Pakistan National PKI

ECAC S/MIME Subordinate CA Certificate Practice Statement

Version control

Version	Date	Description / Status	Responsible
V2.0	29/11/2024	Initial version after the changes in the PKI hierarchy and ECAC's intermediate CAs /NTC CAs termination for review & approval	ECAC
V2.1	20/02/2025	Introduction of CAA for S/MIME	ECAC

Document Signoff

Version	Date	Responsible	Validated By	Reviewed and Approved By
V2.1	/ /2025	ECAC	ECAC (PMA)	ECAC (PMA)

Table of Contents

1 Introduction 11
1.1 Overview 11
1.1.1 Overview of ECAC Policy Management Authority (PMA) 13
1.2 Document Name and Identification 14
1.3 PKI Participants 14
1.3.1 Certification Authorities 14
1.3.2 Registration Authorities 15
1.3.3 Subscribers 16
1.3.4 Relying Parties 16
1.3.5 Other Participants 16
1.4 Certificate Usage 16
1.4.1 Appropriate Certificate Uses 16
1.4.2 Prohibited Certificate Uses 16
1.5 Policy Administration 16
1.5.1 Organization Administering the Document 16
1.5.2 Contact Person 17
1.5.3 Person Determining CPS Suitability for the Policy 17
1.5.4 CPS Approval Procedures 17
1.6 Definitions and Acronyms 18
1.6.1 Definitions 18
1.6.2 Acronyms 22
1.6.3 References 23
2 Publication and Repository Responsibilities 25
2.1 Repositories 25
2.2 Publication of Certification Information 25
2.3 Time or Frequency of Publication 25
2.3.1 CA Certificates 25
2.3.2 CRLs 25
2.4 Access Controls on Repositories 26
3 Identification and Authentication 27
3.1 Naming 27
3.1.1 Types of Names 27
3.1.2 Need for Names to be Meaningful 28

3.1.3 Anonymity or Pseudonymity of Subscribers 28
3.1.4 Rules for Interpreting Various Name Forms 28
3.1.5 Uniqueness of Names 28
3.1.6 Recognition, Authentication, and Role of Trademarks 28
3.2 Initial Identity Validation 29
3.2.1 Method to Prove Possession of Private Key 29
3.2.2 Authentication of Organization Identity 29
3.2.3 Validation of Mailbox Authorization or Control 30
3.2.4 Authentication of Individual Identity 30
3.2.5 Non-verified Subscriber Information 31
3.2.6 Validation of Authority 31
3.2.7 Criteria for Interoperation 31
3.3 Identification and Authentication for Re-key Requests 31
3.3.1 Identification and Authentication for Routine Re-key 31
3.3.2 Identification and Authentication for Re-key after Revocation 32
3.4 Identification and Authentication for Revocation Request 32
4 Certificate Life-Cycle Operational Requirements 33
4.1 Certificate Application 33
4.1.1 Who Can Submit a Certificate Application 33
4.1.2 Enrollment Process and Responsibilities 33
4.2 Certificate Application Processing 34
4.2.1 Performing Identification and Authentication Functions 34
4.2.2 Approval or Rejection of Certificate Applications 34
4.2.3 Time to Process Certificate Applications 35
4.3 Certificate Issuance 35
4.3.1 CA Actions During Certificate Issuance 35
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 35
4.4 Certificate Acceptance 36
4.4.1 Conduct Constituting Certificate Acceptance 36
4.4.2 Publication of the Certificate by the CA 36
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 36
4.5 Key Pair and Certificate Usage 36
4.5.1 Subscriber Private Key and Certificate Usage 36
4.5.2 Relying Party Public Key and Certificate Usage 36

4.6 Certificate Renewal 37
4.6.1 Circumstance for Certificate Renewal 37
4.6.2 Who May Request Renewal 37
4.6.3 Processing Certificate Renewal Requests 37
4.6.4 Notification of New Certificate Issuance to Subscriber 37
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 37
4.6.6 Publication of the Renewal Certificate by the CA 37
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 37
4.7 Certificate Re-Key 37
4.7.1 Circumstance for Certificate Re-Key 37
4.7.2 Who May Request Certification of a New Public Key 37
4.7.3 Processing Certificate Re-Keying Requests 37
4.7.4 Notification of New Certificate Issuance to Subscriber 37
4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 38
4.7.6 Publication of the Re-Keyed Certificate by the CA 38
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 38
4.8 Certificate Modification 38
4.8.1 Circumstance for Certificate Modification 38
4.8.2 Who May Request Certificate Modification 38
4.8.3 Processing Certificate Modification Requests 38
4.8.4 Notification of New Certificate Issuance to Subscriber 38
4.8.5 Conduct Constituting Acceptance of Modified Certificate 38
4.8.6 Publication of the Modified Certificate by the CA 38
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 38
4.9 Certificate Revocation and Suspension 38
4.9.1 Circumstances for Revocation 38
4.9.2 Who Can Request Revocation 40
4.9.3 Procedure for Revocation Request 40
4.9.4 Revocation Request Grace Period 42
4.9.5 Time Within Which CA Must Process the Revocation Request 42
4.9.6 Revocation Checking Requirement for Relying Parties 42
4.9.7 CRL Issuance Frequency (If Applicable) 42
4.9.8 Maximum Latency for CRLs (if applicable) 42
4.9.9 On-Line Revocation/Status Checking Availability 42

4.9.10 On-Line Revocation Checking Requirements 42
4.9.11 Other Forms of Revocation Advertisements Available 43
4.9.12 Special Requirements Re Key Compromise 43
4.9.13 Circumstances for Suspension 44
4.9.14 Who Can Request Suspension 44
4.9.15 Procedure for Suspension Request 44
4.9.16 Limits on Suspension Period 44
4.10 Certificate Status Services 44
4.10.1 Operational Characteristics 44
4.10.2 Service Availability 44
4.10.3 Optional Features 44
4.11 End of Subscription 44
4.12 Key Escrow and Recovery 45
4.12.1 Key Escrow and Recovery Policy and Practices 45
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 45
5 Facility, Management, and Operational Controls 46
5.1 Physical Security Controls 46
5.1.1 Site Location and Construction 46
5.1.2 Physical Access 46
5.1.3 Power And Air Conditioning 47
5.1.4 Water Exposures 47
5.1.5 Fire Prevention and Protection 47
5.1.6 Media Storage 47
5.1.7 Waste Disposal 47
5.1.8 Off-Site Backup 47
5.2 Procedural Controls 48
5.2.1 Trusted Roles 48
5.2.2 Number of Persons Required per Task 49
5.2.3 Identification and Authentication for each Role 49
5.2.4 Roles Requiring Separation of Duties 49
5.3 Pesonnel Controls 49
5.3.1 Qualifications, Experience, and Clearance Requirements 49
5.3.2 Background Check Procedures 50
5.3.3 Training Requirements 50

5.3.4 Retraining Frequency and Requirements 50
5.3.5 Job Rotation Frequency and Sequence 51
5.3.6 Sanctions for Unauthorized Actions 51
5.3.7 Independent Contractor Requirements 51
5.3.8 Documentation Supplied to Personnel 51
5.4 Audit Logging Procedures 51
5.4.1 Types of Events Recorded 51
5.4.2 Frequency of Processing Log 53
5.4.3 Retention Period for Audit Log 53
5.4.4 Protection Of Audit Log 54
5.4.5 Audit Log Backup Procedures 54
5.4.6 Audit Collection System (Internal vs. External) 54
5.4.7 Notification to Event-Causing Subject 54
5.4.8 Vulnerability Assessments 54
5.5 Records Archival 55
5.5.1 Types of Records Archived 55
5.5.2 Retention Period for Archive 55
5.5.3 Protection of Archive 56
5.5.4 Archive Backup Procedures 56
5.5.5 Requirements for Timestamping of Records 56
5.5.6 Archive Collection System (Internal or External) 56
5.5.7 Procedures to Obtain and Verify Archive Information 56
5.6 Key Changeover 56
5.7 Compromise And Disaster Recovery 57
5.7.1 Incident and Compromise Handling Procedures 57
5.7.2 Computing Resources, Software, and/or Data are Corrupted 57
5.7.3 Entity Private Key Compromise Procedures 57
5.7.4 Business Continuity Capabilities after a Disaster 57
5.8 CA or RA Termination 58
6 Technical Security Controls 60
6.1 Key Pair Generation and Installation 60
6.1.1 Key Pair Generation 60
6.1.2 Private Key Delivery to Subscriber 61
6.1.3 Public Key Delivery to Certificate Issuer 61

6.1.4 CA Public Key Delivery to Relying Parties 61
6.1.5 Key Sizes 61
6.1.6 Public Key Parameters Generation and Quality Checking 61
6.1.7 Key Usage Purposes (as per X.509 v3 key usage field) 61
6.2 Private Key Protection and Cryptographic Module Engineering Controls 61
6.2.1 Cryptographic Module Standards and Controls 61
6.2.2 Private Key (n out of m) Multi-person Control 61
6.2.3 Private Key Escrow 62
6.2.4 Private Key Backup 62
6.2.5 Private Key Archival 62
6.2.6 Private Key Transfer into or from a Cryptographic Module 62
6.2.7 Private key Storage on Cryptographic Module 62
6.2.8 Method of Activating Private Key 62
6.2.9 Method of Deactivating Private Key 63
6.2.10 Method of Destroying Private Key 63
6.2.11 Cryptographic Module Rating 63
6.3 Other Aspects of Key Pair Management 63
6.3.1 Public Key Archival 63
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 63
6.4 Activation Data 64
6.4.1 Activation Data Generation and Installation 64
6.4.2 Activation Data Protection 64
6.4.3 Other Aspects of Activation Data 64
6.5 Computer Security Controls 64
6.5.1 Specific Computer Security Technical Requirements 64
6.5.2 Computer Security Rating 65
6.6 Life Cycle Technical Controls 65
6.6.1 System Development Controls 65
6.6.2 Security Management Controls 65
6.6.3 Life Cycle Security Controls 65
6.7 Network Security Controls 66
6.8 Timestamping 66
7 Certificate, CRL, and OCSP Profiles 67
7.1 Certificate Profiles 67

7.1.1 Version Number(s) 76
7.1.2 Certificate Extensions 76
7.1.3 Algorithm Object Identifiers 76
7.1.4 Name forms 76
7.1.5 Name Constraints 76
7.1.6 Certificate Policy Object Identifier 77
7.1.7 Usage of Policy Constraints Extension 77
7.1.8 Policy Qualifiers Syntax and Semantics 77
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 77
7.2 CRL Profile 78
7.2.1 Version Number(S) 80
7.2.2 CRL and CRL Entry Extensions 80
7.3 OCSP Profile 81
7.3.1 Version Number(s) 84
7.3.2 OCSP Extensions 84
8 Compliance Audit and Other Assessments 85
8.1 Frequency or Circumstances of Assessment 85
8.2 Identity/Qualifications of Assessor 85
8.3 Assessor's Relationship to Assessed Entity 85
8.4 Topics Covered by Assessment 85
8.5 Actions Taken as a Result of Deficiency 86
8.6 Communication of Results 86
8.7 Self-audit 86
9 Other Business and Legal Matters 87
9.1 Fees 87
9.1.1 Certificate Issuance or Renewal Fees 87
9.1.2 Certificate Access Fees 87
9.1.3 Revocation Or Status Information Access Fees 87
9.1.4 Fees for Other Services 87
9.1.5 Refund Policy 87
9.2 Financial Responsibility 87
9.2.1 Insurance Coverage 87
9.2.2 Other Assets 87
9.2.3 Insurance or Warranty Coverage for End-Entities 87

9.3 Confidentiality of Business Information 87
9.3.1 Scope of Confidential Information 87
9.3.2 Information Not within the Scope of Confidential Information 87
9.3.3 Responsibility to Protect Confidential Information 87
9.4 Privacy of Personal Information 88
9.4.1 Privacy Plan 88
9.4.2 Information Treated as Private 88
9.4.3 Information Not Deemed Private 88
9.4.4 Responsibility to Protect Private Information 88
9.4.5 Notice and Consent to Use Private Information 89
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 89
9.4.7 Other Information Disclosure Circumstances 89
9.5 Intellectual Property Rights 89
9.6 Representations and Warranties 89
9.6.1 CA Representations and Warranties 89
9.6.2 RA Representations and Warranties 90
9.6.3 Subscriber Representations and Warranties 90
9.6.4 Relying Party Representations and Warranties 90
9.6.5 Representations and Warranties of Other Participants 90
9.7 Disclaimers Of Warranties 91
9.8 Limitations of Liability 91
9.9 Indemnities 91
9.10 Term And Termination 91
9.10.1 Term 91
9.10.2 Termination 91
9.10.3 Effect of Termination and Survival 92
9.11 Individual Notices and Communications with Participants 92
9.12 Amendments 92
9.12.1 Procedure for Amendment 92
9.12.2 Notification Mechanism and Period 92
9.12.3 Circumstances under which OID Must Be Changed 92
9.13 Dispute Resolution Provisions 92
9.14 Governing Law 92
9.15 Compliance with Applicable Law 92

9.16 Miscellaneous Provisions 93
9.16.1 Entire Agreement 93
9.16.2 Assignment 93
9.16.3 Severability 93
9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights) 93
9.16.5 Force Majeure 93
9.17 Other Provisions 93

1 Introduction

The present document is the Certification Practice Statement (CPS) describing the certification practices that apply to the Electronic Certification Accreditation Council (ECAC) S/MIME Subordinate CA. This CPS complies with the TSP Certificate Policy that is applicable to the provision of certification services offered by the Trust Services Providers (TSP) issuing publicly trusted certificates to end-entities in Pakistan.

This CPS addresses the technical, procedural, and organizational policies of the S/MIME Subordinate CA that is established and operated by ECAC under the Pakistan national PKI hierarchy, with regards to the complete lifetime of certificates issued by this CA.

This 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 ECAC S/MIME Subordinate CA. Such sections are denoted as "Not applicable". Additional information is presented in subsections of the standard structure where required.

This CPS complies with the Electronic Transaction Ordinance 2002 of Pakistan for Digital Signature and Electronic Certification.

This 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 – S/MIME
- WebTrust Principles and Criteria for Certification Authorities – Network Security

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

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates.
- CA/Browser Forum Network and Certificate System Security Requirements

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

Further information with regards to this CPS can be obtained from the PMA, using contact information provided in clause 1.5.

1.1 Overview

The Pakistan National PKI aims to provide digital certification and trust services to government and commercial sectors, enabling individuals and entities within Pakistan to conduct secure electronic transactions.
In this framework, ECAC operates as a trust service provider, delivering trust services to the government sector via a structured hierarchy of Certification Authorities (CAs). Furthermore, ECAC establishes a foundation for additional trust service providers that support both the commercial & Government sectors.

This setup provides a resilient framework to support variance in requirements between government and non-government sectors regarding the offering and consumption of certification and other trust services.

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

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

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

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

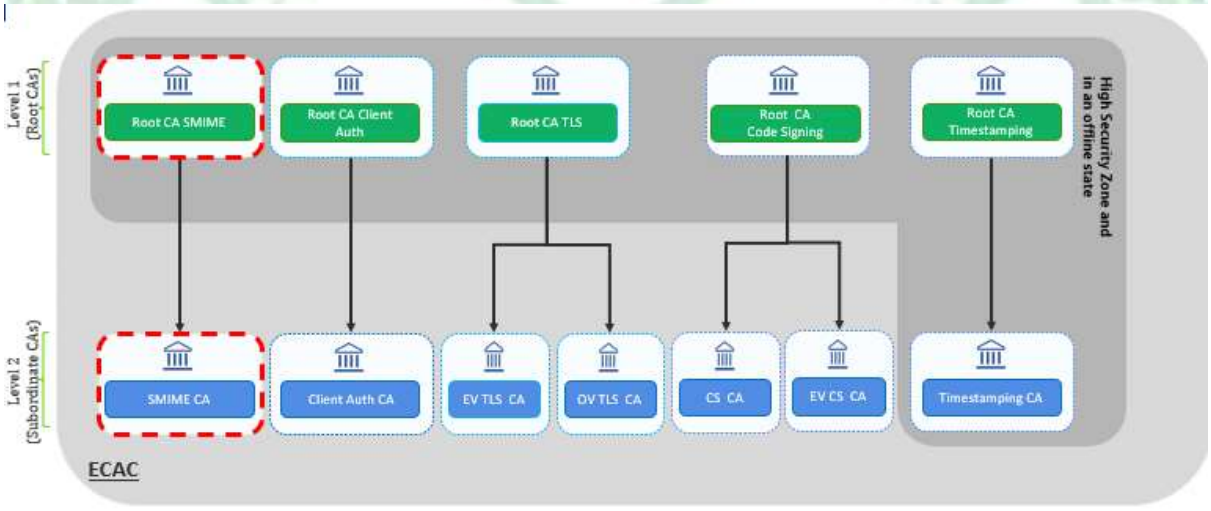

Figure 1 - Pakistan national PKI hierarchy

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

- **Code Signing CA:** Subordinate CA that will issue Non-EV code signing certificates to sign the libraries, exe, msi files etc.

[1] For S/MIME certificates, only the S/MIME Root CA is relevant since it signs the S/MIME Subordinate CAs certificates. Other Root CAs belongs to the ECAC PKI but aren't pertinent to code signing certificates issuance and are not included in the code signing hierarchy as depicted in Figure 1.

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

The above use cases are key enablers of digital transformation as they represent the corner stone of securing electronic transactions. Supporting these use cases under a unified trust model with government assurance, facilitates adoption, enables interoperability, and enhances user trust.

1.1.1 Overview of ECAC Policy Management Authority (PMA)

The ECAC PMA serves as the highest-level management body with ultimate authority and responsibility for Pakistan's national PKI. It is directly responsible for managing the operations of the NR-CAs and their Subordinate CAs (owned by ECAC), while also overseeing both Commercial and Government 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:

- **Responsible for the operations of the NR-CAs and their Subordinate CAs (owned by ECAC):** The ECAC runs the Registration Authority (RA) function as well as the technical operations of the NR-CAs and their Subordinate 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 maintains the National PKI framework including:
  - The PKI governance framework (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-CAs) 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 Commercial & Government TSPs in Pakistan:** The ECAC PMA manages the licensing of Commercial and Government TSPs under the national TSP accreditation framework. It accordingly approves, maintains, and publishes the list of approved TSPs/TS under the national TSP accreditation framework.

1.2 Document Name and Identification

This document is the "Certificate Practice Statement for Electronic Certification Accreditation Council (ECAC) S/MIME Subordinate CA", it's approved by the ECAC Policy Management Authority (PMA) for the publication. This CPS document is published at https://ecac.pki.gov.pk

ECAC will use the OID **1.3.6.1.4.1.59337.1.5** to identify this document.

1.3 PKI Participants

1.3.1 Certification Authorities

The S/MIME Subordinate CA (hereinafter, CA) are owned and operated by ECAC through its premises in Pakistan. These CAs has been approved by the PMA and signed by the S/MIME Root CA, as depicted in Figure 1 (section 1.1).

This CA provides the following certification services:

- **Certificate Generation Service —** it issues end-entity certificates based on the verification conducted by the Registration Authorities.
- **Dissemination Service —** it disseminates OCSP, CRL and CA certificates and makes them available to relying parties. This service also makes available any public policy and practice information to Subscribers and relying parties.
- **Revocation Management Service —** it processes requests and reports revocation data for determining the appropriate action to be taken. The results of this service are available through the certificate validity status service.
- **Certificate Validity Status Service —** it provides certificate validity status information to relying parties based upon certificate revocation lists and an OCSP responder service. The status information always reflects the current status of the certificates issued by this CA.

1.3.2 Registration Authorities

1.3.2.1 PMA RA function

A Registration Authority (RA) is the entity that performs the identification and authentication of certificate applicants for end-user certificates, initiates, or forwards revocation requests, and approves applications for certificate renewal on behalf of the CA.
ECAC PMA operates its own RA function and does not rely on Delegated Third Parties for RA functions.

The RA function falls within the PKI operations structure and responsible for identity verification and validation for the Pakistan government entities wishing to act as a local registration authority to issue Sponsor- validated S/MIME certificates to their own user communities (see section 1.3.2.2).

ECAC PMA does not delegate the validation process of domain ownership or control (domain portion of an email address) to a third-party.

1.3.2.2 Local RAs (LRAs)

ECAC provides the ability to government entities aiming to manage certificates lifecycle of their own user communities to act as a local registration authority (LRA) for a certain type of certificates that are issued for natural persons (ie. Sponsor-validated S/MIME certificates).
In this case, the requesting entity enters a contractual relationship (through an LRA agreement) with ECAC whereby the requesting entity establishes a local registration authority (LRA office) where RA officers belonging to the entity can operate.

The LRA agreement enforces obligations that include but not limited to:

- Authenticating, approving, or rejecting certificate application and revocation requests,
- Identify subscribers as per the naming conventions defined in this CPS, so that each subscriber is uniquely and unambiguously identified,
- Process certificate issuance and revocation requests with this CA based on validated and approved requests,
- Creating and maintaining an audit-log journal that records all significant events related to the RA's operations,
- Providing selective access to audit-log journal records as specified in this CPS,
- Implementing other operational controls as specified in this CPS,
- Processes and stores information according to the requirements defined in this CPS (particularly, in section 5).

ECAC technically implements the LRA function through a Web-based application offered for a duly authorized LRA officer(s) operating from designated LRA offices. A dedicated LRA account is issued for each LRA officer to manage certificates limited to

the user community belonging to the entity that LRA office belongs to. The LRA officers meet and follow the requirements set forth in Sections 4.2 and 5.3.

1.3.3 Subscribers

Subscribers of the CA are natural persons identified in association with a legal person (i.e., entity's employees) who apply for S/MIME (Sponsor-validated) Certificates from the CA and agree to be bound by the relevant Subscriber Agreement.

1.3.4 Relying Parties

Relying Parties must consistently refer to ECAC's Certificates Validity Status Service (i.e., CRL and OCSP), prior to relying on information featured in said certificate.

1.3.5 Other Participants

Other Participants include:

- Qualified independent WebTrust auditor who verifies the requirements set out in section 8.2.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The certificates issued pursuant to this CPS may be used for:

1) **Natural Person certificates**:
    a) **Sponsor- validated S/MIME**: used to digitally sign and encrypt an email message from a verified email address.
2) **OCSP Responder Certificates –** used to sign the Online Certificate Status Protocol (OCSP) responses for certificates issued by this CA.

1.4.2 Prohibited Certificate Uses

Subscribers are authorized to use their certificates for the purposes specified in section 1.4.1 of this CPS. The use of certificates for any other purposes is strictly prohibited.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The PMA has the overall responsibility for producing and publishing this document. The PMA maintains the PKI-OID subtree which represents the OID value used in the context of the Pakistan PKI framework.

The PMA is comprised of members with relevant PKI policy experience and appointed to conduct the following:

- Approve the ECAC's Root CP/CPSs and the TSP Subordinate CAs CPSs
- Supervise the operations of the NR-CAs and their Subordinate CAs through the operations team, ensuring alignment with the practices outlined in the CPS.
- Oversee the TSPs subordinate CAs operations.

- Produce, maintain, and publish the relevant policy documentation for the Pakistan PKI framework that includes TSP CP, this CP/CPS, CPS for the ECAC's Subordinate CA security policy and key management policy.
- Produce the key ceremony documentation for the NR-CAs and Subordinate CAs.
- Assess and decide on any changes that may impact the whole PKI hierarchy, including changes related to the PKI facility in both primary and DR sites and reflect these changes on the related NR-CAs policy documentation.

1.5.2 Contact Person

Information requests or inquiries related to the present document will only be accepted if addressed to the PMA at:

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 document only when they are addressed to the contact above.

Certificate Problem Report

ECAC maintains a continuous 24/7 ability to internally respond to any high priority revocation requests and certificate problem reports provides instructions for certificate revocation and certificate problem reporting on a dedicated page in its public repository, accessible at https://ecac.pki.gov.pk/repository/Certificate_Problem_Report.html. If ECAC deems appropriate, it may forward the revocation reports to law enforcement

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

The ECAC PMA will validate and investigate the request before taking an action 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 CPS based on the results and recommendations received from a Qualified Auditor as specified in Section 8.

1.5.4 CPS Approval Procedures

The PMA is responsible for formally approving this CPS and any subsequent versions before their publication in the public repository.

The Process entails reviewing the initial draft of this CPS and any subsequent modifications by the PMA's specialist staff (i.e. PMA members) to determine consistency with implemented best practice and with TSP CP prior to PMA approval. The modifications may take the form of a document containing a modified version of the CPS, or an update notice. Changes made into this CPS will be tracked in the revision table.

The PMA reviews this CPS at least annually, making revisions and updates to the policies as deemed necessary or as required by specific circumstances.

Prior to becoming applicable, the updated version of the CPS is announced in the repository as available on: https://ecac.pki.gov.pk.

Upon published, the updated version is binding on all Subscribers, including Subscribers and parties relying on Certificates issued under a previous version of the CPS.

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. In context of this CPS, Subordinate CAs issue certificates exclusively to government legal entities.

Applicant Representative – In the context of this document, the applicant representative is responsible for submitting legal entity's enrolment request as well LRAO management requests to the ECAC's PMA RA. He may be an LRAO himself. The words Applicant Representative and requester are used interchangeably.

Application Software Supplier: A supplier of email client software or other relying-party application software such as mail user agents (web-based or application based) and email service providers that process S/MIME Certificates.

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 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 Authority Authorization (or CAA) - From RFC 9495: "The Certification Authority Authorization (CAA) DNS resource record (RR) provides a mechanism for domains to express the allowed set of Certification Authorities that are authorized to issue certificates for the domain."

Certificate Beneficiaries: All Application Software Suppliers with whom the CA or its Root CA has entered into a contract for distribution of its Root Certificate in software distributed by such Application Software Suppliers and all Relying Parties who reasonably rely on such a Certificate while a Code Signature associated with the Certificate is valid.

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 define requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. Section 7 in the the present document provides a list of the certificate profiles defined within it.

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.

Delegated Third Party - A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.

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

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, county, etc.).

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria

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

Issuing CA – In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

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.

Local Registration Authority Officer (LRAO) - An employee or agent of an organization unaffiliated with the CA (i.e.g., ECAC) who authorizesis authorized to approve the issuance of Natural Person Certificates tofor that organization. In the case of ECAC, the the LRAO must be an employee or agent other than the RA officer.

Linting - A process in which the content of digitally signed data such as a Precertificate [RFC 6962], Certificate, CRL, or OCSP response, or data-to-be-signed object such as a tbsCertificate (as described in RFC 5280, Section 4.1.1.1) is checked for conformance with the profiles and requirements defined in these Requirements.

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.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

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. In the context of this CPS, the RA function is operated by ECAC.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

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.

Sponsor-validated - Refers to a Certificate Subject which combines Individual (Natural Person) attributes in conjunction with an subject:organizationName (an associated Legal Entity) attribute. Registration for Sponsor-validated Certificates MAY be performed by an Enterprise RA where the subject:organizationName is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject Organization

Subject – The Natural Person identified in a Certificate as the Subject. The Subject is either the Subscriber or a mailbox under the control and operation of the Subscriber.

Subject Identity Information – Information that identifies the Certificate Subject. Subject Identity Information does not include a Mailbox Address listed in the subject:commonName or subject:emailAddress fields, or in the subjectAltName extension.

Subordinate CA – A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA. In the context of this CPS, the Subordinate CA, are signed by S/MIME Root CA.

Subscriber – A Natural Person 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.

Validation Specialists: Someone who performs the information verification duties specified by these Requirements

Validity Period – The period of time from notBefore through notAfter, inclusive.

See S/MIME BR for additional definitions.

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
CS	Code Signing
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
LRAO	Local Registration Authority Officer
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
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
TSA	Timestamping Authority
TLS	Transport Layer Security
TSP	Trust Service Provider
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:

- X.509 - The standard of the ITU-T (International Telecommunications Union-T) for Certificates.
- 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 Principles and Criteria for Certification Authorities
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – S/MIME
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Network Security

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
- CA/Browser Forum Network and Certificate System Security Requirements
- Electronic Transaction Ordinance 2002 of Pakistan for Digital Signature and Electronic Certification

2 Publication and Repository Responsibilities

2.1 Repositories

ECAC maintains an online repository available 24 × 7 and accessible at: https://ecac.pki.gov.pk.

ECAC is responsible for making available the following information to be published on its repository:

- Current and previous version of ECAC's Subordinate CA CPSs;
- Current version of Root CP/CPS & TSP CP;
- Subscriber, LRA and relying party agreements, PKI disclosure statement, TSA CP/PS and TSA disclosure statement.
- The valid self-signed Root CA Certificates, as well as the Subordinate CA certificates, OCSP certificates, certificate Authority revocation lists (CARLs) and certificate revocation lists (CRLs) issued by the Subordinate CAs;
- Time-stamping Unit Certificates (TSU);
- Audit reports.

2.2 Publication of Certification Information

ECAC is the entity tasked with providing the information for publication, as outlined in section 2.1 of this document.

ECAC publishes certificate validity status information in frequent intervals as indicated in this 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 CA 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 these Subordinate CAs.

2.3 Time or Frequency of Publication

The PMA reviews this CPS at least once annually and makes appropriate changes so that the CA operations remain fully aligned to the requirements listed in section 1 of this CPS. Modified versions of the CPS and agreements (Subscriber and Relying party) are published within five days after the PMA approval.

2.3.1 CA Certificates

The CA and OCSP certificates are published to the public repository once they are issued until they are expired or rekeyed and the new certificates are issued, after which they are be moved to the archive.

2.3.2 CRLs

This CA maintain and publish CRLs as follows:

- A new CRL is generated every 24 hours, even if no changes have occurred since the last CRL issuance,
- CRL lifetime (i.e., value of the nextUpdate field) is set to 26 hours.

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 Subject names in the CA certificates comply with the X.500 distinguished names standards. The subject name used in the CA certificates is verified and validated by the RA function of the PMA, shall be meaningful, and shall never be reassigned to another entity.

The CA are identified in the Issuer's name field of the subscriber certificates as follows.

3.1.1.1 ECAC's S/MIME CA

The DN format allowed for the ECAC S/MIME is:

S/MIME CA certificate

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

Table 1 – ECAC S/MIME CA Distinguished Name

3.1.1.2 Subscriber certificates

The tables below specify the DN structures followed for each certificate types supported.

Sponsor-validated S/MIME certificates for natural persons

Attribute	Value
Country – "C"	PK
O	organization's legal name
OrganizationIdentifier	Registration Reference[2] for a Legal Entity assigned in accordance with the identified Registration Scheme
GivenName	Individual's authenticated given name
SurName	Individual's authenticated surname
SERIALNUMBER	It contains an identifier[3] assigned by the CA or RA to identify and/or to disambiguate the Subscriber.

[2] Must be GOVPK. If the Government Entity is verified at a subdivision (state or province) level, then it must be ''GOVPK+ an ISO 3166-2 identifier for the subdivision (up to three alphanumeric characters)''

[3] Such as Passeport number, National ID card number, Tax reference number or national civic registration number.

3.1.1.3 OCSP certificates

S/MIME CA OCSP

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

3.1.2 Need for Names to be Meaningful

S/MIME Certificates include a non-null Subject DN containing the verified information of the entity that sponsored the Certificate issuance and the name of the individual. The rfc822Name (subjectAltName) includes the email address controlled by the individual requesting the S/MIME Certificate.

For OCSP certificates: name is meaningful since it indicates the Subordinate CA OCSP name.

3.1.3 Anonymity or Pseudonymity of Subscribers

This CPS does not permit 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

As per section 3.1.1 of this CPS, this CA enforces uniqueness through the combination of the individual's name and sponsor organization's name.

Additionally, uniqueness is enforced through the use of certificate serial numbers, which are included in end-entity certificates. These serial numbers are assigned in such a way that they are guaranteed to be unique.

For the OCSP certificates: The OCSP responder unique name is included in the subject DN of issued OCSP certificate at each issuing CA level.

3.1.6 Recognition, Authentication, and Role of Trademarks

Applicants agree by submitting a certificate request to the Subordinate CA that their request does not contain data which in any way interferes with or infringes upon the rights of any third parties in any jurisdiction with respect to trademarks, service marks, trade names, company names, "doing business as" (DBA) names, or any other intellectual property right, and that they are not presenting the data for any unlawful purpose whatsoever.

The PMA has the right to revoke a certificate or certificates containing a disputed subject name, as well as upon receipt of a properly authenticated order from a court of competent jurisdiction that mandates the revocation.

3.2 Initial Identity Validation

The following methods described in this Section are used to ascertain the identity of a Subscriber.

3.2.1 Method to Prove Possession of Private Key

The Applicant provides a digitally signed PKCS#10 CSR to establish that it holds the private key corresponding to the public key to be included in the certificate. The RA systems enforce validation of the proof of possession of the private key as part of the certificate request processing. The proof of possession is submitted to the RA through CSRs in PKCS#10 format.

3.2.2 Authentication of Organization Identity

3.2.2.1 Organization Identity

The authentication of an organization's identity is conducted in compliance with current Pakistan legislation through the following validation processes. An RA (Registration Authority) officer performs the initial identity validation of the organization and its representatives and enrolls the organization in the WebRA portal.

The organization’s identity is verified using reliable and authoritative data sources, expected to provide detailed information about the entity, including its legal name, address, and information about its authorized representatives.

To verify the identity of a government entity, the RA officer relies on the “Official Government Gateway” or other direct communication methods with the jurisdiction or authority responsible for the entity's legal creation, existence, or recognition. For the organization's authorized representative, verification can be established through either the organization's official records or an approved formal communication between the RA officer and the government entity's HR department.

The RA officer may also request the applicant to provide official documentation to confirm the entity's identity, such as a corporate charter, government-issued tax document, professional letter (e.g., from an accountant or legal counsel), or other relevant documents. A site visit may also be conducted to verify the organization’s address.

Additionally, the RA officer ensures the validation of the applicant’s right to use domain names (e.g., the domain portion of an email address) listed in the certificate, following the procedures specified in Section 3.2.3.

To maintain compliance, the RA officer ensures that any obtained validation data—such as authority over the mailbox via domain verification—is revalidated within 398 days of the last verification.

Finally, the RA officer confirms the association between the applicant and the certificate subject by ensuring that the information provided in the application form exactly matches the details to be inserted into the certificate.

.

The authority of the person requesting the certificate is verified in accordance with section 3.2.6.

3.2.2.2 Authentication for organizations applying to operate a Local registration authority (LRA)

This scenario applies to organizations wishing to issue and manage natural person certificates. The organization and its authorized representative are verified in accordance with the process described above (section 3.2.2.1) then the authorized representative signs the LRA agreement. Upon organization's enrolment approval, the RA initiates an internal process whereby the organization and its LRAO officers are created on the web RA portal so that they can use their web RA account to perform certificate requests and other certificate management operations.

3.2.3 Validation of Mailbox Authorization or Control

Prior to issuing an S/MIME Certificate, the RA officer verifies the Applicant controls the email accounts associated with all Mailbox fields referenced in the certificate by confirming:

- Validating authority over mailbox via domain: The Domain Name contained in the domain portion of the email address is owned or controlled by the Legal Entity in the Organization field using the approved methods in Section 3.2.2.4 of the ECAC TLS CA CPS. The RA must refer to the internal RA processes document for more details.

3.2.4 Authentication of Individual Identity

3.2.4.1 Authentication for Individuals Applying for Natural Person certificates

This section describes the process followed by an LRAO for verifying the identity of the natural persons as part of the certificate enrolment processes.

The LRAO relies on Authoritative and Supplementary evidence to perform identity verification. The types of supported evidence are listed below:

- **Authoritative Evidence**: Primary evidence are defined as governmental authoritative sources including secure photo ID evidence, issued with robust identity proofing, issuance and management processes. Examples of Primary evidences are: passports, (electronic) citizen identity cards, (electronic) resident identity cards, (international) driving license, civil servant cards, police forces identification / Military cards.
- **Supplementary Evidence**: Supplementary evidence is evidence used as support for the authoritative evidence (i.e. trusted registers, proof of access in particular a bank account, official document and attestations). Examples are: Human Resource (HR) attestation letters,

The identity verification process is conducted by the LRAO through an in-person meeting with the individual or an equivalent method and includes the following steps:

a) The LRAO obtains the following individual's identity proofing Supplementary evidence from the entity HR as part of employee induction, from a direct line of business manager or from the individual himself:

- A completed and signed certificate application form.
- An attestation Letter confirming the affiliation of the individual to the entity and providing details such that full name and date of birth, email address.
- An email from entity representative to enrol the individual into the Web RA to enable it to benefit from an S/MIME certificate (as per the business need).

b) The LRAO validates the identity proofing documents through a documented internal process.

c) The LRAO verifies the link between the claimed identity and the applicant as outlined in a documented internal process.

Upon the initial approval of the individual identity, the LRA initiates a technical procedure through which the individual is enrolled into the Web RA portal with multi-factor authentication credentials that he can use to execute certificate requests and related certificate management operations.

3.2.5 Non-verified Subscriber Information

All fields constituting the subscriber information written in the certificate are verified by the LRAO.

3.2.6 Validation of Authority

The RA verifies the authority of the entity official representative as the signatory of the entity registration form and the LRA agreement. The RA also verifies the authority of the LRAO as the person authorized to submit application requests and other certificate managements operations. Refer to sections 3.2.2.2 for further details.

3.2.7 Criteria for Interoperation

No Stipulation.

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 initial registration, in addition to the below rules:

- The LRAO officer checks the existence and validity of the certificate to be re-keyed and that the information used to verify the identity and attributes of the subject is still valid.
- If any of the terms and conditions have changed, these will be communicated by the LRAO to the subscriber.

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.

3.4 Identification and Authentication for Revocation Request

The ECAC RA officer / LRAO authenticates the revocation request through one of the following methods:

- Receiving a revocation request from a pre-agreed and a concerned department with the entity (e.g., HR, direct manager of the individual) if the subscriber is terminated or changed role within the entity which would trigger the revocation request. The LRAO would have the internal means to confirm the validity of the revocation request.
- Receiving a revocation request from the subscriber through agreed channels, this may include:
    - A face-to-face visit to the LRAO office, telephone call from the subscriber where the LRAO asks an identity validation questions (e.g., employee ID, name, date of birth etc.),
    - An email from the subscriber using an email address that can be verified by the RA officer / LRAO
    - through the web RA portal (user account).

For OCSP responder certificate: The present CPS does not specify detailed provisions for revoking any of these certificates. Such revocation may be triggered by a compromise or suspected compromise of the related private keys which is considered as a disaster and treated as such in conformance with the disaster recovery and business continuity plan.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Certificate applications can be initiated directly by the applicants themselves through the Web RA portal. The LRAO is authorized to approve and submit the certificate applications. The applicant is responsible for the authenticity of all data submitted as part of the certificate applications. The LRAO ensures subscriber's agreements are ratified by the applicant as part of the certificate request process. The LRAO maintains a blacklist of individuals affiliated to the entity for whom certificate requests will not be accepted.

When the applicant is the LRAO himself, only an another LRAO (i.e., someone other than the LRAO identified as the applicant) is authorized to approve and submit the certificate applications.

For OCSP responder certificate: The RA and an authorized PKI administrator in trusted role oversee the execution of authorized internal operational ceremonies through which OCSP certificates for the S/MIME CA are issued

4.1.2 Enrollment Process and Responsibilities

The process is described as following:

- The individual is registered into the Web RA portal.
- The individual authenticates to the Web RA portal (using multi-factor authentication).
- The individual completes a certificate request form.
- A technical process is executed that results in the personalization of the token key pair and CSR generation.
- The individual ratifies the subscriber agreement and submits the certificate request application to the LRAO.
- The LRAO is authorized to review and approve the certificate applications. He logs into his Web RA portal and execute the technical steps to verify, approve and submit the certificate request.
- The LRAO maintains a blacklist of individuals affiliated to the entity for whom certificate request will not be accepted.

For OCSP responder certificate: The ECAC RA and an authorized PKI administrator in trusted role oversee the execution of an operational ceremonies through which these certificates can be issued. The PMA approves the operational ceremony documentation and validates the embedded certificate template and naming conventions against the provisions of this CPS. The PMA authorizes then the ceremony and confirms the list of involved trusted role staff.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The LRAO identifies the Subscriber based on the identifying documents and evidence that the Subscriber presents, In summary:

a) The LRAO ensures a unique ID is assigned to each certificate application record,

b) The LRAO records all activities (e-mail communication, phone calls, vetting evidence) along with the certificate application record,

c) Any malicious certificate or revocation request or a request that fails multiple (more than 3) times is added to a blacklist, the blacklist includes the necessary details to avoid ambiguously in identifying future malicious requests,

d) The LRAO conduct a blacklist check against his RA's own blacklist. If the applicant is in the blacklist, the certification application is rejected,

e) The applicant signs or ratifies a dedicated subscriber agreement.

f) The LRAO identifies the individual as described in section 3.2.4;

g) The LRAO validates the individual's eligibility for the requested certificate according to the entity's internal processes (e.g., performing this validation through a communication with the individual's direct manager);

h) The LRAO proceeds with the technical procedures related to issuing the requested certificate.

Age of Validated Data

The LRAO may reuse completed validations and/or supporting evidence performed in accordance with Section 3.2 within the following limits:

- **Validation authority over mailbox via domain:** 398 days prior to issuing the Certificate.
- **Authentication of organization identity:** 825 days prior to issuing certificate.
- **Authentication of individual identity:** 825 days prior to issuing certificate.

A prior validation is not reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate

4.2.2 Approval or Rejection of Certificate Applications

The LRAO officer approval of the certificate application is subject to:

- Successful identification and authentication of all required Subscriber information according to Section 3.2.4

The LRAO officer rejects a certificate application if:

- Identification and authentication of all required Subscriber information according to Section 3.2.4 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request.

For OCSP responder certificate: The ECAC RA and an authorized PKI administrator in trusted role oversee the execution of an operational ceremonies through which these certificates can be issued. The PMA approves the operational ceremony documentation and validates the embedded certificate template and naming conventions against the provisions of this CPS. The PMA authorizes then the ceremony and confirms the list of involved trusted role staff.

4.2.2.1 Certification authority authorization (CAA)

Prior to issuing an S/MIME certificate, the RA officer check the DNS for the existence of a CAA record in accordance with RFC 9495 for each Mailbox Address in the subjectAltName extension of the S/MIME certificate to be issued. ECAC processes the “issuemail” property tag. ECAC's CAA issuer domain is " ecac.pki.gov.pk.".

Certificates passing the CAA check are issued within the Time to Live (TTL) of the CAA record, or 8 hours, whichever is greater. ECAC RA does not use iodef property tag of the CAA record for communicating with the contact(s) stipulated in the CAA iodef record(s).

The RA officer logs all actions related to CAA record checks and processing. Additionally, the RA officer documents any potential certificate issuances that were prevented due to a CAA record, providing sufficient detail to enable feedback to the CA/Browser Forum on the circumstances.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Certificate issuance by the CA requires the LRAO to perform the required verification/vetting steps as per section 4.2.1of this CPS and execute the technical steps and direct commands for submitting the Certificate Signing Request (CSR) to the CA.

The CA validates the format and structure of the request then generates the certificate in accordance with the configured certificate template. The certificate then is made available for download from the web RA portal. The CA issues the certificate in “Active” state.

For OCSP responder certificate: The issuance and management of these certificates happen as part of operational ceremonies that are approved by at least two members of the PMA to establish: (1) authorizing the ceremony execution, (2) approving the list of ceremony attendees involving the ECAC RA, a member of PKI operations management, and designated administrators from the PKI operations team, (3) validating embedded certificate templates and naming conventions against the provisions of this CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The subscriber is notified by email that his certificate has been generated. The certificate is made available for download on his Web RA portal account

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The subscriber downloads the certificate from the web RA portal then validates its content. In case of any discrepancies, the subscriber initiates a discussion with the LRAO which may lead to certificate revocation to issue a corrected certificate.

The certificate is deemed accepted if no complaints are raised by the subscriber to the LRAO within 5 business days of receiving the email notification of certificate generation.

For OCSP responder certificate: A certificate is deployed on the target system as part of the overall authorized internal operational ceremony.

4.4.2 Publication of the Certificate by the CA

The CA does not publish end-user certificates apart from sharing it with the Subscriber.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The subscribers adhere to the following obligations:

- Provide correct and up-to-date information to the LRAO as part of his application,
- Not tampering with a certificate,
- Only using certificates for legal and authorized purposes in accordance with the common general requirements applicable to the TSP CP and this CPS,
- Protect the private key (and related secrets) from compromise, loss, disclosure, or otherwise from unauthorized use of their private key,
- Notify the LRAO immediately if any details in the certificate become invalid, or because of any compromise, loss, disclosure, or otherwise unauthorized use,
- Not using the certificate outside its validity period, or after it has been revoked.
- No longer use the private key after the validity period of the certificate expires, or when a certificate has been revoked.

Refer to section 9.6.3 of this CPS for complementary details.

4.5.2 Relying Party Public Key and Certificate Usage

A party relying on a certificate issued by these Subordinate CAs:

- Uses software that is compliant with X.509 and applicable IETF PKIX standards to validate the certificate signature and validity period,
- Validates the certificate by using the CRL, or the OCSP validity status information service in accordance with the certificate path validation procedure,
- Trusts the certificate only if it has not been revoked and is within the validity period,

- Trusts the certificate only for its intended purpose and in accordance with this CPS.

4.6 Certificate Renewal

Certificate Renewal is the act of issuing a new certificate with a new validity period while the identifying information and the public key from the old certificate are duplicated in the new certificate. Certificate renewal is not supported by the Subordinate 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 refers to the issuance of a new certificate with a new subject public key for a subject to whom a certificate has previously been issued by the CA. Subject attributes and other certified attributes can be updated.

4.7.1 Circumstance for Certificate Re-Key

Certificate re-key may happen while the certificate is still active, after it has expired, or after a revocation. The re-key operation may invalidate any existing active S/MIME certificates.

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 CA 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 wants 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

ECAC provides a continuous ability for subscribers to submit certificate requests. This is available through an online system that is accessible 24 x 7 to authenticated subscribers. Certificate suspension is prohibited. Only permanent certificate revocation is permitted.

The revocation of subscribers' certificates is handled as per the below subsections.

4.9.1 Circumstances for Revocation

4.9.1.1 Circumstances for Subscriber certificates revocation

The RA /LRAO revokes a Certificate within 24 hours if one or more of the following occurs:

1. Received a written request from the Subscriber,
2. The RA /LRAO is notified that the original Certificate Request was not authorized and does not retroactively grant authorization.
3. The RA /LRAO obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise.
4. the RA /LRAO is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys) ;
5. The RA obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address in the Certificate is not relied upon.

The RA /LRAO revokes a Certificate within 24 hours if one or more of the following occurs:

6. The Certificate no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
7. The RA /LRAO obtains evidence that the Certificate was misused;
8. The RA /LRAO is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
9. The RA /LRAO is made aware of any circumstance indicating that use of an email address or Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g., a court or arbitrator has revoked the right to use an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);
10. The RA /LRAO is made aware of a material change in the information contained in the Certificate.
11. The RA /LRAO is made aware that the Certificate was not issued in accordance with this CPS.
12. The RA /LRAO determines or is made aware that any of the information appearing in the Certificate is inaccurate.
13. ECAC's right to issue Certificates under the baseline requirements expires or is revoked or terminated, unless ECAC has planned to continue maintaining the CRL/OCSP Repository
14. Revocation is required by the CPS; or

15. The RA /LRAO is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.1.2 Circumstances for Subordinate CA revocation

CA Certificates will be revoked within seven (7) days if one or more of the following occurred:

1. The revocation is requested in writing;
2. The CA notifies the Issuing CA (i.e., Root CA) that the original certificate request was not authorized and does not retroactively grant authorization;
3. ECAC obtains evidence that the CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
4. ECAC (i.e., Root CA) obtains evidence that the CA Certificates was misused;
5. ECAC (i.e., Root CA) is made aware that the CA Certificates was not issued in accordance with or that CA has not complied with this document.
6. ECAC (i.e., Root CA) determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. CAs ' right to issue Certificates under these Requirements expires or is revoked or terminated, unless the (i.e., Root CA) has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the ECAC's Certificate Policy and/or Certification Practice Statement.

4.9.2 Who Can Request Revocation

Revocation can be requested by the following:

- The RA /LRAO in the cases described in section 4.9.1,
- The Subscriber may submit a revocation request for his own certificate,
- Any relying party or application software supplier possessing evidence of compromise of the subscriber's certificate or its usage to promote malware,
- ECAC at its own discretion (if for instance a compromise is known for the CA key),
- Subscribers, relying parties, application software suppliers, and other third parties may submit Certificate Problem Reports to notify ECAC of a suspected reasonable cause to initiate the certificate revocation process.

Only authorized revocation requests are accepted.

4.9.3 Procedure for Revocation Request

Revocation directly by a Subscriber or a Requester:

The subscriber may submit a revocation request through the Web RA portal. Such requests will be processed automatically by the relevant CA that issues a new CRL.

Revocation through a RA /LRAO is conducted as follows:

- The RA /LRAO authenticates the revocation request and validates the identity of the subscriber as described in section 3.4.
- The RA/LRAO executes the certificate revocation.
- The CA revokes the certificate, and the certificate status is updated[4].
- The RA /LRAO notifies via internal communication the concerned departments (e.g. HR, direct line of business) about the completion of the certificate revocation operation;
- If applicable, the RA /LRAO updates its internal blacklist with the details of the subscriber.

Certificate Revocation handling by the RA officer following a Certificate problems reporting:

ECAC maintains a continuous 24/7 ability to internally respond to any high priority revocation requests and certificate problem reports provides instructions for certificate revocation and certificate problem reporting on a dedicated page in its public repository, accessible at https://ecac.pki.gov.pk/repository/Certificate_Problem_Report.html

Subscribers, relying parties, application software suppliers, and other third parties may submit certificate problem reports via ecac.certification.problem@pki.gov.pk

For any certificate problem report, the reporter is requested to include his contact details, suspected abuse and related Subject.

The RA officer begins the investigation of a certificate problem report within 24 hours of receipt and decide whether revocation or other appropriate actions are required based at least on the following criteria:

- The nature of the alleged problem,
- The number of Certificate Problem Reports received about a particular Certificate or Subject,
- The entity making the report (for example, a notification from an Anti-Malware Organization or law enforcement agency carries more weight than an anonymous complaint),
- Relevant local legislation.

In case of deciding that a certificate is going to be revoked because of the certificate problem report, the RA officer executes the revocation procedure as specified earlier in this section.

If ECAC deems appropriate, it may forward the revocation reports to law enforcement.

[4] The new certificate status will appear in the next CRL, while the OCSP responder will immediately make this new certificate status information available to relying party applications.

4.9.4 Revocation Request Grace Period

There is no revocation grace period. Revocation requests are processed timely after a decision for revocation is made and in all circumstances within the timeframes listed under section 4.9.1 of this CPS.

4.9.5 Time Within Which CA Must Process the Revocation Request

Certificate revocation requests are processed within 24 hours.

For certificate problem reports, RA officer begins investigations within 24 hours from receiving the report. RA officer initiates communication with the Subscriber and where appropriate, with other concerned authorities (e.g. law enforcement). A preliminary communication on the certificate problem is sent to the Subscriber and to the originator of the problem report.

The RA officer performs further investigations involving the PMA, the subscriber and other relevant authorities (e.g. law enforcement) 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, RA officer may agree with subscriber on a plan to issue a new certificate.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties are solely responsible for performing revocation checking on all Certificates in the chain before deciding whether to rely on the information in a Certificate. The CA provides revocation status via mechanisms that are embedded in the Certificate i.e. CRL and OCSP.

4.9.7 CRL Issuance Frequency (If Applicable)

CRLs is issued as per Section 2.3 of this CPS.

4.9.8 Maximum Latency for CRLs (if applicable)

CRLs are issued timely by the CA as per the CRL issuance frequency listed in section 4.9.7 of this CPS .

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 responder avails information immediately to relying party applications based on the CA actions on issued certificates.

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

4.9.10 On-Line Revocation Checking Requirements

The OCSP responder supports both HTTP GET and HTTP POST methods.

For the status of Subscriber Certificates:

- OCSP responses have a validity interval greater than or equal to eight hours;
- OCSP responses have a validity interval less than or equal to ten days;
- For OCSP responses with validity intervals less than sixteen hours, then Subordinate CAs update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.
- For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

A certificate serial number within an OCSP request is one of the following three options:

1. "assigned" if a certificate with that serial number has been issued by the CA, using any current or previous key associated with that CA subject; or
2. "reserved" if a Precertificate [RFC6962] with that serial number has been issued by:
    a. the CA; or
    b. a Precertificate Signing Certificate [RFC6962] associated with the CA; or
3. "unused" if neither of the previous conditions are met.

If the OCSP responder receives a request for the status of a certificate serial number that is "unused" (i.e., not issued by these CA) then the OCSP responder responds with a "revoked" status as defined by RFC 6960 (section 4.4.8. Extended Revoked Definition).

The ECAC operations team monitors the OCSP responder 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

The CA only use OCSP and CRL as methods for publishing certificate revocation information.

4.9.12 Special Requirements Re Key Compromise

If ECAC discovers, or has a reason to believe, that there has been a compromise of the private key of the CA, it will immediately declare a disaster and invoke its business continuity plan. ECAC will also:

- determine the scope of certificates that must be revoked,
- revoke impacted certificates within 24 hours and publish online CRLs within 30 minutes of creation,
- use reasonable efforts to notify government entities, subscribers and potential relying parties that there has been a key compromise, and
- generate new CA key pair as per the operational policies and procedures.

Relaying Parties may advise ECAC of a private key compromise using one of the following methods:

- Submission of a signed CSR, Private Key or other challenge response signed by the Private Key and verifiable by the Public Key, or
- The private key itself.

4.9.13 Circumstances for Suspension

Not Applicable.

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

Refer to section 4.9.6 of this CPS. In addition, the following provisions have been made

4.10.1 Operational Characteristics

The CA publishes its CRLs at the public repository accessible to relying parties.

The CA's OCSP responder exposes an HTTP interface that is also publicly available to relying parties.
Revocation entries in a CRL or OCSP response remains until after the revoked certificate's Expiry Date.

4.10.2 Service Availability

The public repository where certificate information and CRLs are published is accessible 24 hours a day and 7 days a week and guarantees an uptime for at least 99.6% over one year period.

The CA operate and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The CA maintain a 24X7 ability to respond internally to high-priority certificate problem reports as described in section 4.9.3 of the present document. When appropriate, they forward such complaints to law enforcement authorities and/or revoke the Certificate that is the subject of the complaint.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Subscription period is linked to the certificate validity period. The subscription ends when the certificate is expired or revok.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow is not supported by the CA.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not Applicable.

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 CA 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.

5.1 Physical Security Controls

The ECAC PMA ensures that appropriate physical controls are implemented at the CA hosting facilities. Such controls are documented as part of the ECAC's internal policies that are enforced and verified through internal audits performed monthly by the 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

The CA systems are protected by multi-tiered (five tiers) physical security measures, with access to the lower tiers only possible by first gaining access through the higher tiers. Sensitive CA operational activities related to certificate lifecycle management occur within very restrictive physical tiers. The access control system implemented record the passage of people through each zone (i.e., tier)

Physical security controls include security guard-monitored building access, biometric authentication, and CCTV monitoring, protect the CA systems from unauthorized access, these controls are monitored on a 24x7x365 basis, forming multiple layers of protection for individuals entering and exiting the premises.

Access to the premises is granted upon presentation of the individual's National Citizens ID document, which is verified by the security guard, this includes monitoring and

registering pertinent information including the person's identity, time of arrival and departure, and provides a visitor badge. Entry is not allowed unless the persons have been duly authorized by a member of the PMA, and must be escorted by one from ECAC's trusted employees.

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.

5.1.3 Power And Air Conditioning

The design of the facility hosting the ECAC CA 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 Subordinate CAs hosting facility. These include installing the ECAC CA equipment on anti-static floors with moisture detectors.

5.1.5 Fire Prevention and Protection

The ECAC CA 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 Subordinate 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 CA :

- **PKI Administrator**: Owning the credentials of the CA software. Responsible for configuring and maintaining the CA.
- **PKI Operator:** Authorized to execute the CA operational cycle and is involved in critical operations such as subscribers' certification operations.
- **Security Officer:** Owning credentials that enable configuring the HSMs and PKI policies on the target systems subject to key generation during relevant key ceremony.
- **RA Officer:** Authorized to conduct the vetting of the certificate requests as part of the certification request processing.
- **M-of-N Custodians:** Owners of the HSM activation data. Custodians of the CAs' safes.
- **CA Domain Owner:** Owning the credential that authorizes CA HSM backup and restore operations.
- **HSM Auditor:** Owning the credentials for retrieving the HSM audit logs.
- **System Administrator:** Authorized to install, configure, troubleshoot, and maintain the supporting operating system and database environment.
- **Network Administrator:** Authorized to install, configure, troubleshoot, and maintain the supporting network equipment.
- **Compliance officer:** Authorized to collect and review the audit logs generated by the CAs' systems and regular internal compliance audits.
- **Data Center Custodians:** Personnel who has the credentials for opening the PKI datacenter while performing the CAs operations.

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
- 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

Individual CA personnel are specifically assigned to the roles defined in Section 5.2.1 above. Roles requiring a separation of duties include:

- Those performing approval of the issuance of Certificates. (RA officers)
- Those performing installation, configuration, and maintenance of the CAs systems. (System and Network Administrators)
- Those with overall responsibility for administering the implementation of the CAs' security practices. (Security Officers)
- Those performing duties related to cryptographic key life cycle management (key custodians).
- Those performing CA systems auditing (Compliance officers) .

5.3 Pesonnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Prior to engagement of an 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 provides essential technical training for its personnel to effectively carry out their duties. This training is regularly updated and conducted annually for the CAs personnel.

The training program encompasses a diverse range of topics and is delivered by a combination of experienced CAs staff and third-party experts specializing in security and PKI. It is meticulously designed to cater to the specific requirements of various trusted roles involved in managing and delivering CAs services. The topics covered in the training are:

- PKI theory and principles
- PKI environmental controls and security policies
- PKI RA processes including vetting and verification procedures.
- PKI operational processes
- PKI products hands-on training
- PKI trusted roles management
- PKI disaster recovery and business continuity procedures

The PMA maintains comprehensive documentation of all personnel who have undergone training and regularly assesses the satisfaction levels of the trainers. At the end of each training session, examination tests are organized, and certificates are awarded to staff who pass these tests. It is mandatory for all trusted roles, including RA officers, to pass these examinations before being authorized to operate as trusted role.

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 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 covers 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 security officer team and are also subject to review as part of the regular internal audits performed by the ECAC PMA compliance function on the CAs operations.

5.4.1 Types of Events Recorded

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

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

1. CAs certificates and key life cycle events, including:
    1. Key generation, backup, storage, recovery, archival and destruction;
    2. Cryptographic device life-cycle management events.
    3. Certificate requests, renewal, and re-key requests, and revocation;
    4. Approval and rejection of Certificate requests;
    5. Generation of CRLs;
    6. Signing of OCSP responses; and
    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate life-cycle management events, including:
    1. Certificate requests, renewal, and re-key requests, and revocation;
    2. All verification activities stipulated in this CPS (e.g. date, time, calls, persons communicated with);
    3. Approval and rejection of certificate requests;
    4. Issuance of certificates.
3. Security events, including:
    1. Successful and unsuccessful PKI system access attempts;
    2. PKI and security system actions performed;
    3. Relevant router and firewall activities (as described in Section 5.4.1.1); and
    4. Security profile changes;
    5. System platform issues (e.g. crashes), hardware failures, and other anomalies
    6. Entries to and exits from the CA facility.
    7. Installation, update and removal of software on a Certificate System;

The PMA also ensures that the following information, not produced by these CA, is maintained (either electronically or manually) by the operations team:

1. CA personnel, security profiles rotations/changes.
2. All versions of this CPS.
3. Minutes of meetings.
4. Compliance internal audit reports.
5. Current and previous versions of Subordinate CAs configuration and operations manuals.

5.4.1.1 Router and firewall activities logs

Router and firewall activities logged include:

1. Successful and unsuccessful login attempts to routers and firewalls; and

2. Logging of all administrative actions performed on routers and firewalls, including configuration changes, firmware updates, and access control modifications; and

3. Logging of all changes made to firewall rules, including additions, modifications, and deletions; and

4. Logging of all system events and errors, including hardware failures, software crashes, and system restarts.

5.4.2 Frequency of Processing Log

The 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 PMA:

- Audit and Security of the online CA systems (Ex. OCSP responder) are reviewed by the Security Officer's 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 PKI systems are reviewed by the Security Officer's team on quarterly basis to validate the physical and logical access policies,
- The PMA audit and compliance function executes an internal audit on the CA operations on yearly basis. Samples of the log review reports and collected audit logs since the last audit cycle is requested by the 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 CA retains the following, for at least two (2) years:

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1(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,
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1(2)) after the revocation or expiration of the Subscriber Certificate,
3. Any security event records (as set forth in Section 5.4.1(3)) 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 CA 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 CA 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 CA operations personnel.

5.4.5 Audit Log Backup Procedures

Incremental backups and full backups are performed periodically. Additionally, the following rules apply for the backup of the CA audit log:

- Backup media are stored locally in the ECAC 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 CA 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 CA systems and infrastructure shall be also subject to regular security assessments as follows:

- Within one (1) week of receiving a request from the CA/Browser Forum,
- After any system or network changes that the CA determines are significant, and
- at least every three (3) months, on public and private IP addresses identified of CA core and supporting PKI system. This regular self-assessment activity is executed by security personnel part of the CA operations team.
- On an annual basis, and after infrastructure or application upgrades or modifications that the CA determines are significant, the ECAC PMA coordinates a third-party independent vulnerability assessment and penetration testing is conducted on the CA 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.

ECAC CA personnel record evidence that each Vulnerability Scan and Penetration Test is performed by individuals or entities possessing the necessary skills, tools, proficiency, adherence to a code of ethics, and independence to ensure reliable results, with all evidence of the execution of these activities being collected and archived by the relevant CA personnel.

5.5 Records Archival

5.5.1 Types of Records Archived

The CA 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 specified in Section 5.5.1, are retained for a period of at least two (2) years and up to seven (7) years. This retention ensures that records are available for investigating potential security incidents or other events requiring retrospection and examination of past activities

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

1. All archived documentation related to the security of CA Systems (as set forth in Section 5.5.1),
2. 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:
    1. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates, or
    2. 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 CA. The CA 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 CA systems is synchronized with the time source of a GPS clock. The time-stamping services setup reaches an accuracy of the time of +/-1s or better with respect to UTC.

Further, the CA operations team enforces a procedure that checks and corrects any clock drift.

5.5.6 Archive Collection System (Internal or External)

The CA 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 the archived material. The CA operations team use the CA 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 CAs' key shall be changed with a frequency that ensures the CA shall have a validity period greater than the maximum lifetime of CA's certificates.

Refer to Section 6.3.2 of this CPS document for key changeover frequency.

The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in chapter 6.1.4.

To support revocation management of issued certificates, the old CA private keys are maintained until all the Certificates signed with the Private Key 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 CA 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 implements the necessary measures to ensure full recovery of the 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 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 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

For Subscribers key compromise, see section 4.9.

Compromise of the CA 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 CA 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 disaster recovery location are made possible considering the CA 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:

- The conditions for activating the plan,
- Emergency procedures,
- Fallback procedures,
- Resumption procedures,
- A maintenance schedule for the plan;
- Awareness and education requirements;
- The responsibilities of the individuals;
- Recovery time objective (RTO);
- Regular testing of contingency plans.
- The CAs' plan to maintain or restore the CAs' business operations in a timely manner following interruption to or failure of critical business processes
- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
- What constitutes an acceptable system outage and recovery time
- How frequently backup copies of essential business information and software are taken;
- The distance of recovery facilities to the main site; and
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either ate the original or a remote site.

5.8 CA or RA Termination

If the PMA determine that termination of the CA services is deemed necessary, the PMA execute its termination plan that has been approved. The termination plan must at minimum:

- Ensure that any disruption caused by the termination of the CA is minimized as much as possible
- Ensure proper arrangements for the retention of archived logs, as specified in Section 5.5

- Ensure proper arrangements for maintaining the validation status service URLs specified in certificates that remain valid for the applicable period after termination,
- Ensure prompt notification of termination is provided to Subscribers, Authorized Relying Parties, Application Software Providers and other relevant stakeholders. This notification should be published in daily newspapers or communicated through other mediums and methods as determined by the PMA
- Where applicable, ensure communication with relevant parties and facilitate the transfer of archived CAs' records to an appropriate custodian
- Ensure the development and execution of a plan to assist, as much as possible, Subordinate CAs' subscribers in transitioning to another TSP,
- ensure that a process for revoking all Digital Certificates issued by the Subordinate CAs at the time of termination is maintained.

6 Technical Security Controls

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

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 ECAC's Subordinate CA

The ECAC PMA plans and supervises the execution of the key generation ceremonies of the CA. 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 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 a 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
- A video of the entire key generation ceremony will be recorded and stored securely for audit purposes

6.1.1.2 Subscriber's Key Pair Generation

The subscriber keys are generated according to the below requirements:

S/MIME certificates generated on cryptographic token: Subscribers' key pairs generated within the memory of hardware cryptographic devices conforming to FIPS 140 Level 2 and that prevents exportation. Key pairs shall be generated using key generation algorithm and key sizes as specified under sections 6.1.5 and 6.1.6 of this CPS.

The CA reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in 6.1.5 and/or 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. The CA are aware of a demonstrated or proven method that exposes the Private Key to compromise.
4. The CAs has previously been made aware that the Subscriber's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;
5. The CA is aware of a demonstrated or proven method to easily compute the Private Key based on the Public Key in the certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

6.1.2 Private Key Delivery to Subscriber

Not Applicable.

6.1.3 Public Key Delivery to Certificate Issuer

This CA accepts CSRs (i.e., commands for certificate generation) only if these requests have been authenticated in the web RA portal .

6.1.4 CA Public Key Delivery to Relying Parties

The CA public key certificates are published on the ECAC public repository.

6.1.5 Key Sizes

The CA's keys size are 4096-bit RSA.

Subscriber keys are 2048-bit RSA or 4096-bit RSA (recommended).

6.1.6 Public Key Parameters Generation and Quality Checking

6.1.6.1 Subordinate CA

The Subordinate CA private and public keys generation is done with state-of-the-art parameter generation. The CA HSMs and associated software meet FIPS 186 requirements for random generation and primality checks. The ECAC PKI operations team references the Baseline Requirements Section 6.1.6 on quality checking.

6.1.6.2 Subscribers

The LRAO officer use reasonable techniques to validate the suitability of public keys presented by Subscribers. Known weak keys are tested for and rejected as described in the CA/B Forum Baseline Requirements section 6.1.6.

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

Certificates issued by the CA contain a key usage bit string in accordance with [RFC 5280]. Refer to section 7.1 and 7.3 of this CPS .

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 CA 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 Subordinate CAs hosting facility.

For the Subscribers' private keys, the provision stipulated in 6.1.1.2 applies.

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

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

CA 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 CA 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 CA 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

Not applicable.

6.2.4 Private Key Backup

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

Backup operations are executed as part of the CA key generation ceremonies. The ECAC CA 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 CA 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 CA key ceremony procedure. Dedicated personnel in trusted roles participate in the transport operation, which is escorted by security guards. Provisions stipulated in Section 6.2.2 are also considered during the transportation.

6.2.5 Private Key Archival

Not Applicable.

6.2.6 Private Key Transfer into or from a Cryptographic Module

The CA 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 CA 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

6.2.8.1 Subordinate CA

Private keys is activated following the principles of dual control and split knowledge. The activation procedure uses a PIN entry device attached to the CA's HSMs.

6.2.8.2 Subscribers

Subscribers are responsible for activating and protecting the access to their key pair in accordance with the obligations that are presented in the form of a Subscriber Agreement.

Subscribers plug in their PKI hardware token to the appropriate reader or slot and when asked they provide the PIN associated with the PKI hardware token to activate their private key.

6.2.9 Method of Deactivating Private Key

6.2.9.1 Subordinate CA

ECAC deactivates CA Private Keys in accordance with the instructions and documentation provided by the manufacturer of the hardware security module.

6.2.9.2 Subscribers

Subscribers are responsible for deactivating and protecting the access to their key pair in accordance with the obligations that are presented in the form of a Subscriber Agreement.

6.2.10 Method of Destroying Private Key

6.2.10.1 Subordinate CA

Destroying the CAs private key outside the context of the end of its lifetime applies to investigation and special authorization from the PMA. This destruction decision includes the assignment of the personnel.

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

6.2.10.2 Subscribers

Subscribers are responsible for the destruction of their keys in accordance with the obligations that are presented in the form of a Subscriber Agreement.

The subscribers can delete their keys and certificates using the appropriate vendor's provided software.

6.2.11 Cryptographic Module Rating

The CA's cryptographic modules are certified/validated against [FIPS 140-2] Level 3.

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 Subordinate CA's certificates are valid for six (6) years, with a key usage period of three (3) years.
The maximum permitted duration of validity for Subscriber's certificates is defined in section 7.1.

The CA private key is not used after the validity period of the associated public key certificate. Additionally, it is not used to sign end-entity certificates after the private key usage period, except for CRLs and OCSP responder certificates for the certificate validity status service.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 Subordinate CA

The CA's 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 CPS for further details.

6.4.1.2 Subscribers

Subscribers sets and protects the activation data for their private keys to the extent necessary to prevent the loss, theft, unauthorized disclosure, and use of these private keys. Such obligation is presented to the subscribers as part of the Subscriber Agreement.

6.4.2 Activation Data Protection

6.4.2.1 Subordinate CA

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

6.4.2.2 Subscribers

Subscribers protects the activation data for their private keys to the extent necessary to prevent the loss, theft, unauthorized disclosure, and use of these private keys. Such obligation is presented to the subscribers as part of the Subscriber Agreement

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 internal policy documentation.

In particular, the CA 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 CA systems and end-point protection

- Backup and recovery mechanisms for CA operations
- Hardening of CA 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 CA operational processes
- The CA systems enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer Security Rating

No stipulation .

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 CA' 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 CA's operations team.

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

A configuration management process is enforced to ensure that Subordinate CAs systems configuration, modification and upgrades are documented and controlled by the PKI operations management.

A vulnerability management process is enforced to ensure that the CA equipment is scanned for malicious code on first use and periodically thereafter. The vulnerability management process supports the processing within 96 hours of discovery of critical vulnerabilities not previously met by the PKI operations team.

6.6.3 Life Cycle Security Controls

Refer to Section 6.5.1 for details.

6.7 Network Security Controls

ECAC implemented strong network security, including managed firewalls and intrusion detection systems. The network is segmented into several zones, based on their functional, logical, and physical relationship. Network boundaries is applied to limit the communication between systems (within zones) and communication between zones, with rules that support only the services, protocols, ports, and communications that the Subordinate CAs have identified as necessary to its operations, disabling all accounts, applications, services, protocols, and ports that are not used in the CAs' operations.

Issuing Systems, Certificate Management Systems, and Security Support Systems are protected within a highly Secure network Zone.

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

6.8 Timestamping

The CA components are regularly synchronized with a reliable time service. The time-stamping services setup reaches an accuracy of the time of +/-1s or better with respect to UTC.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profiles

S/MIME CA

*CE = Critical Extension.
*O/M: O = Optional, M = Mandatory.
* CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	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	Root CA Signature	Root CA's signature value
TBSCertificate					
Version	False	M	S		
Version		M	S	2	Version 3
SerialNumber	False	M	D		
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M	S		
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M	S	<Root CA's Subject>	The issuer field is defined as the X.501 type "Name"
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	UTF8 encoded
CommonName		M	S	ECAC SMIME Root CA G1	UTF8 encoded
Validity	False	M	D		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 + **[72]** Months	Suggested validity for the subordinate certificate is up to 06 years
Subject	False				
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	UTF8 encoded
CommonName		M	S	ECAC SMIME CA G1	UTF8 encoded
SubjectPublicKeyInfo	False	M	D		
AlgorithmIdentifier		M	D	RSA (OID: 1.2.840.113549.1.1.1) NULL	
SubjectPublicKey		M	D	Key length: 4096	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M	D		Mandatory in all certificates except for self-signed certificates

KeyIdentifier		M	D	160-bit SHA-1 Hash of the Root CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M	S		
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		M	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		M	S	http://repository-ecac.pki.gov.pk/repository/cert/smime_root_ca.p7b	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M	S		
DistributionPoint		M	S	http://repository-ecac.pki.gov.pk/repository /crl/smime_root_ca.crl	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M	S		
keyCertSign, cRLSign		M	S	True	
Policy Properties					
certificatePolicies	False	M	S		

	PolicyIdentifier		M	S	1.3.6.1.4.1.59337.1.1	
	policyQualifiers:policyQualifierId		M	S	id-qt 1	
	policyQualifiers:qualifier:cPSuri		M	S	https://ecac.pki.gov.pk/repository/cps	
certificatePolicies		False	M	S		
	PolicyIdentifier		M	S	2.23.140.1.5.3.3	Sponsor-validated Strict
certificatePolicies		False	M	S		
	PolicyIdentifier		M	S	2.23.140.1.5.4.3	Individual-validated Strict
certificatePolicies		False	M	S		
	PolicyIdentifier		M	S	2.23.140.1.5.2.3	Organization-validated Strict
certificatePolicies		False	M	S		
	PolicyIdentifier		M	S	2.23.140.1.5.1.3	Mailbox-validated Strict
Extended Key Usage Properties						
extKeyUsage		False	M	S		
	emailProtection		M	S	True	
Basic Constraints Properties						
basicConstraints		True	M	S		
	cA		M	S	True	
	pathLenConstraint		M	S	0	

S/MIME Sponsor-Validated Certificate

*CE = Critical Extension.
*O/M: O = Optional, M = Mandatory.
* CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	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	Subordinate CA Signature.	SMIME Subordinate CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
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		<Subordinate Issuing CA's Subject>	The issuer field is defined as the X.501 type "Name"
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	UTF8 encoded

CommonName		M	S	ECAC SMIME CA G1	UTF8 encoded
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 + **[24]** Months	Validity for the end user certificate is up to 825 days
Subject	False				
CountryName		M	S	Country Name	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280). If present shall be "IQ"
OrganizationName		M	D	The Subject's full legal organization name and/or an Assumed Name. If both are included, the Assumed Name SHALL appear first, followed by the full legal organization name in parentheses.	UTF8 encoded
OrganizationIdentifier		M	D	Registration Reference[5] for a Legal Entity assigned in accordance with the identified Registration Scheme.	a PrintableString or UTF8String
GivenName		M	D	Given Name of the Subject	UTF8 encoded
Surname		M	D	Surname of Subject	UTF8 encoded

[5] Must be GOVPK. If the Government Entity is verified at a subdivision (state or province) level, then it must be ''GOVPK+ an ISO 3166-2 identifier for the subdivision (up to three alphanumeric characters)''

SERIALNUMBER		M	D	an identifier assigned by the CA or RA to identify and/or to disambiguate the Subject	PrintableString encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA (OID: 1.2.840.113549.1.1.1) NULL	
SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M	D		Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate Issuing CA public key	When this extension is used, this field MUST be supported as a minimum
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		M	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		M	S	http://ocsp.pki.gov.pk/repository/certs/smime_ca.p7b	Subordinate Issuing CA Certificate/Chain download URL over HTTP

crlDistributionPoints	False	M			
DistributionPoint		M	S	http://ocsp.pki.gov.pk/repository/crl/smime_ca.crl	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M			
digitalSignature keyEncipherment		M	S	True	
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	1.3.6.1.4.1.59337.1.5	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://ocsp.pki.gov.pk/repository/cps	
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.23.140.1.5.3.3	Sponsor-validated Strict
certificatePolicies	False	M			
PolicyIdentifier		M	S	1.3.6.1.4.1.59337.3.1.3	
Extended Key Usage Properties					
extKeyUsage	False	M			
emailProtection		M	S	True	
Subject Alternative Name Properties					

subjectAlternativeName		False	M			
	rfc822name		M	D	One or more email addresses of the certificate owner	

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

The CA complies with RFC 5280 and the "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates" in all certificates it issues.
The CA and end entity certificates for S/MIME purposes include an Extended Key Usage extension containing key usage purposes id-kp-emailProtection.

AnyExtendedKeyUsage KeyPurposeId cannot be included in the certificates.

7.1.3 Algorithm Object Identifiers

Certificates are issued with algorithms indicated by the following OIDs

Algorithm	Object Identifier
sha256WithRSAEncryption	OBJECT IDENTIFIER ::= { iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }

7.1.4 Name forms

7.1.4.1 Name Encoding

The CA issues Certificates with name forms compliant to RFC 5280 and section 7.1.4 of the Baseline Requirements.

7.1.4.2 Subject Information - Subscriber Certificates

The applicable subject information for S/MIME certificates is specified in the table below. ECAC issues Certificates where the contents of the Subject DN fields are compliant with their corresponding definitions stated in section 7.1.4 of the Baseline Requirements

TLS Certificate Type	Subject DN	Subject Alternative Name
Sponsor-validated S/MIME Certificates	• countryName • organizationName • OrganizationIdentifier • givenName • Surname • SERIALNUMBER	• rfc822name

7.1.4.3 Subject Information – Subordinate CA Certificates

For CA certificate, commonName, organizationName and countryName attributes are present and the combination of these contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.

7.1.5 Name Constraints

ECAC follows the requirements of section 7.1.5 of the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates.

7.1.6 Certificate Policy Object Identifier

ECAC uses an OID scheme specified for the Pakistan National PKI Policy. Refer to section 7.1 of this CPS for more details.

Following Object Identifier is also used:

End entity certificate policies	
2.23.140.1.5.3.3	CAB SMIME Reserved Policy for Sponsor-validated Strict Certificates

7.1.7 Usage of Policy Constraints Extension

No Stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

The Subordinate CA contain a CPS Policy Qualifier that points to the applicable CPS .

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No Stipulation.

7.2 CRL Profile

S/MIME CA CRL

*CE = Critical Extension.
*O/M: O = Optional, M = Mandatory.
* CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	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	The signature of the CA issuing the CRL.	The signature of the authority issuing the CRL.
TbSCertList					
Version	False	M			
Version			S	1	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	PK	
OrganizationName		M	S	Electronic Certification Accreditation Council	
CommonName		M	S	ECAC SMIME CA G1	
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**	**Validity period** is 6 months for CRLs issued by the Root CA
RevokedCertificates		False	M			
	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	M			
	reasonCode		M	D	As per BR 7.2.2	Identifies the reason for the certificate revocation
CRLExtensions		False	M			
	AuthorityKeyIdentifier	False	M	D	160-bit SHA-1 hash of the public key of the CA issuing the CRL	
	CRL Number	False	M	D		Sequential CRL Number

7.2.1 Version Number(S)

The CA support X509 v2 CRLs.

7.2.2 CRL and CRL Entry Extensions

The profile of the CRL is provided in section 7.2 above.

7.3 OCSP Profile

S/MIME CA OCSP

*CE = Critical Extension.
*O/M: O = Optional, M = Mandatory.
* CO = Content: S = Static, D = Dynamic

Field	CE	O/M	CO	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.
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
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		<Subject of the CA issuing the OCSP Certificate>	The issuer field is defined as the X.501 type "Name"
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	UTF8 encoded

CommonName		M	S	ECAC SMIME CA G1	UTF8 encoded
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 + validity period	**Validity period** is 12 months for OCSP Certificates
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	UTF8 encoded
CommonName		M	S	ECAC SMIME CA G1 OCSP	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 4096 (RSA)	
Extensions		M			
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Authority Properties					

AuthorityKeyIdentifier	False	M			Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 hash of the public key of the CA issuing the OCSP Certificate	When this extension is used, this field MUST be supported as a minimum
Policy Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
extKeyUsage	False	M			
id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck	False	M			

7.3.1 Version Number(s)

As per the OCSP certificate profile, section 7.3.

7.3.2 OCSP Extensions

As per the OCSP certificate profile, section 7.3.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

The PMA audit function conducts internal audits at least annually, which encompass the Subordinate CA operations. This internal audit is part of the PMA operational cycle and the PMA ensures that mitigations are implemented timely for the audit findings.

External audits are conducted by an independent WebTrust practitioner in accordance with the WebTrust audit scheme. These audits ensure that ECAC complies with applicable requirements, standards, procedures, and service levels. The period during which the Subordinate CA issue certificates is divided into a continuous sequence of audit periods, with each audit period not exceeding one (1) year in duration.

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 audits, 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 NR-CAs are audited for compliance to the following standard:

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities – S/MIME
- WebTrust Principles and Criteria for Certification Authorities – Network Security.

8.5 Actions Taken as a Result of Deficiency

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

Regarding compliance audits of Subordinate CA operations, any notable exceptions or deficiencies discovered during the audit process prompt a decision on necessary actions. This decision is made by the PMA with input from the auditor. Should exceptions or deficiencies arise, PMA assumes responsibility for formulating and executing a corrective action plan. Following implementation of the plan, PMA initiates an additional audit to ensure that identified deficiencies have been carried out.

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

ECAC, through its compliance function, monitors and strictly controls adherence to the procedures outlined in this CPS document, and the S/MIME Baseline Requirements. This is achieved by conducting regular internal audits (at least on a quarterly basis) using randomly selected samples. The audits cover at least 3% of the Certificates issued by S/MIME CA issued since the last internal audit.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Not Applicable.

9.1.2 Certificate Access Fees

No fees will be charged to access the certificates issued.

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

Not Applicable.

9.1.5 Refund Policy

Not Applicable.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

ECAC ensures that the CA is covered by existing insurance provisions.

9.2.2 Other Assets

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

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 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 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 Subordinate CA 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 Pakistan.

Private information will not be disclosed by the ECAC to subscribers except for information about themselves and only covered by the contractual agreement between the ECAC and the subscribers

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 shall preserve the privacy and confidentiality of any exchanged private information. Data encryption shall be used when electronic communication channels are used with the CA systems. This includes:

- The communications between the RA systems and the subscribers.
- The communications between the RA and the CA 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.

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 NR-CAs databases, repository, the Subordinate CAs digital certificates and any other publication originating from the ECAC PMA, including this CPS.

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement.
2. All Application Software Suppliers with whom the Pakistan National Root CA will enter into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier.
3. and all Relying Parties who reasonably rely on a Valid Certificate.

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

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

1. **Right to Use Mailbox Address:** That, at the time of issuance, the CA (i.) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Mailbox Addresses listed in the Certificate's subject field and subjectAltName extension (or was delegated such right or control by someone who had such right to use or control); (ii). Followed the procedure when issuing the Certificate; and (iii). accurately described the procedure in the CA's CP and/or CPS;
2. **Authorization for Certificate**: That, at the time of issuance, the CA (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 CPS;

3. **Accuracy of Information**: That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:serialNumber attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;
4. **Identity of Applicant**: That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2 and 7.1.4.2.2 of SMIME BR; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;
5. **Subscriber Agreement**: That, if the CA 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;
6. **Status**: That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates;
7. **Revocation**: That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

9.6.2 RA Representations and Warranties

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

9.6.3 Subscriber Representations and Warranties

Not Applicable.

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 the 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 damage suffered whether directly or indirectly because of an uncontrollable disruption of the CA service.
- Any form of misrepresentation of information by Subscriber or relying parties on information contained in this CPS or any other documentation made public by the PMA and related to the ECAC service.

9.8 Limitations of Liability

- ECAC will not incur any liability to Subscribers to the extent that such liability results from their negligence, fraud, or wilful misconduct
- ECAC assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under this CPS for any use other than in accordance with this document,
- 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, Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations; and
- Subscribers 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
- ECAC denies any financial or any other kind of responsibility for damages or impairments resulting from the CA operations.

9.9 Indemnities

Not Applicable.

9.10 Term And Termination

9.10.1 Term

This CPS is approved by the ECAC PMA and shall remain in force until amendments are published on the ECAC repository.

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 relevant stakeholders in relation to the termination (and related effects) of this document.

9.11 Individual Notices and Communications with Participants

Notices related to this 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 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 CPS becomes effective. The older versions of this document are archived on the ECAC public repository.

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

The ECAC PMA reserve the right to amend this 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

The PMA reserves the right to amend content of any published CPS. Any major change of this CPS will not alter the OID of the CPS published in the PMA public repository. The OID value corresponds to the current applicable and valid version for the CPS.

9.13 Dispute Resolution Provisions

All disputes associated with the provisions of this 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 CPS.

9.15 Compliance with Applicable Law

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

9.16.3 Severability

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