self-signed certificates,
- Sign OCSP certificates for the NR-CA OCSP service

For certificate issued to the Government and Commercial Intermediate CAs: those are used for:

- Sign Subordinate CAs and Issuing CAs Certificates for Government and Commercial TSPs
- Sign CRLs containing the list of revoked Subordinate CAs and Issuing CAs Certificates
- Sign OCSP Certificate for the their own OCSP responders

1.4.2 Prohibited Certificate Uses

CA certificates issued under this CP/CPS cannot be used to sign end-entity certificates (other than the certificate of its OCSP responder).

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP/CPS document is administered by the ECAC PMA.

1.5.2 Contact Person

Requests for information on the compliance of the TSPs' CAs with the national TSP accreditation framework as well as any other inquiry associated with this CP/CPS should be addressed to:

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 ECAC PMA accepts comments regarding the present CP/CPS only when they are addressed to the contact above.

Certificate Problem Report

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 Root CA or 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 in accordance with section 4.9.

1.5.3 Person Determining CPS Suitability for the Policy

The ECAC PMA is responsible for determining the suitability and applicability of this CP/CPS based on the results and recommendations received from a Qualified Auditor as specified in Section 8.

1.5.4 CPS Approval Procedures

Dedicated personnel from the ECAC PMA reviews the CP/CPS for the initial draft and subsequent changes to determine the consistency with the best practices implemented prior to the approval.

Amendments shall either be in the form of a document containing an amended form of the CP/CPS or an update notice.

Changes made into this CP/CPS will be tracked in the revision table.

1.6 Definitions and Acronyms

1.6.1 Definitions

The following is a list of the definitions of terms and acronyms used. The source is cited where relevant.

Applicant – The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber.

Applicant Representative – A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent 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, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA. In the context of this CP/CPS, the applicant representative is in charge of submitting certificate requests and certificate revocation requests on behalf of the applicant.

Activation data – Secret information, other than cryptographic keys, that are required to operate cryptographic modules that need to be protected, e.g. a PIN, a password or passphrase, or a manually held key share.

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 CP/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)

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 Policy (CP) – 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 time-stamped 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., a Section in a CA's CPS or a certificate template file used by CA software.

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.

CSPRNG – A random number generator intended for use in cryptographic system.

Expiry Date – The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

HSM – Hardware Security Module – a device designed to provide cryptographic functions specific to the safekeeping of private keys

IP Address – A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.

Issuing CA – Issuing CAs are used to provide certificates to users, computers, and other services. In this CP/CPS, Issuing CA is issued by a Subordinate CA, and it issues certificates to the end entities only.

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.

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.

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.

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.

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.

Subject – The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device 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. In the context of this CP/CPS, Subordinate CAs are ECAC

Government CAs and Commercial CAs whose certificates are signed by the Pakistan National Root CA

Subscriber – A natural person or Legal Entity 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.

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.

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
DN	Distinguished Name
ECAC	Electronic Certification Accreditation Council
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
ISO	International Standards Organization
NTC	National Telecom Corporation
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Information Number

PKCS#10	Certification Request Syntax Specification
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RSA	Rivest-Shamir-Adelman (The names of the inventors of the RSA algorithm)
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SSL	Secure Sockets Layer
TSA	Timestamping Authority
TLS	Transport Layer Security
TSP	Trust Service Provider (collective term for TCs and PSCEs)
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier, a URL, FTP address, email address, etc.
URL	Universal Resource Locator
VPN	Virtual Private Network

1.6.3 References

This document refers to the following:

- 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 for Certification Authorities Principles and Criteria
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- Electronic Transaction Ordinance 2002 of Pakistan for Digital Signature and Electronic Certification

2 Publication and Repository Responsibilities

2.1 Repositories

The ECAC publishes the information about Certificates, CRLs and CP/CPS documents of the NR-CA and its intermediate CAs on a repository that is publicly accessible at https://ecac.pki.gov.pk.

2.2 Publication of Certification Information

The ECAC publishes a copy of the NR-CA certificate, the NR-CA intermediate CAs' certificates, the OCSP certificate of each of these CA, as well as this CP/CPS on the public repository.

The ECAC also retains other documents that make certain disclosures about its PKI's policies, practices, and procedures as part of the public repository. The ECAC reserves its right to make available and publish information on its policies by any means it sees fit.

The ECAC publishes digital certificate status information in frequent intervals as indicated in this CP/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. The NR-CA CA and its intermediate CAs 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 the NR-CA CA and its intermediate CAs.

2.3 Time or Frequency of Publication

The ECAC PMA reviews this CP/CPS at least once annually and makes appropriate changes so that the NR-CA and its intermediate CAs operations remain fully aligned to the CA/B forum Baseline Requirements and other requirements as listed in section 1 of this CPS.

Modified versions of the CP/CPS are published within five working days after the ECAC PMA approval.

2.3.1 Certificates

The CAs' and OCSP certificates are published to the public repository once they are issued.

2.3.2 CRLs

The ECAC maintains the CRL distribution point and the information on this URL until minimum 7 years after the expiration date of all certificates, containing the CRL distribution point.

The ECAC publishes CRLs at regular intervals according to the following rules:

- At minimum, once every six months, at an agreed time. In addition, a new CRL will be generated and published following the revocation of any certificate,
- CRLs lifetime shall be set to 184 days..

2.4 Access Controls on Repositories

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

The ECAC implemented 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 Types of Names

The ECAC CAs follow the standard X500 distinguished names in English. The names must be unique and meaningful.

The tables below specify the DNs used for the NR-CA and its intermediate CAs.

3.1.1.1 The NR-CA

The NR-CA is a self-signed Certificate carries the following DN:

Attribute	Value
Common Name – "CN"	ECAC Root CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK

Table 1 - National Root CA Distinguished Name

The National Root CA OCSP Certificate carries the following DN:

Attribute	Value
Common Name – "CN"	ECAC Root CA OCSP - 2023
Organization Name – "O"	Electronic Certification Accreditation Council
State Or Province – "S"	Pakistan
Country – "C"	PK

Table 2 - National Root CA OCSP Distinguished Name

3.1.1.2 Government Intermediate CAs

3.1.1.2.1 DNs used for CAs and OCSP responders

The Government intermediate CAs use the following DNs:

Attribute	Value
Government SMIME CA	
Common Name – "CN"	ECAC Government SMIME CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Government Client Authentication	
Common Name – "CN"	ECAC Government Client Authentication CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Government TLS CA	
Common Name – "CN"	ECAC Government TLS CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Government Code Signing CA	
Common Name – "CN"	ECAC Government Code Signing CA G1
Organization Name – "O"	Electronic Certification Accreditation Council

Country – "C"	PK
Government Timestamping CA	
Common Name – "CN"	ECAC Government Timestamping CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK

Table 3 - Government Intermediate CAs Distinguished Names

The Government Intermediate CAs' OCSP Certificates use the following DNs:

Attribute	Value
Government SMIME CA	
Common Name – "CN"	ECAC Government SMIME CA OCSP - 2023
Organization Name – "O"	Electronic Certification Accreditation Council
State Or Province – "S"	Pakistan
Country – "C"	PK
Government Client Authentication CA	
Common Name – "CN"	ECAC Government Client Authentication CA OCSP - 2023
Organization Name – "O"	Electronic Certification Accreditation Council
State Or Province – "S"	Pakistan
Country – "C"	PK
Government TLS CA	
Common Name – "CN"	ECAC Government TLS CA OCSP - 2023
Organization Name – "O"	Electronic Certification Accreditation Council
State Or Province – "S"	Pakistan
Country – "C"	PK
Government Code Signing CA	
Common Name – "CN"	ECAC Government Code Signing CA OCSP - 2023
Organization Name – "O"	Electronic Certification Accreditation Council
State Or Province – "S"	Pakistan
Country – "C"	PK
Government Timestamping CA	
Common Name – "CN"	ECAC Government Timestamping CA OCSP - 2023
Organization Name – "O"	Electronic Certification Accreditation Council
State Or Province – "S"	Pakistan
Country – "C"	PK

Table 4 - Government Intermediate CAs OCSP Distinguished Names

3.1.1.2.2 Government TSPs

The Government TSP CAs use the following DN scheme:

Attribute	Value
Common Name – "CN"	Meaningful name of the TSP organization
Organization Name – "O"	Name of the TSP organization
Country – "C"	PK
SerialNumber (For EV CAs only)	The organization's registration number that is verified according to the EV guidelines. For Government Entities that do not have a

	Registration Number or readily verifiable date of creation, CA SHALL enter appropriate language to indicate that the Subject is a Government Entity
BusinessCategory (For EV CAs only)	The organization's business category that is verified as per the EV guidelines
JurisdictionCountryName (For EV CAs only)	PK

Table 5 Government TSPs Distinguished Name

3.1.1.3 Commercial Intermediate CAs

3.1.1.3.1 DNs used for CAs and OCSP responders

The Commercial intermediate CAs use the following DNs:

Attribute	Value
Commercial SMIME CA	
Common Name – "CN"	ECAC Commercial SMIME CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Commercial Client Auth	
Common Name – "CN"	ECAC Commercial Client Authentication CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Commercial TLS CA	
Common Name – "CN"	ECAC Commercial TLS CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Commercial Code Signing CA	
Common Name – "CN"	ECAC Commercial Code Signing CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Commercial Timestamping CA	
Common Name – "CN"	ECAC Commercial Timestamping CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK

Table 6 - Commercial CAs Distinguished Names

The Commercial Intermediate CAs' OCSP Certificates use the following DNs:

Attribute	Value
Commercial SMIME CA	
Common Name – "CN"	ECAC Commercial SMIME CA OCSP - 2023
Organization Name – "O"	Electronic Certification Accreditation Council
State Or Province – "S"	Pakistan
Country – "C"	PK
Commercial Client Authentication CA	
Common Name – "CN"	ECAC Commercial Client Authentication CA OCSP - 2023
Organization Name – "O"	Electronic Certification Accreditation Council

State Or Province – "S"	Pakistan
Country – "C"	PK
Commercial TLS CA	
Common Name – "CN"	ECAC Commercial TLS CA OCSP - 2023
Organization Name – "O"	Electronic Certification Accreditation Council
State Or Province – "S"	Pakistan
Country – "C"	PK
Commercial Code Signing CA	
Common Name – "CN"	ECAC Commercial Code Signing CA OCSP - 2023
Organization Name – "O"	Electronic Certification Accreditation Council
State Or Province – "S"	Pakistan
Country – "C"	PK
Commercial Timestamping CA	
Common Name – "CN"	ECAC Commercial Timestamping CA OCSP - 2023
Organization Name – "O"	Electronic Certification Accreditation Council
State Or Province – "S"	Pakistan
Country – "C"	PK

Table 7 - Commercial CAs OCSP Distinguished Names

3.1.1.3.2 Commercial TSPs

The Commercial TSP CAs use the following DN scheme:

Attribute	Value
Common Name – "CN"	Meaningful name of the TSP organization
Organization Name – "O"	Name of the TSP organization
Country – "C"	PK
SerialNumber (For EV CAs only)	The organization's registration number that is verified according to the EV guidelines. For Government Entities that do not have a Registration Number or readily verifiable date of creation, CA SHALL enter appropriate language to indicate that the Subject is a Government Entity
BusinessCategory (For EV CAs only)	The organization's business category that is verified as per the EV guidelines
JurisdictionCountryName (For EV CAs only)	PK

Table 8 Commercial TSPs Distinguished Names

3.1.2 Need for Names to be Meaningful

Names are meaningful since the CN (Common Name) contains the name of the subscriber and the name O(Organization) is the name of the organization subscriber's.

3.1.3 Anonymity or Pseudonymity of Subscribers

This CP/CPS does not permit the anonymous or pseudonymous subscribers.

3.1.4 Rules for Interpreting Various Name Forms

The naming convention used by ECAC PKI is based on ISO/IEC 9595 (X.500)Distinguished Name (DN).

3.1.5 Uniqueness of Names

All the DNs used within the ECAC PKI are specified in section 3.1.1, that are all unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

Certificate Applicants SHALL NOT use names in their Certificate Application or Certificate Request that infringes upon the intellectual property rights of organizations outside of their authority.

Names can only contain trademarks in case the subscriber has the legal right to use the trademark in question. Where applicable, the ECAC PMA enforces this verification as part of the certificate enrolment process.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The ECAC demands to validate the proof of possession of private key by TSPs. The proof of possession is submitted in the form of PKCS#10 format. The PKCS#10 digital signature is validated by the corresponding intermediate CA at the time of Certificate issuance against the subject private key.

3.2.2 Authentication of Organization Identity

3.2.2.1 NR-CA and its intermediate CAs:

The NR-CA and its intermediate CAs constitutes the ECAC's PKI that is owned and operated by the ECAC under a direct control and supervision of the ECAC PMA. Therefore, the approval of the corresponding certification requests is handled internally by the ECAC PMA as part of approving the establishment of these CAs. That is further verified as part of the approval and organization of the key generation ceremonies by the ECAC PMA.

3.2.2.2 Government TSPs

The ECAC PMA authenticates the identity of a government TSP organization as follows:

1. Verification of presence and legal standing:
   1.1. Verify the existence of the Organization using an authoritative source (such as *the Official Government Gateway*) that provides information on the formation of organization including its legal name, address and a reference of the decree or law issued to establish the organization under its designated name. The ECAC PMA also conducts a site visit to the organization's site to validate the address.
   1.2. Verify the organization's authorized representative approving the certification request. This can be established either based on the organization's record at the authoritative source or based on a formal communication between the ECAC and the Government Entity's HR.
2. Verification of association with the certificate subject: The ECAC PMA verifies that the organization name to be inserted in the certificate matches the legal name of the

organization requesting the certificate. The full organization's name of an abbreviated version can be included in the certificate

3. Processing of any additional paperwork required by the ECAC PMA as part of the verification process that is required to conclude the review and validation of the TSP request by the ECAC PMA.

3.2.2.3 Commercial TSPs

The ECAC PMA authenticates the identity of a commercial TSP organization as follows:

1. Verification of presence and legal standing:
   1.1. Verify the existence of the Organization using an authoritative source (such as *"Securities and Exchange Commission of Pakistan" or "Federation of Pakistan Chambers of Commerce & Industry"*) that provides information on the formation of organization including its legal name. The ECAC PMA also conducts a site visit to the organization's site to validate the address.
   1.2. Verify the organization's authorized representative approving the certification request. This shall be established either based on the organization's record at the authoritative source.
2. Verification of association with the certificate subject: The ECAC PMA verifies that the organization name to be inserted in the certificate matches the legal name of the organization requesting the certificate. The full organization's name of an abbreviated version can be included in the certificate.
3. Processing of any additional paperwork required by the ECAC PMA as part of the verification process that is required to conclude the review and validation of the TSP request by the ECAC PMA.

3.2.3 Authentication of Individual Identity

The ECAC CAs do not issue certificates to individuals.

3.2.4 Non-verified Subscriber Information

All information included in the DN is checked and authenticated by the ECAC PMA.

3.2.5 Validation of Authority

The organization's authorized representative shall nominate a certificate requester from the organization who undergoes the certificate request process with the ECAC PMA. The Authorization of certificate requester is performed as follows with:

1. The ECAC PMA receives a legible copy of a valid government-issued photo ID for the certificate requester. The ID copy shall be inspected for indication of alteration or falsification,
2. The ECAC PMA receives a completed and signed certificate request form from the requestor. The form is signed by the authorized representative, that attests the authority of the requestor,
3. The ECAC PMA verifies the authority of the authorized representative through an authoritative source. In case of government TSPs, the authority of authorized representative can be established based on a formal communication with the government entity,

4. An in-person verification is finally conducted with the requester to conclude the validation process.

3.2.6 Criteria for Interoperation

The ECAC's PKI conforms with the following standards to facilitate interoperation:

- X.509 certificates and CRLs in accordance with the profiles listed in this CP/CPS,
- Offers certificate revocation information through X.509 CRLs, in addition to an OCSP responder that complies with RFC 6960.

Any CA wishing to interoperate, join or cross certify with the NR-CA shall adhere to the requirements specified above.

3.3 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 in initial registration.

3.3.2 Identification and Authentication for Re-key after Revocation

Identification and authentication procedures for re-key after revocation is same as during initial certification. This follows the conclusion of relevant analysis and investigations by the ECAC PMA.

3.4 Identification and Authentication for Revocation Request

For the NR-CA's intermediate CAs: In the event of a revocation due to a key compromise, internal procedures will be executed as per ECAC Disaster Recovery and Business Continuity Plan.

For the TSP CAs:

The following revocation procedure is enforced by the ECAC PMA:

- Signed revocation request from an authorized representative or a formal delegate by an authorized representative,
- Verification of the identity of the form signatory based on the information collected during the registration. If the signatory was not involved during the registration, the process defined in section 3.2.5 is followed to authorize the request.
- Communication with the TSP to provide reasonable assurances on confirming the revocation. Such communication, depending on the circumstances, may include one or more of the following: telephone, e-mail, or courier service.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 The NR-CA's intermediate CAs:

Certificate applications to the NR-CA are limited to the Government and Commercial Intermediate CAs that are owned and operated by ECAC. Therefore, the processing of

those applications involves authorized representative(s) from RA function within operated by the ECAC PMA itself.

4.1.1.2 Government TSPs:

The TSP authorized representative submits the certificate application as part of the overall process through which the RA function is authorized by the ECAC PMA to setup its subscribing CA under the Government Intermediate CAs.

4.1.1.3 Commercial TSPs:

The TSP authorized representative submits the certificate application as part of the overall process through which the RA function is authorized by the ECAC PMA to setup its subscribing CA under the Commercial Intermediate CAs.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 The NR-CA and its intermediate CAs:

The processes related to standard certificate lifecycle (Issuance, rekey and revocation) of the NR-CA, Government intermediate CAs and Commercial intermediate CAs are specified as part the ECAC PMA operations manuals and key ceremony documentation.

Any of the certificate lifecycle management processes is authorized by the ECAC PMA and executed by the RA function.

The RA Function executes a verification checklist on the data used to process certifications requests to ensure full compliance with this CP/CPS. The ECAC PMA compliance function conducts regular supervision audits on the RA function operations to validate that the aforementioned verification is done properly.

4.1.2.2 Government and Commercial TSPs:

TSPs submit the certificate application to ECAC (RA Function) as follows:

1. The TSP downloads the Application form with the Subscriber Agreement from the ECAC repository website https://ecac.pki.gov.pk
2. The form is filled and signed by the Official Representative of the Applicant. The applicant must provide the following information in the form:
    a. Information related to the organization:
        i. Legal Name of the entity (organization)
        ii. Official address of the entity for correspondence
        iii. Official Representative name of the entity
        iv. Applicant Representative(s) name of the entity
    b. Information related to the TSP CA Certificate
        i. Description of the planned TSP certificate usage
        ii. Select the TSP certificate types if more than one certificate usage is required
        iii. TSP registered domain name(s) e.g., example.com if the TLS or SMIME CA certificates will be issued
        iv. Required certificate profiles and the values of each attribute that should be present in the CA certificate
    c. Subscriber Agreement:

i. The Subscriber Agreement must be initialed by the Official Representative of the entity
ii. The last page should be signed and stamped by the Official Representative

d. Information on Compliance Requirements:
   i. CP/CPS document of the TSP
   ii. Proof of the Physical Site requirements to run the TSP
   iii. Proof the Hardware Security Module used to hold the CA key
   iv. Details of the PKI Application that will be used to run the CA operations
   v. Proof on the conducted conformance assessment as per the TSP accreditation framework

3. The Application form is scanned and submitted to the RA function ECAC

Certificate applications will be deemed acceptable only if the below checklist is cleared by the RA function:

- Organization identity verification as per section 3.2.2,
- Identification of authorized representative(s) as per section 3.2.2,
- Validation of authority as per section 3.2.5,
- Presentation of a compelling business case by the TSP for the requested CA
- Conformance of the certificate request format and structure, this includes the conformance of the certificate request with the corresponding CA profile specified in this CP/CPS
- The organization name to be added to the certificate matches the validate formal organization name or an abbreviated version,
- The subject TSP CA is technically constrained using a combination of extended key usage and name constraint extensions to limit the scope within which the issuing CA may issue end user certificates,
- A formal, signed subscriber agreement by the applicant's authorized representative,
- Provision of reasonable assurance on the TSP control on its internal and/or external RA function(s)
- All other requirements are met by the TSP as per the national TSP framework, this includes but not limited to:
  - The CPS and other documentation are developed by the TSP and reviewed by the ECAC PMA,
  - Required conformance assessment cycle has been established by the TSP.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 The NR-CA and its intermediate CAs:

Certificate applications to the NR-CA are limited to the Government and Commercial Intermediate CAs that are owned and operated by ECAC. Therefore, the processing of those applications involves authorized representative(s) from RA function within operated by the ECAC PMA itself.

4.2.1.2 Government and Commercial TSPs:

The certificate application is only processed once the RA function has performed the following identification and authentication:

- Blacklist check: If the requestor/organization is in the blacklist, the certificate application is rejected,
- Any malicious certificate or revocation request or a request that fails multiple (more than 3) times is added to the ECAC blacklist,
- Verify the identity of the organization, authorized representative and the requester as specified in section 3.2.2,
- Verify the signed approval is received from the authorized representative though a signed certificate request form and certificate subscriber agreement,
- Verify that the legal name of the organization requesting a certificate and the organization name to be inserted in the requested certificate are matching. The full name or the abbreviated version may be added to the certificate as agreed with the requesting organization.

All above activities (e-mail communication, phone calls, vetting evidence) are stored along with the certificate application.

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 The NR-CA and its intermediate CAs:

The NR-CA, Government intermediate CAs and Commercial intermediate CAs are established as part of the ECAC PMA internal processes. The ECAC PMA authorizes the setup of these CAs after validating that all pre-requisites are met including the fulfilment of all compliance verifications (refer to the steps described in section 4.2.1).

4.2.2.2 Government and Commercial TSPs:

Once the identification and authentication as done as described in section 4.2.1 and an authorization granted by the ECAC PMA as described in section 4.1.2, the ECAC PMA shall plan the ceremony execution with relevant stakeholders to conduct the subordinate CA signing key ceremony.

In case of application rejection, the ECAC PMA shares formal response detailing the reasons of rejection with the applicant.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

4.3.1.1 The government and commercial intermediate CAs:

The required ECAC CA operators, keys custodians and the ECAC PMA representatives gather at the ceremony room located at the primary facility to conduct the key and certificate generation ceremony of the subject CA(s).

The key stages of the ceremonies conducted by the ECAC PKI is summarized below:

- Identity verification is done for all the ceremony attendees by the ceremony auditor,
- Ceremony authorization is verified by the ceremony auditor as well as the key custodians,
- Verify that the certificate request contains valid data as per the corresponding certificate profile defined in this CP/CPS,

After the successful verification of the above, the following actions are performed:

- The operators of the intermediate CA (to which the certificate is being issued) generated the CA key using the CA software on the CA's designated HSM,
- The intermediate CA operators issue the certificate request based on the generated key pair (in PKCS#10 format),
- The intermediate CA operators submit the certificate request to the ECAC NR-CA operators,
- The ECAC NR-CA operators submit the certificate request to the NR-CA to perform a certificate signing operation,
- The NR-CA CA operators and the ceremony auditor, validate the issued certificate's content against the profile defined and this CP/CPS,
- The certificate is then handed over to the corresponding Intermediate CA operators,
- Intermediate CA operators imports the certificate into the target CA software.

Further details on the certificate issuing process are documented in the designated key ceremony documentation.

4.3.1.2 Government and Commercial TSPs:

The required ECAC CA operators, keys custodians and other relevant ceremony attendees gather at the ceremony room located at the primary facility to conduct the certificate generation ceremony of the subject CA(s).

The key stages of the ceremonies conducted by the ECAC PKI is summarized below:

- Identity verification is done for all the ceremony attendees by the ceremony auditor/witness,
- Ceremony authorization is verified by the ceremony auditor/witness as well as the key custodians,
- Verify the certificate request format (shall be in PKCS#10 format),
- Verify that the certificate request contains valid subscriber data as per the certificate application,

After the successful verification of the above, the following actions are performed:

- The ECAC CA operators submit the certificate request to the relevant Intermediate CA to perform a certificate signing operation,
- The ECAC CA operators and the ceremony auditor/witness, validate the issued certificate's content against the profile defined and this CP/CPS and the information submitted in the certificate application,

- The certificate is then handed over to the TSP representative.

Further details on the certificate issuing process are documented in the designated key ceremony documentation.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Following issuance of a certificate, the issued certificate is handed over to the subscriber.

The ECAC RA function also publishes the issued certificate through the Trust List as if applicable on the CA repository.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

4.4.1.1 The government and commercial intermediate CAs:

The certificate is considered as accepted if successfully imported to the target CA systems as part of the same ceremony where the certificate is generated. The certificate is then published on the CA repository.

In case issues are raised in relation to certificate contents or to the acceptance of the certificate by the target systems, The RA function will then coordinate with the ECAC PMA to plan and execute another ceremony to issue a corrected certificate.

4.4.1.2 Government and Commercial TSPs:

After the successful key ceremony completion, the certificate is delivered to the TSP representative. The TSP imports the certificate into their CA System. If the certificate is imported successfully, the RA function is notified, and the certificate is published on the TSP repository which constitutes the formal acceptance by the TSP of the certificate issued by the ECAC Intermediate CA.

In case, the certificate could not be processed by the TSP CA System, an investigation is started by the TSP involving the ECAC RA function. If no options can be agreed to obtain the certificate acceptance by the TSP System, the certificate shall be revoked by the ECAC RA function. The RA function will then coordinate with the TSP to plan and execute another ceremony to issue a corrected certificate.

4.4.2 Publication of the Certificate by the CA

4.4.2.1 The government and commercial intermediate CAs:

Following the acceptance of a certificate, ECAC publishes the issued certificate on the CA Repository.

4.4.2.2 Government and Commercial TSPs:

Following the acceptance of a certificate, ECAC publishes the issued certificate through the Trusted List.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No other entities or organizations are notified directly of the certificate issuance. They are indirectly notified through the CA Repository as well as the Trusted List.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Unless otherwise stated in this CP/CPS, the subscriber's responsibilities include:

- Providing correct and up-to-date information as part of its application,
- Only using certificates for legal and authorized purposes in accordance with the common general requirements applicable to this CP/CPS, and with its CPS,
- Protecting its own CA private keys (and related secrets) from compromise, loss, disclosure, or otherwise unauthorized use of their private keys,
- Notifying the RA function immediately if any details in the certificate become invalid, or because of any compromise, loss, disclosure, or otherwise unauthorized use of their private keys,
- Not using the certificate outside its validity period, or after it has been revoked.

4.5.2 Relying Party Public Key and Certificate Usage

A party relying on a certificate issued by the NR-CA or its intermediate CAs shall:

- Use software that is compliant with X.509 and applicable IETF PKIX standards to validate the certificate signature and validity period,
- Validate the certificate by using the CRL, or the OCSP validity status information service in accordance with the certificate path validation procedure,
- Trust the certificate only if it has not been revoked and is within the validity period,
- Trust the certificate only for the signing of certificates and CRLs.

4.6 Certificate Renewal

Certificate Renewal is the process of issuing of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate except the validity period.

The Certificate Renewal is not supported for the NR-CA nor its intermediate CAs. Only certificate re-key is supported.

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

Not 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.

4.7.1 Circumstance for Certificate Re-Key

The following are the possible reasons for the certificate re-key:

1. The CA certificate has expired or about to expire
2. The CA certificate has been revoked
3. The Key Usage Period has reached or about to reach as described in Section 6.3.2

The re-key operation may not invalidate existing active certificate(s) since the existing certificate(s) can still be continued to sign CRLs and OCSP responder certificates.

The re-key process (including identity validation, certificate issuance and communication to relevant parties) is similar to the initial certificate application.

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

The NR-CA and its intermediate CAs do not support the certificate modification. In case the Subscriber wants to change the certified information, or the certificate has been revoked due to any of the circumstances mentioned in Section 4.9 and want to get a new certificate, the Subscriber shall apply for a certificate re-key.

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

Certificate suspension is not allowed. Only permanent certificate revocation is allowed.

The revocation of the NR-CA certificate or an NR-CA's intermediate CA certificate is a critical process that is described in the ECAC Disaster Recovery and Business Continuity Plan.

The revocation of the Government and Commercial TSPs certificates is handled as per the below subsections.

4.9.1 Circumstances for Revocation

Revocation of a TSP certificate can be initiated based on the following events:

- Receiving a revocation request from the TSP in writing,
- Receiving a notification from the TSP that the original certificate request was not authorized and does not retroactively grant authorization,
- TSP ceases operations and activates its TSP termination plan which involves the TSP CAs certificate revocation,
- Obtained evidence that any of the information appearing in the Certificate is inaccurate or misleading,
- Obtained an evidence that the TSP Private Key corresponding to the Public Key in the Certificate no longer complies with the requirements of SSL Baseline Requirements Sections 6.1.5 and 6.1.6,
- Obtained evidence that the TSP CA's Private Key has been a lost, stolen, or compromised,
- Obtained evidence that the TSP certificate was misused,
- TSP did not successfully complete the regular surveillance audit as per the national TSP accreditation framework, or didn't operate continuously in accordance with the provisions of this CP/CPS and the TSP CP, leading the ECAC

PMA to conclude that the identified issues cause an unacceptable risk to the Web Trust status of the Pakistan National PKI,

- The ECAC ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate,
- The ECAC issuing CA or the TSP CA's right to issue Certificates under these requirements expires or is revoked or terminated,
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Supplier or Relying Parties.
- Revocation is required by this CP/CPS.

Whenever any of the above circumstances occur, a PMA meeting is organized no later than twenty-four (24) hours after the circumstance of certificate revocation is realized. The outcome of this meeting is the validation of the circumstances triggering the TSP CA certificate revocation request and the related revocation reason. The ECAC PMA may request additional information/evidence which shall be provided within a maximum of seventy-two (72) hours. At the end of this process, the TSP CA certificate revocation is approved by the ECAC PMA, that is followed by the following actions:

- A certificate revocation ceremony is then planned and executed no later than seventy-two (72) hours after the CA certificate revocation is approved,
- Update the Trusted list to reflect the certificate/service revocation,
- Notify the TSP (and other relevant stakeholders). It the responsibility of the TSP to trigger its termination plan and initiate proper communication towards all their affected subscribers,
- Update the CCADB and communicate as required with the Root Programs,
- Record all communication, reports, and evidence in relation to the certificate revocation operation for future reference and audit processes.

4.9.2 Who Can Request Revocation

The authority to revoke the NR-CA or its intermediate CAs rests within the ECAC.

A revocation of a TSP certificate can be requested by:

1. The Subscriber himself, or
2. The ECAC at its own discretion (as per revocation reasons listed in section 4.9.1).

Revocation requests from TSPs are only accepted if the subscriber is authorized and authenticated to request revocation for the specific certificate (i.e., the subscriber is linked to the certificate through the certificate application request or other means).

Subscribers, relying parties, application software suppliers, and other third parties may submit Certificate Problem Reports to notify the ECAC PMA of a suspected reasonable cause to initiate the certificate revocation process.

4.9.3 Procedure for Revocation Request

The procedure for a Subordinate certificate revocation is as follows:

- A request to revoke certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (Ex. digitally, or manually signed),
- The request is authenticated by the RA function as per section 3.4,
- A PMA meeting is organized as described in section 4.9.1 to study the request, conclude a decision, then plan the revocation ceremony,
- The ECAC's intermediate CAs produces a new CRL which is published to its repository, the CA also pushes the revocation status to the OCSP service,
- The ECAC PMA addresses the actions specified in section 4.9.1 following the revocation ceremony,
- If applicable based on the circumstance of revocation, the ECAC may update its internal blacklist with details of the revoked certificate and/or the subscriber's details.

Certificate problems reporting:

Subscribers, relying parties, application software suppliers, and other third parties may submit certificate problem reports to ECAC via contact details provided in this document.

The ECAC discloses instructions related to certificate revocation and certificate problem reporting on its public repository. For any certificate problem report, the notifier is requested to include his contact details, suspected abuse, and related domain name. The ECAC PMA begins the investigation of a certificate problem report within 24 hours of receipt and decide whether revocation or other appropriate actions are required.

4.9.4 Revocation Request Grace Period

There is no revocation grace period. Revocation requests are processed by the RA function timely after a decision for revocation is made and within the timeframes listed under section 4.9.1.

4.9.5 Time Within Which CA Must Process the Revocation Request

For certificate problem reports, The ECAC PMA begins investigations within 24 hours from receiving the report. The ECAC PMA initiates communication with the Subscriber and where appropriate, with other concerned authorities. A preliminary communication on the certificate problem is sent to the Subscriber and to the originator of the problem report.

The ECAC PMA performs further investigations involving the TSP and other relevant authorities 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 within the timeframe set forth in Section 4.9.1.

Based on the revocation circumstance, the ECAC PMA may agree with the TSP on a plan to issue a new certificate as permitted by the national TPS accreditation framework.

4.9.6 Revocation Checking Requirement for Relying Parties

The revocation information is made available to the relying parties through CRLs which are publicly available on the CA repository and through the OCSP responders. Relying parties can use either method to validate the certificate.

4.9.7 CRL Issuance Frequency (If Applicable)

CRLs shall be issued as per Section 2.3 of this CP/CPS.

4.9.8 Maximum Latency for CRLs (if applicable)

Not stipulation.

4.9.9 On-Line Revocation/Status Checking Availability

The ECAC OCSP responders conform to RFC 6960. The OCSP certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC 6960.

The OCSP URL to be queried by relying party organizations is referenced in the certificates issued by the ECAC CAs.

4.9.10 On-Line Revocation Checking Requirements

The ECAC OCSP responders support both HTTP GET and HTTP POST methods.

The NR-CA and its intermediate CAs update information provided via their OCSP responders (i) every six months; and (ii) within 24 hours after revoking a Subordinate CA Certificate.

The ECAC OCSP responders that receive a request for status of a certificate that has not been issued, shall not respond with a "good" status for such Certificates. OCSP responders for CAs which are not Technically Constrained, in line with Section 7.1.5, will not respond with a "good" status for such Certificates.

The ECAC operations team monitors the OCSP responders for requests for "unused" serial numbers as part of its security monitoring procedures and any such case will trigger further investigation.

4.9.11 Other Forms of Revocation Advertisements Available

Not stipulation.

4.9.12 Special Requirements Re Key Compromise

Not stipulation.

4.9.13 Circumstances for Suspension

The ECAC CAs do not support the certificate suspension.

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

4.10.1 Operational Characteristics

CRLs shall be published on a public repository to be available to relying parties through HTTP protocol queries.

OCSP responder exposes an HTTP interface accessible to relying parties.

4.10.2 Service Availability

The public repository where certificate information and CRLs are published shall be available 24 hours a day and 7 days a week, with an availability percentage of minimum 99 % over one year.

The ECAC PMA commits to 24X7 availability for responding to high-priority certificate problem report as described in section 4.9.3 of this CP/CPS.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

The TSP subscription ends when a certificate is revoked, expired or the service is terminated. The end of subscription shall occur as part of an execution of the TSP's termination plan.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

ECAC CAs Private Keys are not escrowed, and the ECAC is not providing the Key Escrow services to the Subordinate CAs.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not supported. The ECAC CAs do not provide session key encapsulation and recovery services.

5 Facility, Management, and Operational Controls

This section specifies the physical and procedural security controls implemented by the ECAC on relevant domains of the ECAC CAs operations.

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

1. Physical security and environmental controls,
2. System integrity controls, including configuration and change management, patch management, vulnerability management and malware/virus detection/prevention,
3. Maintaining an inventory of all assets and manage the assets according to their classification,

4. Network security and firewall management, including port restrictions and IP address filtering,
5. User management, separate trusted-role assignments, education, awareness, and training, and
6. Logical access controls, activity logging and monitoring, and regular user access review to provide individual accountability.

The TSPs shall implement similar security controls to protect the operation of their CA(s) in line with this CP/CPS as well as the TSP CP.

5.1 Physical Security Controls

The ECAC PMA ensures that appropriate physical controls are implemented at the ECAC CAs hosting facilities. Such controls are documented as part of the ECAC's internal policies that are enforced and verified regularly through internal audits performed by the ECAC PMA on the ECAC 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 ECAC. Physical security controls are enforced so that access of unauthorized persons is prevented through five 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 ECAC CAs' systems.

5.1.2 Physical Access

With the five tiers of physical security protecting the ECAC CA systems are protected, access to the lower tiers is possible only by first gaining access through the higher tiers. Sensitive CA operational activities related to certificate lifecycle management occur within very restrictive physical tiers.

Physical security controls include security guard-controlled building access, biometric access, and CCTV monitoring protect the CA systems from unauthorized access, these controls are be monitored on a 24x7x365 basis. 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.

Unauthorized personnel, including un-trusted or third-party employees or visitors, are not allowed into the enclave(cage) without a prior approval and without an escort from one of ECAC's trusted employees.

5.1.3 Power And Air Conditioning

The design of the facility hosting the ECAC CAs provides UPS and backup generators with enough capability to support the CA 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 CA systems. All these systems ensure that the ECAC CAs' equipment continuously operate within the manufacturers' range of operating temperatures and humidity.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

The ECAC CAs hosting facility follows leading practices and applicable safety regulations in Pakistan, 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 shall be destroyed before discarding. Paper media shall be shredded using a crosshatch shredder, and magnetic media shall be wiped by de-magnetization, or physically destroyed. HSMs and related key management devices shall be physically destroyed, or securely wiped (zeroized) prior to disposal.

Authorization shall be granted for the destruction or disposable of any media.

5.1.8 Off-Site Backup

Full and incremental backups of the ECAC CAs' systems are taken regularly to provide enough recovery information when the recovery of the ECAC CAs' systems is necessary.

At least one full backup and several incremental backups of the ECAC CAs' online systems are taken daily in accordance with documented backup policies and procedures followed by the ECAC CAs operations team.

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 procedurals controls that apply to the primary facility.

5.2 Procedural Controls

The ECAC PMA follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the ECAC CAs' staff members, and the satisfactory performance of their duties in the field of PKI governance, operations, and service delivery.
The procedural controls include the following:

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 shall be maintained and reviewed annually.

The following are the trusted roles for the ECAC CAs:

- **PKI System Administration:** Staff authorized to install and configure the ECAC CAs, and to perform back-up, recovery, and maintenance operations. Also authorized to add other users in the target CA systems
- **PKI System Operation:** Staff Authorized to execute the ECAC CAs operational cycle and is involved in critical operations such as subscribers' certification operations and ECAC CAs' CRLs generation
- **Key Management Operation:** Staff Authorized to operate as key custodians and hold key material and secrets necessary for the execution of ECAC CAs' operational ceremonies
- **HSM Administration:** Staff Authorized to hold HSM activation data and secrets necessary for the HSM operations
- **Monitoring & Compliance:** Staff authorized to collect and review the audit logs generated by the ECAC CAs' systems for monitoring purposes and regular internal compliance audits.
- **Registration Authority**: Staff Authorized to conduct the vetting as part of the certification requests' processing.

5.2.2 Number of Persons Required per Task

The ECAC operations team 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 presence of two or more persons:

- Physical access to the secure enclave where the 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 ECAC PMA confirms the identity and history of the employee by carrying out background and security checks

- When instructed through the internal ECAC processes, the facility operations team issues an access card to each staff who needs to physically access equipment located in the secure enclave
- ECAC CAs dedicated staff (system administrators) issue the necessary ICT system credentials for ECAC CAs staff to perform their respective functions.

5.2.4 Roles Requiring Separation of Duties

The ECAC PMA ensures separation of duties among the following work groups:

- Operating personnel (RA officers, PKI Operators, key custodians, Support etc.)
- Administrative personnel (system admins, network admins, HSM admins etc.)
- Security personnel (enforce security measures)
- Audit personnel (review audit logs)

5.3 Personnel Controls

The ECAC ensures implementation of security controls regarding the duties and performance of the members of the ECAC CAs staff. These security controls are documented in an internal confidential policy, yet it includes the areas below.

5.3.1 Qualifications, Experience, and Clearance Requirements

Prior to engagement of an NTC PKI staff member, whether as an employee, agent, or an independent contractor, the ECAC PMA 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:

1. Verify the Identity of Such Person: Verification of identity MUST be performed through:
   A. Personal (physical) presence of such person before trusted persons who perform human resource or security functions, and
   B. Verification of well-recognized forms of government-issued photo identification; and
2. Verify the Trustworthiness of Such Person: Verification of trustworthiness includes background checks, which address at least the following, or their equivalent:
   A. Criminal convictions for serious crimes,
   B. Misrepresentations by the candidate,
   C. Appropriateness of references, and
   D. 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 ECAC PMA ensures that these checks are performed once yearly for all personnel holding trusted roles.

5.3.3 Training Requirements

The ECAC PMA makes available relevant technical training for their personnel to perform their functions.

For personnel performing information verification and vetting (i.e.,RA officers), public key infrastructure topics, authentication and vetting policies and procedures, applicable CP and CPS material and common threats to the information verification process are included.

The required skills and knowledge for validation specialists are tested through an examination on the information verification requirements outlined in the Baseline Requirements.

5.3.4 Retraining Frequency and Requirements

The training curriculum is delivered to all ECAC CAs staff. The training content is reviewed and amended on a yearly basis to reflect the latest leading practices and the CA systems' configuration changes.

5.3.5 Job Rotation Frequency and Sequence

The ECAC PMA ensures that any change in the ECAC CAs staff will not affect the operational effectiveness, continuity, and integrity of the CA services.

5.3.6 Sanctions for Unauthorized Actions

To maintain accountability on ECAC CAs' staff, the ECAC PMA sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems, according to the relevant human resources policy and procedures, and the applicable Pakistan law.

5.3.7 Independent Contractor Requirements

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

A. Criminal convictions for serious crimes,
B. Misrepresentations by the candidate,
C. Appropriateness of references,
D. Any clearances as deemed appropriate,
E. Privacy protection, and
F. Confidentiality conditions.

5.3.8 Documentation Supplied to Personnel

The ECAC PMA shall document all training material and make it available to ECAC CAs staff.

The ECAC PMA shall also ensure that the key operational documentation is made available to the relevant staff members. This includes, at a minimum, this CP/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 is covering 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 shall be generated and preserved.

These logs shall be reviewed by the ECAC CAs Monitoring and Compliance team and are also subject to review as part of the regular internal audits performed by the ECAC PMA on the ECAC CAs operations.

5.4.1 Types of Events Recorded

Audit logs are generated for all events relating to the security and services of the ECAC CAs systems. 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 ECAC CAs operations team and may be made available during compliance audits.

Following events occurring in relation to the ECAC CAs operations are recorded:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival and destruction
  - Cryptographic device life-cycle management events
- CA and Subscriber Certificate lifecycle management events, including:
  - Certificate requests, re-key requests, and revocation
  - All issued certificates including revoked and expired Certificates
  - Verification activities evidence (e.g., date, time, calls, persons communicated with)
  - Acceptance and rejection of certificate requests
  - Issuance of certificates
  - CRL updates (including OCSP entries updates where applicable)
- Security events, including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed
  - Security profiles and configuration changes
  - User management operations
  - System platform issues (e.g., crashes), hardware failures
  - Firewall and router activities
  - Entries an exists from the CA facility.

5.4.2 Frequency Of Processing Log

The ECAC PMA 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 ECAC PMA:

- Audit and Security logs of the CA applications shall be reviewed by the Monitoring & Compliance team every six months (since the CAs are all offline),
- Audit and Security of the online CA systems (Ex. OCSP responder) shall be 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 ECAC CAs systems shall be reviewed by the Monitoring & Compliance team on quarterly basis to validate the physical and logical access policies
- The ECAC PMA audit and compliance function executes an internal audit on the ECAC CAs operations on yearly basis. Samples of the log review reports and collected audit logs since the last audit cycle shall be requested by the ECAC PMA 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 ECAC CAs shall retain the following, for at least two (2) years:

A. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1) after the later occurrence of:
   i. the destruction of the CA Private Key; or
   ii. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509 v3 basic Constraints extension with the CA field set to true and which share a common Public Key corresponding to the CA Private Key,

B. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1) after the revocation or expiration of the Subscriber Certificate,

C. Any security event records (as set forth in Section 5.4.1) 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:

- The ECAC CAs systems generates cryptographically protected audit logs
- The security of audits logs is maintained while these logs transit by the backup system and when these logs are archived
- The access control policies enforced on the ECAC CAs systems ensures that read access only is granted to personnel having access to audit logs as part of their operational duties
- 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 ECAC CAs operations personnel.

5.4.5 Audit Log Backup Procedures

The following rules apply for the backup of the ECAC CAs audit log:

- Backup media are stored locally in the ECAC CAs main site, in a secure location
- 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 ECAC PMA 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 ECAC CAs 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 the ECAC has in place to counter such threats.

The ECAC CAs systems and infrastructure shall be also subject to regular security assessment as follows:

- Quarterly automated vulnerability scan of all public and internal IP addresses of ECAC CAs core and supporting PKI systems. This regular self-assessment activity is executed by security personnel part of the ECAC CAs operations team
- On an annual basis, the ECAC PMA coordinates a third-party independent vulnerability assessment and penetration testing is conducted on the ECAC CAs systems,
- The outcome of the regular assessments and identified issues shall be made available to the ECAC PMA and PKI operations management, who shall be responsible to organize and oversee the execution of the remediations by the respective teams.

Evidence of the vulnerability assessment and penetration testing activities execution are collected and archived by the relevant ECAC CAs personnel.

5.5 Records Archival

5.5.1 Types of Records Archived

The ECAC CAs shall archive all audit logs (as set forth in Section 5.4.1) in addition to the following:

A. Documentation related to the security of CA systems, and
B. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

5.5.2 Retention Period for Archive

Archived audit logs (as set forth in Section 5.5.1) shall be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

Additionally, the ECAC CAs shall retain, for at least two (2) years:

A. All archived documentation related to the security of CA Systems (as set forth in Section 5.5.1),
B. 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:
    i. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates, or
    ii. 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 are able to 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 ECAC CAs. The ECAC CAs 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 ECAC CAs online systems is synchronized with the time source of a GPS clock. Further, the ECAC CAs operations team enforce a procedure that checks and corrects any clock drift.

5.5.6 Archive Collection System (Internal or External)

The EAC CAs archive collection system is internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized and authenticated staff shall be allowed to access archived material. The ECAC CAs operations team use the ECAC 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 ECAC CAs' key shall be changed with a frequency that ensures the ECAC CAs shall have 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 CP/CPS document for key changeover frequency.

To support revocation management of issued certificate, the old CA private keys are maintained until such time as all relying certificates 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 ECAC CAs is detected by the ECAC PMA, it shall perform 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 ECAC's Business continuity and disaster recovery plan shall be followed. Otherwise, the scope of potential damage shall be 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 ECAC PMA 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 ECAC 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

The ECAC shall implement the necessary measures to ensure full recovery of the ECAC CAs' services in case of a disaster, corrupted servers, software, or data. That is subject to the PMA authorization to trigger incident recovery procedures.

The ECAC 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 ECAC 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

Compromise of the ECAC CAs private key(s), or of the associated activation data is considered as a mission-critical incident that triggers a process and related procedures, detailed in the ECAC disaster recovery and business continuity plan.

Considering the criticality of such compromise situation and its impact on the Pakistan National PKI, The ECAC PMA will be invited for 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 ECAC disaster recovery and business continuity plan is triggered to restore the minimum ECAC CAs required operational capabilities, in a timely fashion. In particular, the plan targets the recovery of the following services, either on the primary location, 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 ECAC CAs disaster recovery location are made possible considering the ECAC CAs backup system that enables the continuous replication of critical ECAC CAs data from the primary site to the disaster recovery site. That allows a recovery of the ECAC CAs critical services at the disaster recovery location within a maximum of twelve (12) hours RTO.

The ECAC business continuity plan defines the following:

- Conditions for activating the plan
- Fall-back and resumption procedures
- The responsibilities of the individuals involved in the plan execution
- Recovery time objective (RTO)
- Recovery procedures
- The plan to maintain or restore the business operations in a timely manner following interruption to or failure of critical business processes
- Key termination plan (in case of ECAC CAs key compromise)
- Procedures for securing the main facility to the extent possible during the period following a disaster and up to recovery of operations in a secure environment in either the main, or secondary site.

5.8 CA or RA Termination

If the ECAC PMA determines that a termination of one or all ECAC CAs is deemed necessary, the CA termination plan shall be executed covering the following:

1. Minimize disruption caused by the termination of CA as much as possible,
2. Ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings. The retention of archived data specified in Section 5.5,

3. Ensure Certificate status information services are maintained for the applicable period,
4. Terminate all authorization of sub-contractors to act on behalf of the terminated CA in the performance of any functions related to the process of issuing certificates,
5. Notify subscribers, relying parties and other stakeholders (Ex. auditors and root programs). Notification procedures shall exist for informing affected entities and transferring archived CA records to an appropriate custodian.

6 Technical Security Controls

This section defines the security measures that the ECAC takes to protect its CAs' cryptographic keys and activation data (Ex. PINs, passwords, or key access tokens).

The TSPs shall defines and follow similar security measures to protect their CA keys in line with this CP/CPS as well as the TSP CP. Nevertheless, certain distinctions for TSPs are made in the below subsection where applicable for better clarity.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 The NR-CA and its intermediate CAs:

The ECAC PMA plans and supervises the execution of the key generation ceremonies of the ECAC CAs (Root CA and Subordinate CAs). Keys are generated and stored on an HSMs that must meet the requirements of FIPS 140-2 Level 3 profile. The ECAC PMA uses a trustworthy system and takes the required precautions to prevent compromise or unauthorized use, according to documented Key Generation Ceremony (KGC) procedures.

Following the WebTrust and CA/Browser Forum Guidelines, the ECAC PMA use trustworthy systems and ensures the incorporation of the following requirements upon execution of KGCs:

- The KGC is subject to the formal authorization of the ECAC PMA
- The KGC is conducted in presence of a combination of authorized personnel with trusted roles including representatives from the ECAC PMA
- The KGC is witnessed by the CA's Qualified Auditor (see section 8 Compliance Audit and Other Assessments)
- Proper distribution of secrets/activation data/key shares to the trusted operatives and key custodians
- The Qualified Auditor issues a ceremony witness report, establishing that the NR-CA and its intermediate CAs, during its Key Pair and Certificate generation process:
    - Documented its key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement (this CP/CPS)
    - Included appropriate detail in its Key Generation Script
    - Maintained effective controls to provide reasonable assurance that the CAs' key pairs were generated and protected in conformity with the procedures described in this CP/CPS and in the Key Generation Script

- Performed, during the key generation process, all the procedures required by its Key Generation Script
- A video of the entire key generation ceremony will be recorded and stored securely for audit purposes

6.1.1.2 Government and Commercial TSPs:

The ECAC PMA oversees the establishment of the Government and Commercial TSPs and approves their respective ceremonies after the completion of several verifications including the successful completion of a surveillance audit on the TSP operations. The key generation ceremony for the TSP CA is witnessed by the ECAC PMA audit function. The security measures that are in place for the key generation of the TSP CAs shall be described in their respective CPS.

6.1.2 Private Key Delivery to Subscriber

For the NR-CA and its intermediate CAs, refer to Section 6.1.1, while ECAC does not generate private keys for Subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

For the intermediate CAs' public keys, public keys are generated and submitted to the NR-CA as part of the corresponding the intermediate CA KGC that includes root-certification of the intermediate CA's public key by the NR-CA.

For the TSPs' public keys, the public keys are submitted to the corresponding intermediate CA by a TSP's representative as part of a certificate generation ceremony.

6.1.4 CA Public Key Delivery to Relying Parties

The ECAC CAs Certificates are published as soon as it is issued on the ECAC public repository.

6.1.5 Key Sizes

NR-CA generates and uses a 4096-bit RSA Key with Secure Hash Algorithm version 2 (SHA256) to self-sign NR-CA certificate, NR-CA OCSP certificate, intermediate CA certificates & NR-CA CRL that it issues.

Each intermediate CA generates and uses a 4096-bit RSA Key with Secure Hash Algorithm version 2 (SHA256) to sign the Subscriber CA certificates, intermediate CA OCSP certificate, and intermediate CA CRL that it issues.

6.1.6 Public Key Parameters Generation and Quality Checking

The CAs' public key module generation is accomplished with HSM devices that conforms to FIPS 186-2 for random generation and primality checks.

The ECAC CAs' operations team references the Baseline Requirements Section 6.1.6 on quality checking.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

The Key usage is set to keyCertSign and CRLSign for the ECAC CAs' certificates.

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 ECAC CAs 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 ECAC CAs hosting facility.

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

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

ECAC CAs personnel are assigned to the trusted roles by the ECAC PMA ensuring segregation of duties and enforcing the principles of multi control and split knowledge. Multi-person control of the ECAC CAs 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 ECAC CAs private key.

The ECAC PMA 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 ECAC CAs are not escrowed. Dedicated backup and restore procedures of the ECAC CAs private key are implemented by the ECAC PMA.

Private keys of the TSP CAs may not be escrowed.

6.2.4 Private Key Backup

The ECAC CAs' private keys are backed up and held stored safely in exclusive safes maintained in the most inner security zones of the ECAC CAs hosting facility.

Backup operations are executed as part of the ECAC CAs' key generation ceremonies. The ECAC CAs' 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 ECAC CAs private keys that are physically transported from the primary facility to the DR one using a dedicated HSM handling and key handling procedure part of the overall ECAC CAs' key ceremony procedure. Dedicated personnel in trusted roles participate in the transport operation, which is escorted by security guards.

Refer to Section 6.2.2 for further details.

6.2.5 Private Key Archival

The ECAC PMA does not require to archive the CAs' private keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The ECAC CAs' key pairs shall 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 shall the ECAC CAs' private keys be 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

Private keys for the ECAC CAs shall be activated following the principles of dual control and split knowledge. The activation procedure shall use a PIN entry device attached to the ECAC CAs' HSMs.

6.2.9 Method of Deactivating Private Key

Private keys for the ECAC CAs shall be deactivated in situations such as:

- There is a power failure within the secure enclave,
- The CA HSM is operated outside the range of supported temperatures, or
- The HSM detects a security breach and deletes all key material within its internal memory.

The ECAC CAs' private keys may also be routinely deactivated through procedures enforcing the principles of dual control and split knowledge and involving individuals holding trusted roles.

6.2.10 Method of Destroying Private Key

Destroying the ECAC CAs' private key outside the context of the end of its lifetime shall be authorized by multiple members of the ECAC PMA.

The ECAC CAs' keys are destroyed through documented procedures involving individuals in trusted roles. These procedures shall enforce the principle of multi-person control and split knowledge. The procedures shall also ensure that the ECAC CAs' keys are destroyed by removing permanently from any hardware modules the keys are stored on.

6.2.11 Cryptographic Module Rating

The ECAC CAs cryptographic modules shall be certified/validated against [FIPS 140-2] Level 3 or [ISO 15408] Common Criteria (CC) EAL 4+ or above and protection profiles from [CEN EN 419 221] series.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Refer to Section 5.5 for archival conditions.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The following table describes the Validity Period and Key Usage Period of all CAs in the Pakistan PKI hierarchy:

CA Name	Validity Period	Key Usage Period
NR-CA	25 years	8 years
NR-CA's Intermediate CAs	17 years	5 years
TSP CAs (non-issuing)	12 years	4 years
TSP CAs (issuing)	8 years	3 years

No Certificate will be issued by the CA that is beyond the life of the CA itself.

The CA will be rekeyed before approaching the Key Usage Period. The original key will not be used to sign the certificates but only CRLs and OCSP responder certificates after the Key Usage Period.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The ECAC CAs' 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 CP/CPS for further details.

6.4.2 Activation Data Protection

The ECAC CAs' key management policy and ceremony procedures ensure that the principles of multi-person control and split knowledge are permanently enforced to protect ECAC CAs keys and HSMs activation data. During the KGCs, activation data are permanently under the custody of the designated ECAC trusted personnel. Refer to Section 6.1 and 6.2 for further details.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The ECAC 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 ECAC CAs internal policy documentation.

In particular, the ECAC CAs systems and its operations are subject to the following security controls:

- Separation of duties and dual controls for CA operations
- Physical and logical access control enforcement
- Audit of application and security related events
- Continuous monitoring of ECAC CAs systems and end-point protection

- Backup and recovery mechanisms for ECAC CAs operations
- Hardening of ECAC CAs servers' operating system according to leading practices and vendor recommendations
- In-depth network security architecture including perimeter and internal firewalls, web application firewalls, including intrusion detection systems
- Proactive patch management as part of the ECAC CAs operational processes
- The ECAC CAs systems enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer Security Rating

No stipulation — this section intentionally left blank.

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 ECAC 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 ECAC CAs' operations team.

All ECAC 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 ECAC CAs shall be dedicated to performing only CAs' related tasks. There shall be no other applications, hardware devices, network connections or component software, which are not part of the PKI, connected to or installed on CA hardware.

The ECAC CAs' equipment is scanned for malicious code on first use and periodically thereafter. Authorized personnel must ensure up-to-date virus definition databases in place before each ECAC CAs usage.

Refer to Section 6.6.1 for further details.

6.6.3 Life Cycle Security Controls

Refer to Section 6.6.1 for details.

6.7 Network Security Controls

The ECAC CAs are deployed on the offline machines that are not connected to the network. The equipment and secret materials are maintained in the innermost zone of the ECAC CAs hosting facility.

The ECAC CAs' repository and OCSP responder are online system supporting the ECAC CAs' operations and enabling service provision to relying parties, in compliance with the provisions of this CP/CPS. An in-depth network security architecture is enforced, including perimeter and internal firewalls, web application firewalls, end-point protection, including intrusion detection systems. The network is segmented into several zones based on a defined conceptual and functional architecture for the ECAC CAs systems. These controls and technologies limit the services allowed to and from the ECAC CAs' online services.

The ECAC PMA ensures regular vulnerability testing is conducted on the ECAC CAs' online services. The ECAC PMA also ensures that at least once a year, penetration testing is conducted on the ECAC CAs connected systems, by an independent third-party.

6.8 Timestamping

The ECAC CAs are deployed on the offline laptops which are not connected to the network hence no NTP service available for these offline machines. The machine time is verified by the quorum in charge of activating the laptops during the ceremonies and the machine time is used to generate the archived logs.

The NTP server is available for the connected infrastructure. It is used to synchronize the time of the servers that hosts the OCSP and Timestamping services.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

ECAC Root CA

National Root CA Certificate Profile					
Field	CE[1]	O/M[2]	CO[3]	Value	Comment
Certificate		M			
TBSCertificate		M	D		See 4.1.2 of RFC 5280
Signature	False	M			
Algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	ECAC Root CA G1 Signature.	ECAC Root CA G1 signature value
TBSCertificate					
Version	False	M			
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
Algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M	S		
CountryName				PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName				Electronic Certification Accreditation Council	PrintableString
CommonName				ECAC Root CA G1	PrintableString
Validity	False	M			Implementations MUST specify using UTC time

[1] CE = Critical Extension.
[2] O/M: O = Optional, M = Mandatory.
[3] CO = Content: S = Static, D = Dynamic

					until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[300]** Months	25 years
Subject	False	M			
CountryName		M	S	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Electronic Certification Accreditation Council	PrintableString
CommonName		M	S	ECAC Root CA G1	PrintableString
SubjectPublicKeyInfo	False	M			
Algorithm		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		M			
Authority Properties					
crlDistributionPoints	False	O			
DistributionPoint		O	D	http://repository-ecac.pki.gov.pk/repository/crl/root_ca.crl	NR CA CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	SHA-1 Hash	
KeyUsage	True	M			
KeyCertSign		M	S	True	
cRLSign		M	S	True	
BasicConstraints	True	M			
CA		M	S	True	TRUE for CA Certificates

ECAC Intermediate CAs

Field	CE[4]	O/M[5]	CO[6]	Value	Comment
Certificate		M			
TBSCertificate		M	D		See 4.1.2 of RFC 5280
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	ECAC Root CA Signature	ECAC Root CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer	False	M	S		
CountryName		M	S	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Electronic Certification Accreditation Council	PrintableString
CommonName		M	S	ECAC Root CA G1	PrintableString
Validity	False	M			Implementations MUST specify

[4] CE = Critical Extension.
[5] O/M: O = Optional, M = Mandatory.
[6] CO = Content: S = Static, D = Dynamic

					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 + **[204]** Months	17 years
subject	False	M			
countryName		M	S	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
organizationName		M	S	Electronic Certification Accreditation Council	PrintableString
commonName		M	S	**For Gov. SMIME CA:** "ECAC Government SMIME CA G1" **For Gov. Client Auth CA:** "ECAC Government Client Authentication CA G1" **For Gov. TLS CA:** ECAC Government TLS CA G1 **For Gov. Code Signing CA:** ECAC Government Code Signing CA G1 **For Gov. Timestamping CA:** ECAC Government Timestamping CA G1 **For Comm. SMIME CA:** "ECAC Commercial SMIME CA G1" **For Comm. Client Auth CA:** "ECAC Commercial Client Authentication CA G1" **For Comm. TLS CA:**	PrintableString

					ECAC Commercial TLS CA G1 **For Comm. Code Signing CA:** ECAC Commercial Code Signing CA G1 **For Comm. Timestamping CA:** ECAC Commercial Timestamping CA G1	
subjectPublicKeyInfo		False	M			
	algorithm			S	RSA OID: 1.2.840.113549.1.1.1	
	subjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions			M			
Authority Properties						
authorityKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the issuer CA public key
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	S	http://ocsp.pki.gov.pk	OCSP responder URL
	AccessMethod		O	S	Id-ad-2 2 *id-ad-caIssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		O	S	http://repository-ecac.pki.gov.pk/repository/cert/root_ca.p7b	NR CA certificate download URL
cRLDistributionPoints		False	M			
	distributionPoint		M	D	http://repository-ecac.pki.gov.pk/repository/crl/root_ca.crl	NR CA CRL download URL.

Subject Properties					
subjectKeyIdentifier	False	M			
keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties					
KeyUsage	True	M			
keyCertSign		M	S	True	
cRLSign		M	S	True	
ExtendedKeyUsage	False	M			
For Gov. SMIME CA: emailProtection **For Gov. Client Auth CA:** clientAuth **For Gov. TLS CA:** serverAuth clientAuth **For Gov. Code Signing CA:** codesigning **For Gov. Timestamping CA:** timeStamping **For Comm. SMIME CA:** emailProtection **For Comm. Client Auth CA:** clientAuth **For Comm. TLS CA:** serverAuth clientAuth **For Comm. Code Signing CA:** codeSigning **For Comm. Timestamping CA:**		M	S	True	

	timeStamping					
Certificate Policy Properties						
certificatePolicies		False	O			
	PolicyIdentifier		M	S	1.3.6.1.4.1.59337.1.1	
	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	https://ecac.pki.gov.pk/repository/cps	
BasicConstraints		True				
	cA		M	S	True	

Issuing TSP CAs

Field	CE[7]	O/M[8]	CO[9]	Value	Comment
Certificate		M			
TBSCertificate		M	D		See 4.1.2 of RFC 5280
Signature	False	M			
algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
signatureValue		M	D	Issuing CA Signature.	Issuing CA signature value
TBSCertificate					
Version	False				
		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy Validated on duplicates.
signature	False	M			

[7] CE = Critical Extension.
[8] O/M: O = Optional, M = Mandatory.
[9] CO = Content: S = Static, D = Dynamic

	algorithm		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
issuer		False	M	S		
	CountryName		M	S	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	OrganizationName		M	S	Electronic Certification Accreditation Council	PrintableString
	CommonName		M	S	CN of the ECAC intermediate CA	PrintableString
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 + **[96]** Months	8 years
subject		False	M			
	jurisdictionCountryName		M	S	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280) Required only in the EV CA certificates.
	businessCategory		M	S	"Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon the TSP type.	PrintableString Required only in the EV CA certificates.

	serialNumber		M	S	For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the relevant authority. For Government Entities that do not have a Registration Number, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity.	PrintableString Required only in the EV CA certificates.
	countryName		M	S	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
	organizationName		M	S	Allocated as per certificate request	PrintableString
	commonName		M	S	Allocated as per certificate request	PrintableString
subjectPublicKeyInfo		False	M			
	algorithm		M	S	RSA	
	subjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Authority Properties						
authorityKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of the issuer CA public key
authorityInfoAccess		False	M			
	AccessMethod		M	S	Id-ad-2 1 *id-ad-ocsp OID i.e.*1.3.6.1.5.5.7.48.1 (ca ocsp)	OCSP Responder field
	accessLocation		M	S	http://ocsp.pki.gov.pk	OCSP responder URL

	AccessMethod		O	S	Id-ad-2 2 *id-ad-caIssuers OID i.e.*1.3.6.1.5.5.7.48.2 (ca cert)	CA Issuers field
	accessLocation		O	S	http://repository-ecac.pki.gov.pk/repository/cert/[intermediate ca]_g1.p7b	Intermediate CA CA Certificate download URL
cRLDistributionPoints		False	M			
	distributionPoint		M	D	http://repository-ecac.pki.gov.pk/repository/crl/[intermediate_ca].crl	Intermediate CA CRL download URL.
Subject Properties						
subjectKeyIdentifier		False	M			
	keyIdentifier		M	D	SHA-1 Hash	
Key Usage Properties						
KeyUsage		True	M			
	keyCertSign		M	S	True	
	cRLSign		M	S	True	
ExtendedKeyUsage		False	M			
	For SMIME CAs: emailProtection **For Client Auth CAs:** clientAuth **For TLS and EV TLS CAs:** serverAuth clientAuth **For Code Signing and EV Code Signing CAs:** codeSigning **For Timestamping CAs:** timestamping		M	S	True	
Certificate Policy Properties						
certificatePolicies		False	O			
	PolicyIdentifier		M	S	1.3.6.1.4.1.59337.1.1	

	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	https://ecac.pki.gov.pk/repository/cps	
certificatePolicies		False	O			
	PolicyIdentifier		M	S	**For Code Signing CAs:** 2.23.140.1.4.1 **For EV Code Signing CAs:** 2.23.140.1.3 **For Timestamping CAs:** 2.23.140.1.4.2 **For TLS CAs:** 2.23.140.1.2.2 **For EV TLS CAs:** 2.23.140.1.1	
BasicConstraints		True				
	cA		M	S	True	
	pathLength		M	S	0	

7.1.1 Version Number(s)

The EACA CAs issue X.509 version 3 certificates as defined in RFC 5280.

7.1.2 Certificate Extensions

X509 V3 extensions are supported and explained in the certificate profiles described in Section 7.1.

TSPs' CA certificates may include any extensions as specified by RFC 5280 in a certificate but must include those extensions required by this CP/CPS. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP/CPS.

7.1.3 Algorithm Object Identifiers

Algorithms OIDs conform to IETF RFC 3279 and RFC 5280 and described in Section 7.1

7.1.4 Name Forms

Name forms are in the X.500 distinguished name form according to RFC 3739. The supported Subject Attributes are detailed in Section 7.1.

7.1.5 Name Constraints

Name constraints are supported as per RFC 5280.

X.509 v3 Name Constraints extension is included in the ECAC CAs' certificates, yet it may be used for the TSPs CAs where the id-kp-serverAuth or id-kp-emailProtection is used.

7.1.6 Certificate Policy Object Identifier

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

The ECAC CAs use certificate policy object identifiers that are defined for the Pakistan National PKI OID scheme.

The used OIDs are specified as part of the certificate profiles in Section 7.1.

7.1.7 Usage of Policy Constraints Extension

Policy Constraints extension is not supported.

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificate policies extensions must be processed as per RFC 5280.

7.2 CRL Profile

CRL Profile					
Field	CE[2]	O/M[3]	CO[4]	Value	Comment
CertificateList		M			
TBSCertificate					
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	CA's Signature.	CA's signature value
TbSCertList	False				
Version	False	M			
Version		M	S	2	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M	S		

CountryName		M	S	PK	
OrganizationName		M	S	Electronic Certification Accreditation Council	
CommonName		M	S	CN of the CAs	
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
thisUpdate		M	D	<creation time>	
NextUpdate		M	D	<Creation time> + **[184]** days	
RevokedCertificates	False	O			
Certificate					
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	O			
CRLReason		M	S	As per RFC 5280	Identifies the reason for the certificate revocation
Invalidity Date		O	S	Date when the certificate is supposed to be invalid	Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
CRLExtensions	False	M			
AuthorityKeyIdentifier	False	M	D	SHA-1 Hash	160-bit SHA-1 hash of subjectPublicKey

					of the issuing CA public key
CRL Number	False	M	D		Sequential CRL Number
expiredCertsOnCRL	False	O	D		< a date-time value specifies the date on or after which revoked certificates are retained on the CRL>
AuthorityInfoAccess	False	O			
AccessMethod		M	S	Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)	
AccessLocation		M	S	http://repository-ecac.pki.gov.pk/repository/cert/[root or intermediate ca].p7b	CA Certificate download URL over HTTP

7.2.1 Version Number(S)

The ECAC CAs support X509 v2 CRLs.

7.2.2 CRL and CRL Entry Extensions

The ECAC CAs' use the CRL and CRL entry extensions as described in section 7.2.

7.3 OCSP Profile

OCSP Response Signing Certificate Profile					
Field	CE[2]	O/M[3]	CO[4]	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	CA's Signature.	CA's signature value

TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M	S	<Issuing CA's Subject>	The issuer field is defined as the X.501 type "Name"
CountryName				PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName				Electronic Certification Accreditation Council	PrintableString
CommonName				CN of the ECAC CAs	PrintableString
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	12 months

Subject	False	M	D		
CountryName		M		PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M		Electronic Certification Accreditation Council	PrintableString
stateOrProvinceName		M	S	Pakistan	PrintableString
CommonName		M		**For Gov. SMIME CA:** "ECAC Government SMIME CA OCSP - 2023" **For Gov. Client Auth CA:** "ECAC Government Client Authentication CA OCSP - 2023" **For Gov. TLS CA:** "ECAC Government TLS CA OCSP - 2023" **For Gov. Code Signing CA:** "ECAC Government Code Signing CA OCSP – 2023" **For Gov. Timestamping CA:** "ECAC Government Timestamping CA OCSP - 2023" **For Comm. SMIME CA:** "ECAC Commercial SMIME CA OCSP - 2023" **For Comm. Client Auth CA:** "ECAC Commercial Client	PrintableString

				Authentication CA OCSP - 2023" **For Comm. TLS CA:** "ECAC Commercial TLS CA OCSP - 2023" **For Comm. Code Signing CA:** "ECAC Commercial Code Signing CA OCSP - 2023" **For Comm. Timestamping CA:** "ECAC Commercial Timestamping CA OCSP - 2023"	
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions		M			
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of subjectPublicKey
Policy Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
nonRepudiation		M	S	True	
extKeyUsage	False	M			
id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck	False	M			
certificatePolicies	False	M			
PolicyIdentifier		M	S	1.3.6.1.4.1.59337.1.1	

	policyQualifiers:policyQualifierId		O	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		O	D	https://ecac.pki.gov.pk/repository/cps	

7.3.1 Version Number(s)

The ECAC CAs support the v1 OCSP responses according to RFC 6960.

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

The ECAC PMA conducts regular internal audits covering the ECAC CAs operations as well as the TSPs operations. Conducting these audits and following up on remediation of audit findings, is part of ECAC PMA operational cycle that is done at least annually.

The ECAC PMA also organizes an external WebTrust audit to ensure that it meets applicable requirements, standards, procedures, and service levels at least on an annual basis. The ECAC 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 ECAC PMA evaluates the results of such audits before further implementing them.

8.2 Identity/Qualifications of Assessor

The external WebTrust 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 for Certification Authorities
- 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 ECAC PMA has its own audit function that is independent of the ECAC PKI operations team.

External auditors are independent third party WebTrust practitioners.

8.4 Topics Covered by Assessment

The ECAC CAs are audited for compliance to the following standard:

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline with Network Security
- WebTrust Principles and Criteria for Certification Authorities - Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities - Code Signing Baseline Requirements

8.5 Actions Taken as a Result of Deficiency

Issues and findings resulting from the assessment are reported to the ECAC PMA.

The final audit report includes the issues and findings as well as the agreed corrective action plan and target date for resolution.

The issues and findings are tracked until resolution by the ECAC PMA. Additional audits are planned and carried out sufficient to reach full compliance.

8.6 Communication of Results

The internal audit reports are communicated to the ECAC PMA and shall not be disclosed to non-authorized third parties.

External audits reports are published on the ECAC CAs public repository.

8.7 Self-audit

The head of each IT Service Line within the IT function shall be responsible for implementing internal controls related to IT within their IT Service Line. They shall establish the KPIs and a process of assessment of the controls to ensure their effective functioning. The established KPIs shall be reviewed and approved by the PMA.

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 the ECAC and the TSP.

9.1.2 Certificate Access Fees

No fees will be charged to access the issued certificates.

9.1.3 Revocation Or Status Information Access Fees

No fees will be charged for the certificate revocation and status information access.

9.1.4 Fees for Other Services

ECAC may charge the for services depending on the business needs and subject to PMA approval.

9.1.5 Refund Policy

No refund will be made for any charged fee.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

The ECAC ensures that the ECAC CAs are covered by existing government insurance provisions. Details of coverage are specified in the applicable agreements.

9.2.2 Other Assets

The ECAC maintains sufficient financial resources to maintain operations and fulfill duties of the ECAC CAs.

9.2.3 Insurance or Warranty Coverage for End-Entities

Refer to section 9.6.1.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The ECAC 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 the ECAC and its suppliers
- ECAC 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 (refer to section 9.3.1) is deemed public. This includes the information published on the ECAC CAs public repository.

9.3.3 Responsibility to Protect Confidential Information

The ECAC protects confidential information through adequate training and policy enforcement with its employees, contractors, and suppliers.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The ECAC observes personal data privacy rules and privacy rules as specified in the present CP/CPS. 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 subscriber private information for the purpose of certificate lifecycle management.

The ECAC will not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. When the ECAC releases private information, ECAC 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 Islamic Republic of Pakistan.

The 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.

All communications channels with the ECAC/its RA function shall preserve the privacy and confidentiality of any exchanged private information. Data encryption shall be used when electronic communication channels are used with the ECAC systems. This shall include:

- Communications between the ECAC RA systems and the subscribers (TSPs)
- Communications between the ECAC CAs and the ECAC RA 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 ECAC employees, suppliers and contractors handle personal information in strict confidence under the ECAC 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

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

Unless otherwise stated in this CP/CPS, the ECAC Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The ECAC 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

The ECAC owns and reserves all intellectual property rights associated with the ECAC CAs databases, repository, the ECAC CAs digital certificates and any other publication originating from the ECAC PMA, including this CP/CPS.

The ECAC CAs use software from third-party PKI products suppliers. This software remains the intellectual property of the product suppliers, and its usage by the ECAC CAs bound by license agreements between the ECAC PMA and these suppliers.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The ECAC warrants that their ECAC procedures are implemented in accordance with this CP/CPS, and that any certificates issued under this document are in accordance with the stipulations specified.

By issuing a certificate, the ECAC 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 NR-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

The ECAC represents and warrants to the Certificate Beneficiaries that, during the period when the certificate is valid, the ECAC has complied with the Baseline Requirements and its CP/CPS in issuing and managing the certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

- **Authorization for Certificate:** That, at the time of issuance, the ECAC:
  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 CP/CPS.
- **Accuracy of Information:** That, at the time of issuance, the ECAC:
  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 CP/CPS.
- **No Misleading Information:** That, at the time of issuance, the ECAC:
  i. implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading,
  ii. followed the procedure when issuing the Certificate,and
  iii. accurately described the procedure in this CP/CPS
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the ECAC:
  i. implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2,
  ii. followed the procedure when issuing the Certificate,
  iii. accurately described the procedure in this CP/CPS.
- **Subscriber Agreement:** That, if the ECAC CAs 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 ECAC maintains a 24 x 7 publicly accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates.
- **Revocation:** That the ECAC will revoke the Certificate for any of the reasons specified in these Requirements.

The ECAC SHALL be responsible for the performance and warranties of Subordinate CAs, for the TSP CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the ECAC CAs were the Subordinate CA issuing the Certificates.

9.6.2 RA Representations and Warranties

The ECAC warrants that it performs RA functions as per the stipulations specified in this CP/CPS.

9.6.3 Subscriber Representations and Warranties

The ECAC implements 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 ECAC, both in the certificate request and as otherwise requested by ECAC in connection with the issuance of the Certificate(s) to be supplied by the ECAC CAs
- **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:** To use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement
- **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 ECAC instructions concerning Key Compromise or Certificate misuse within a specified time period.
- **Acknowledgment and Acceptance:** An acknowledgment and acceptance that the ECAC 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 this CP/CPS, or the Baseline Requirements,

- **Caseation of certificate use:** Upon termination of Subscriber Agreement, revocation, or expiration of the Subscriber Certificate, immediately cease use of the Subscriber Certificate according to the subscriber's termination plan.

9.6.4 Relying Party Representations and Warranties

Relying Parties who rely upon the certificates issued under the ECAC shall:

- 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 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 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 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 TSPs or relying parties on information contained in this CP/CPS or any other documentation made public by the ECAC PMA and related to the ECAC services.

9.8 Limitations of Liability

- The ECAC will not incur any liability to TSPs or their Subscribers to the extent that such liability results from their negligence, fraud, or willful misconduct
- The ECAC assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under this CP/CPS for any use other than in accordance with this document. TSPs will immediately indemnify the ECAC from and against any such liability and costs and claims arising there from

- The ECAC will not be liable to any party whosoever for any damages suffered whether directly or indirectly because of an uncontrollable disruption of its services
- TSPs are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by ECAC
- TSP to compensate a Relying Party which incurs a loss because of the TSP's breach of Subscriber's agreement
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations; and
- The ECAC denies any financial or any other kind of responsibility for damages or impairments resulting from the ECAC CAs'operations.

9.9 Indemnities

This CP/CPS does not include any claims of indemnity.

9.10 Term And Termination

9.10.1 Term

This CP/CPS is approved by the ECAC PMA and shall remain in force until amendments are published on the ECAC CAs repository and relevant communication towards TSPs.

9.10.2 Termination

Amendments to this document are applied and approved by the ECAC PMA and marked by an indicated new version of the document. Upon publishing on the ECAC repository, the newer version becomes effective. The older versions of this document are archived by the ECAC on its repository.

9.10.3 Effect of Termination and Survival

The ECAC PMA coordinates communications towards the TSPs in relation to the termination (and related effects) of this document.

9.11 Individual Notices and Communications with Participants

Notices related to this CP/CPS can be addressed to the ECAC PMA contact address as stated in section 1.5.

9.12 Amendments

When changes are required to be done on this CP/CPS. The ECAC PMA 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 ECAC repository, the newer version of the CP/CPS becomes effective. The older versions of this document are archived on the ECAC CAs repository.

The ECAC PMA coordinates communication in relation to the amendments of this CP/CPS and related effects.

The ECAC PMA reserve the right to amend this CP/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

Major changes to this CP/CPS that may materially change the acceptability of certificates for specific purposes, may require corresponding changes to the OID or qualifier (URL). The ECAC PMA shall coordinate proper communication with relevant parties.

9.13 Dispute Resolution Provisions

All disputes associated with the provisions of this CP/CPS and the ECAC CA services, shall be first addressed by the ECAC PMA legal function. If mediation by the ECAC PMA legal function is not successful, then the dispute shall be adjudicated by the relevant courts of Pakistan.

9.14 Governing Law

The laws of the Islamic Republic of Pakistan shall govern the enforceability, construction, interpretation, and validity of this CP/CPS.

9.15 Compliance with Applicable Law

This CP/CPS and provision of ECAC CAs certification services are compliant to relevant and applicable laws of the Islamic Republic of Pakistan. In particular:

- Electronic Transaction Ordinance, 2002

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 the ECAC CA CP/CPS or any of its rights or duties under this CP/CPS, without the prior written consent of the ECAC.

9.16.3 Severability

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

In the event of a conflict between the Baseline Requirements and any regulation in Pakistan, the ECAC may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in Pakistan. This applies only to operations or certificate issuances that are subject to that Law. In such event, the ECAC 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 ECAC. The ECAC will also (prior to issuing a certificate

under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP/CPS. Any modification to the ECAC practice enabled under this section will be discontinued if and when 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 CP/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

The ECAC shall not be liable for any failure or delay in their performance under the provisions of this CP/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

No stipulation.

Document Approval

Reviewed By:

Name: ----------

Job Role/Function: ----------

Date: ----------

Signature: ----------

Approved By:

Name: ----------

Job Role/Function: ----------

Date: ----------

Signature: ----------