Pakistan National PKI

ECAC Root Certification Authorities CP/CPS

Version control

Version	Date	Description / Status	Responsible
V1.0	08/12/2022	Initial version for review & approval	ECAC
V1.1	22/12/2022	Reviewed and updated the Email Addresses, URLs and Object IDs	ECAC
V1.2	28/12/2022	Reviewed and updated the CA Common Name, Subject Name in section 7	ECAC
V1.3	22/02/2023	Updated based on feedback from design authority and WebTrust auditor	ECAC
V1.4	06/07/2023	Corrected certificate and CRL addresses in section 7. Addressed the findings in point-in-time audit	ECAC
V2.0	01/11/2024	Updated to accommodate the changes in the PKI hierarchy after ECAC's intermediate CAs /NTC CAs termination.	ECAC
V2.1	25/02/2025	Clarifying the ECAC scope (section 1.1) and Rectifying typos.	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 12
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 14
1.3.3 Subscribers 15
1.3.4 Relying Parties 15
1.3.5 Other Participants 15
1.4 Certificate Usage 15
1.4.1 Appropriate Certificate Uses 15
1.4.2 Prohibited Certificate Uses 15
1.5 Policy Administration 15
1.5.1 Organization Administering the Document 15
1.5.2 Contact Person 16
1.5.3 Person Determining CPS Suitability for the Policy 17
1.5.4 CPS Approval Procedures 17
1.6 Definitions and Acronyms 17
1.6.1 Definitions 17
1.6.2 Acronyms 21
1.6.3 References 22
2 Publication and Repository Responsibilities 24
2.1 Repositories 24
2.2 Publication of Certification Information 24
2.3 Time or Frequency of Publication 24
2.3.1 CA Certificates 24
2.3.2 CARLs 24
2.4 Access Controls on Repositories 25
3 Identification and Authentication 26
3.1 Naming 26
3.1.1 Types of Names 26
3.1.2 Need for Names to be Meaningful 29

3.1.3 Anonymity or Pseudonymity of Subscribers 29
3.1.4 Rules for Interpreting Various Name Forms 29
3.1.5 Uniqueness of Names 29
3.1.6 Recognition, Authentication, and Role of Trademarks 29
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 Authentication of Individual Identity 30
3.2.4 Non-verified Subscriber Information 30
3.2.5 Validation of Authority 30
3.2.6 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 31
3.4 Identification and Authentication for Revocation Request 31
4 Certificate Life-Cycle Operational Requirements 32
4.1 Certificate Application 32
4.1.1 Who Can Submit a Certificate Application 32
4.1.2 Enrollment Process and Responsibilities 32
4.2 Certificate Application Processing 33
4.2.1 Performing Identification and Authentication Functions 33
4.2.2 Approval or Rejection of Certificate Applications 34
4.2.3 Time to Process Certificate Applications 34
4.3 Certificate Issuance 34
4.3.1 CA Actions During Certificate Issuance 34
4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 35
4.4 Certificate Acceptance 35
4.4.1 Conduct Constituting Certificate Acceptance 35
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 36

4.6.1 Circumstance for Certificate Renewal 36
4.6.2 Who May Request Renewal 36
4.6.3 Processing Certificate Renewal Requests 36
4.6.4 Notification of New Certificate Issuance to Subscriber 36
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 36
4.6.6 Publication of the Renewal Certificate by the CA 36
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 36
4.7 Certificate Re-Key 36
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 37
4.7.6 Publication of the Re-Keyed Certificate by the CA 37
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 37
4.8 Certificate Modification 37
4.8.1 Circumstance for Certificate Modification 37
4.8.2 Who May Request Certificate Modification 37
4.8.3 Processing Certificate Modification Requests 37
4.8.4 Notification of New Certificate Issuance to Subscriber 37
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 39
4.9.3 Procedure for Revocation Request 39
4.9.4 Revocation Request Grace Period 40
4.9.5 Time Within Which CA Must Process the Revocation Request 40
4.9.6 Revocation Checking Requirement for Relying Parties 40
4.9.7 CRL Issuance Frequency (If Applicable) 40
4.9.8 Maximum Latency for CRLs (if applicable) 40
4.9.9 On-Line Revocation/Status Checking Availability 40
4.9.10 On-Line Revocation Checking Requirements 41

4.9.11 Other Forms of Revocation Advertisements Available 41
4.9.12 Special Requirements Re Key Compromise 41
4.9.13 Circumstances for Suspension 41
4.9.14 Who Can Request Suspension 41
4.9.15 Procedure for Suspension Request 41
4.9.16 Limits on Suspension Period 41
4.10 Certificate Status Services 41
4.10.1 Operational Characteristics 41
4.10.2 Service Availability 41
4.10.3 Optional Features 42
4.11 End of Subscription 42
4.12 Key Escrow and Recovery 42
4.12.1 Key Escrow and Recovery Policy and Practices 42
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 42
5 Facility, Management, and Operational Controls 43
5.1 Physical Security Controls 43
5.1.1 Site Location and Construction 43
5.1.2 Physical Access 43
5.1.3 Power And Air Conditioning 44
5.1.4 Water Exposures 44
5.1.5 Fire Prevention and Protection 44
5.1.6 Media Storage 44
5.1.7 Waste Disposal 44
5.1.8 Off-Site Backup 44
5.2 Procedural Controls 45
5.2.1 Trusted Roles 45
5.2.2 Number of Persons Required per Task 45
5.2.3 Identification and Authentication for each Role 46
5.2.4 Roles Requiring Separation of Duties 46
5.3 Personnel Controls 46
5.3.1 Qualifications, Experience, and Clearance Requirements 46
5.3.2 Background Check Procedures 47
5.3.3 Training Requirements 47
5.3.4 Retraining Frequency and Requirements 47

5.3.5 Job Rotation Frequency and Sequence 47
5.3.6 Sanctions for Unauthorized Actions 47
5.3.7 Independent Contractor Requirements 48
5.3.8 Documentation Supplied to Personnel 48
5.4 Audit Logging Procedures 48
5.4.1 Types of Events Recorded 48
5.4.2 Frequency Of Processing Log 49
5.4.3 Retention Period for Audit Log 50
5.4.4 Protection Of Audit Log 50
5.4.5 Audit Log Backup Procedures 50
5.4.6 Audit Collection System (Internal vs. External) 50
5.4.7 Notification to Event-Causing Subject 51
5.4.8 Vulnerability Assessments 51
5.5 Records Archival 51
5.5.1 Types of Records Archived 51
5.5.2 Retention Period for Archive 52
5.5.3 Protection of Archive 52
5.5.4 Archive Backup Procedures 52
5.5.5 Requirements for Timestamping of Records 52
5.5.6 Archive Collection System (Internal or External) 52
5.5.7 Procedures to Obtain and Verify Archive Information 52
5.6 Key Changeover 52
5.7 Compromise And Disaster Recovery 53
5.7.1 Incident and Compromise Handling Procedures 53
5.7.2 Computing Resources, Software, and/or Data are Corrupted 53
5.7.3 Entity Private Key Compromise Procedures 53
5.7.4 Business Continuity Capabilities after a Disaster 53
5.8 CA or RA Termination 54
6 Technical Security Controls 54
6.1 Key Pair Generation and Installation 55
6.1.1 Key Pair Generation 55
6.1.2 Private Key Delivery to Subscriber 56
6.1.3 Public Key Delivery to Certificate Issuer 56
6.1.4 CA Public Key Delivery to Relying Parties 56

6.1.5 Key Sizes 56
6.1.6 Public Key Parameters Generation and Quality Checking 56
6.1.7 Key Usage Purposes (as per X.509 v3 key usage field) 56
6.2 Private Key Protection and Cryptographic Module Engineering Controls 56
6.2.1 Cryptographic Module Standards and Controls 56
6.2.2 Private Key (n out of m) Multi-person Control 57
6.2.3 Private Key Escrow 57
6.2.4 Private Key Backup 57
6.2.5 Private Key Archival 57
6.2.6 Private Key Transfer into or from a Cryptographic Module 57
6.2.7 Private Key Storage on Cryptographic Module 57
6.2.8 Method of Activating Private Key 58
6.2.9 Method of Deactivating Private Key 58
6.2.10 Method of Destroying Private Key 58
6.2.11 Cryptographic Module Rating 58
6.3 Other Aspects of Key Pair Management 58
6.3.1 Public Key Archival 58
6.3.2 Certificate Operational Periods and Key Pair Usage Periods 58
6.4 Activation Data 58
6.4.1 Activation Data Generation and Installation 58
6.4.2 Activation Data Protection 58
6.4.3 Other Aspects of Activation Data 59
6.5 Computer Security Controls 59
6.5.1 Specific Computer Security Technical Requirements 59
6.5.2 Computer Security Rating 59
6.6 Life Cycle Technical Controls 59
6.6.1 System Development Controls 59
6.6.2 Security Management Controls 60
6.6.3 Life Cycle Security Controls 60
6.7 Network Security Controls 60
6.8 Timestamping 60
7 Certificate, CRL, and OCSP Profiles 61
7.1 Certificate Profiles 61
7.1.1 Version Number(s) 78

7.1.2 Certificate Extensions 78
7.1.3 Algorithm Object Identifiers 78
7.1.4 Name Forms 78
7.1.5 Name Constraints 78
7.1.6 Certificate Policy Object Identifier 78
7.1.7 Usage of Policy Constraints Extension 78
7.1.8 Policy Qualifiers Syntax and Semantics 78
7.1.9 Processing Semantics for the Critical Certificate Policies Extension 78
7.2 CRL Profile 79
7.2.1 Version Number(S) 91
7.2.2 CRL and CRL Entry Extensions 91
7.3 OCSP Profile 92
7.3.1 Version Number(s) 110
7.3.2 OCSP Extensions 110
8 Compliance Audit and Other Assessments 111
8.1 Frequency or Circumstances of Assessment 111
8.2 Identity/Qualifications of Assessor 111
8.3 Assessor's Relationship to Assessed Entity 111
8.4 Topics Covered by Assessment 111
8.5 Actions Taken as a Result of Deficiency 112
8.6 Communication of Results 112
8.7 Self-audit 112
9 Other Business and Legal Matters 113
9.1 Fees 113
9.1.1 Certificate Issuance or Renewal Fees 113
9.1.2 Certificate Access Fees 113
9.1.3 Revocation Or Status Information Access Fees 113
9.1.4 Fees for Other Services 113
9.1.5 Refund Policy 113
9.2 Financial Responsibility 113
9.2.1 Insurance Coverage 113
9.2.2 Other Assets 113
9.2.3 Insurance or Warranty Coverage for End-Entities 113
9.3 Confidentiality of Business Information 113

9.3.1 Scope of Confidential Information 113
9.3.2 Information Not within the Scope of Confidential Information 113
9.3.3 Responsibility to Protect Confidential Information 114
9.4 Privacy of Personal Information 114
9.4.1 Privacy Plan 114
9.4.2 Information Treated as Private 114
9.4.3 Information Not Deemed Private 114
9.4.4 Responsibility to Protect Private Information 114
9.4.5 Notice and Consent to Use Private Information 115
9.4.6 Disclosure Pursuant to Judicial or Administrative Process 115
9.4.7 Other Information Disclosure Circumstances 115
9.5 Intellectual Property Rights 115
9.6 Representations and Warranties 115
9.6.1 CA Representations and Warranties 115
9.6.2 RA Representations and Warranties 116
9.6.3 Subscriber Representations and Warranties 116
9.6.4 Relying Party Representations and Warranties 116
9.6.5 Representations and Warranties of Other Participants 117
9.7 Disclaimers Of Warranties 117
9.8 Limitations of Liability 117
9.9 Indemnities 118
9.10 Term And Termination 118
9.10.1 Term 118
9.10.2 Termination 118
9.10.3 Effect of Termination and Survival 118
9.11 Individual Notices and Communications with Participants 118
9.12 Amendments 118
9.12.1 Procedure for Amendment 118
9.12.2 Notification Mechanism and Period 118
9.12.3 Circumstances under which OID Must Be Changed 118
9.13 Dispute Resolution Provisions 119
9.14 Governing Law 119
9.15 Compliance with Applicable Law 119
9.16 Miscellaneous Provisions 119

9.16.1 Entire Agreement 119
9.16.2 Assignment 119
9.16.3 Severability 119
9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights) 119
9.16.5 Force Majeure 120
9.17 Other Provisions 120

1 Introduction

This Certificate Policy and Certification Practice Statement (CP/CPS) of the Electronic Certification Accreditation Council (ECAC) governs the policies and practices for Pakistan's National Root Certification Authorities (NR-CAs) in performing root certification services.

This CP/CPS applies to all processes associated with the issuance and management of digital certificates for subordinate certification authorities (Subordinate CAs) operating under the NR-CAs' trust hierarchy.

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

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

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

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

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline
- WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- WebTrust Principles and Criteria for Certification Authorities – Network Security
- WebTrust Principles and Criteria for Certification Authorities – S/MIME

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

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
- CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates
- CA/Browser Forum Network and Certificate System Security Requirements

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates

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

Further information with regard to this CP/CPS, and the NR-CAs can be obtained from the ECAC 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 non-government 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 via a structured hierarchy of Certification Authorities (CAs). Furthermore, ECAC establishes a foundation for additional trust service providers that support both the non-government & Government sectors.
This setup provides a resilient framework to support variance in requirements between government and non-government sectors regarding the offering and consumption of certification and other trust services.

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

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

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

(ii) **Level 2:** This level includes ECAC's Subordinate CAs dedicated to serving the government and non-government sectors, each certified by the corresponding Root CA at the top (Level 1) of the hierarchy.

Additionally, Subordinate CAs operated by authorized (i.e., licensed) Trust Service Providers (TSPs) for delivering trust services to the commercial and government sectors are also part of this level. These Subordinate CAs will be technically constrained through a combination of Extended Key Usage and, optionally, Name Constraint extensions to restrict the scope within which TSPs may issue end-user certificates.

The licensing process is addressed to TSPs that meets the contractual, audit and policy requirements of ECAC root services with regard to operational practices and technical implementation.

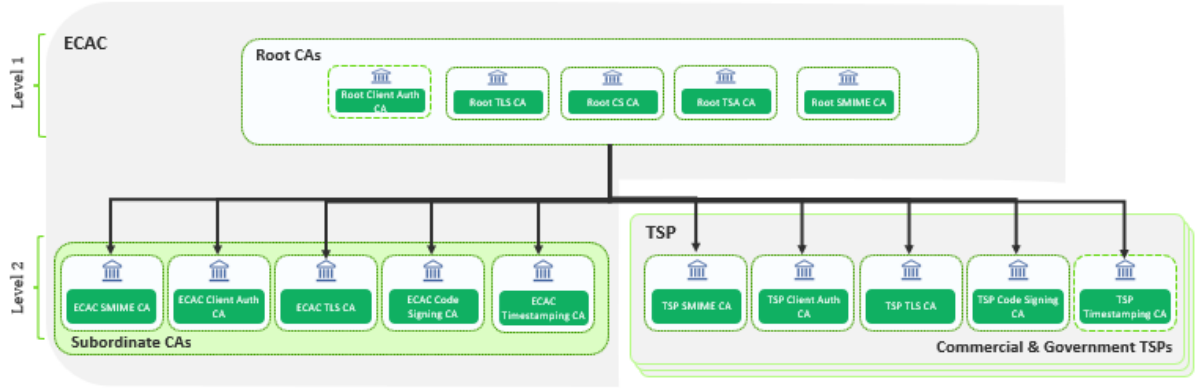

Figure 1 - Pakistan national PKI hierarchy

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

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

1.3 PKI Participants

PKI Participants defined within the scope of this document are the parties bearing relevant rights and obligations within the certification services of the NR-CAs.
These parties are defined as Certification Authorities, Registration Authority, Subscribers and Relying Parties.

1.3.1 Certification Authorities

The NR-CAs is the trust anchor of the Pakistan's PKI hierarchy for ECAC's subscribers and relying parties. NR-CAs is owned by ECAC and renders certification services to itself (issues and renews its own certificates) as well to their Subordinate CAs and the TSP's Subordinate CAs in accordance with this CP/CPS under the responsibility of the ECAC's PMA. The NR-CAs is maintained offline.

The PMA seeks inclusion and maintenance of the NR-CAs and its Subordinate CAs into major operating system and software providers (namely into the corresponding "root programs" from Google, Apple, Microsoft, Adobe and Mozilla), this will result in the recognition of the NR-CAs certificates in off-the-shelf applications and web browsers, supporting the technical and trust recognition of the electronic signatures, electronic end-entity certificates and other trust service outputs from the TSP services approved under the Pakistan's PKI framework.

Commercial and Governmental TSPs will be responsible for seeking the inclusion and maintenance of their subordinate CAs into the "root program".

1.3.2 Registration Authorities

The PMA organizational structure includes the Registration Authority function, this RA function is tasked to request the issuance and the revocation of certificates under this CP/CPS from the NR-CAs.

The RA participates in the execution of the NR-CAs operational cycle, including the key ceremonies for the TSP Subordinate CAs, as well as the generation of Certificate Authority Revocation Lists (CARLs).

1.3.3 Subscribers

The NR-CAs issue certificates exclusively to their Subordinate CAs and to external entities (TSPs) operating Subordinate CAs under the NR-CAs.

1.3.4 Relying Parties

Relying Parties are entities that rely on a Certificate and/or digital signature issued by the NR-CAs. The relying parties shall always verify the validity of a digital certificates issued by the NR-CAs using the NR-CAs Certificates Validity Status Services (i.e., CRL and OCSP), prior to relying on information featured in said certificate.

The NR-CAs certificates are published on the public repository

1.3.5 Other Participants

There are no other participants.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The following NR-CAs are self-signed certificates:

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

The NR-CAs certificate can be used to:

a) Sign certificates for the Subordinate CAs.
b) Sign authority revocation lists (CARLs), containing the list of Subordinate CAs revoked certificates.
c) Sign OCSP responder certificates for the NR-CAs OCSP service

1.4.2 Prohibited Certificate Uses

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

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 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 NR-CAs or their own Subordinate CAs by sending an email to ecac.certification.problem@pki.gov.pk

The ECAC PMA will validate and investigate the request before taking an action in accordance with section 4.9.

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS Approval Procedures

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

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

On an annual basis, if no other changes are made to this CP/CPS, its version number is incremented, and a dated changelog entry is added to denote that.

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 CP/CPS, NR-CAs issue certificates exclusively to their Subordinate CAs and to external entities (TSPs) operating Subordinate CAs under the NR-CAs.

Applicant Representative – A natural person or human sponsor who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a certificate request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root 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 CP/CPS, attestation letters are signed by Human Resource teams of the legal 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 Revocation List (CARL): A revocation list containing a list of CA-certificates issued to certification authorities that have been revoked by the certificate issuer.

Certification Authority – An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement – One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certificate Profile – A set of documents or files that 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. .

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.

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

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.

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.

Relying Party – Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.

Repository – An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Root CA – The top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate – The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Subject – The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information – Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

Subordinate CA – A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA. In the context of this CP/CPS, ECAC's Subordinate CAs, TSP's Government Subordinate CAs and Commercial Subordinate CAs are signed by NR-CAs.

Subscriber – A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use. In the context of this CP/CPS,

the ECAC's NR-CAs issue certificates exclusively to their Subordinate CAs and to external entities (TSPs) operating Subordinate CAs under the NR-CAs.

Subscriber Agreement – An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage and/or Name Constraint extensions, as defined within the relevant Certificate Profiles of this document, to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use – Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Valid Certificate – A Certificate that passes the validation procedure specified in RFC 5280.

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

1.6.2 Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CCTV	Closed Circuit TV
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CV	Curriculum Vitae
DN	Distinguished Name
ECAC	Electronic Certification Accreditation Council
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
ISO	International Standards Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier

PIN	Personal Information Number
PKCS#10	Certification Request Syntax Specification
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RSA	Rivest-Shamir-Adelman (The names of the inventors of the RSA algorithm)
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SSL	Secure Sockets Layer
TSA	Timestamping Authority
TLS	Transport Layer Security
TSP	Trust Service Provider
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 - SSL Baseline
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Network Security
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – S/MIME

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates
- CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates
- 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 Subordinate CAs add a pointer (URL) to the relevant CRL to Subscribers' certificates as part of the CDP extension whenever this extension is present,
- An OCSP responder compliant with RFC 6960. The OCSP URL is referenced in the AIA extension of the Subscribers' certificates issued by these Subordinate CAs.

2.3 Time or Frequency of Publication

The PMA reviews this CP/CPS at least once annually and makes appropriate changes so that the NR-CAs' operations remain fully aligned to the requirements listed in section 1 of this CPS.
Modified versions of the CP/CPS are published within five working days after the ECAC PMA approval.

2.3.1 CA Certificates

The CAs' and OCSP certificates are published to the public repository once they are issued , after which they are be moved to the archive.

2.3.2 CARLs

The ECAC maintains the CRL distribution point and the information on this URL as long as it is required to be retained per section 5.5.2 after the expiration date of all certificates containing the CRL distribution point.

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

- At minimum, once every six months, at an agreed time. In addition, a new CARL will be generated and published following the revocation of any Subordinate CA certificate,
- CARLs lifetime shall be set to six months (i.e., 184 days).

2.4 Access Controls on Repositories

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

The ECAC implemented measures regarding logical and physical security to prevent unauthorized persons from adding, erasing, or modifying entries from the repository.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The ECAC NR-CAs follow the standard X500 distinguished names. The names must be unique and meaningful.

The tables below specify the DNs used for the NR-CAs.

3.1.1.1 ECAC's NR-CAs

The NR-CAs are self-signed Certificate carries the following DN:

Code Signing Root CA:

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

Table 1 - CS Root CA Distinguished Name

Client Auth Root CA:

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

Table 2 – Client Auth Root CA Distinguished Name

TLS Root CA:

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

Table 3 - TLS Root CA Distinguished Name

S/MIME Root CA:

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

Table 4 – S/MIME Root CA Distinguished Name

TSA Root CA:

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

Table 5 - TSA Root CA Distinguished Name

The NR-CAs OCSP Certificates carry the following DN:

Attribute	Value
Common Name – "CN"	<Common Name of the Root CA OCSP Certificate>
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK

Table 2 - National Root CA OCSP Distinguished Name

3.1.1.2 ECAC's Subordinate CAs

The DN format allowed for the ECAC subordinate CAs is:

Attribute	Value
Common Name – "CN"	<Common Name of the ECAC's Subordinate CA>
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK

Table 1 – ECAC's Subordinate CAs Distinguished Name

3.1.1.3 Government & Commercial TSPs

The TSP CAs use the following DN scheme:

Attribute	Value
Common Name – "CN"	Meaningful name of the TSP organization
Organization Name – "O"	Name of the TSP organization
Country – "C"	PK
SerialNumber (For EV CAs only)	The organization's registration number that is verified according to the EV guidelines.
BusinessCategory (For EV CAs only)	The organization's business category that is verified as per the EV guidelines
JurisdictionCountryName (For EV CAs only)	PK

Table 1 Government TSPs Distinguished Name

3.1.1.4 Old PKI heirarchy

The Root CA listed below was replaced to align the ECAC's PKI hierarchy with the latest changes in the target vendor root program, and it will be retained solely for legacy purposes.

Root CA

Attribute	Value
Common Name – "CN"	ECAC Root CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Serial Number	75f3520c33e0e4d4f3f36799b7db1cf15f20b265

Table 2 – Old Root CA Distinguished Name

The below Intermediate CAs was terminated:

Government domain:

Attribute	Value
Government SMIME CA	
Common Name – "CN"	ECAC Government SMIME CA G1

Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Serial Number	50716918a1ffb95858e090d039be0a5c33a9e62e
Government Client Authentication	
Common Name – "CN"	ECAC Government Client Authentication CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Serial Number	3fd0e0ea61b72bdd2599163127015add0e0c37b6
Government TLS CA	
Common Name – "CN"	ECAC Government TLS CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Serial Number	55763e2dcf7c02dd776c551d79dc8f1be0047e8f
Government Code Signing CA	
Common Name – "CN"	ECAC Government Code Signing CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Serial Number	3d7958777463c7486c818f88f370553cd5716998
Government Timestamping CA	
Common Name – "CN"	ECAC Government Timestamping CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Serial Number	30acf22688ddb7acb4290f27df5a41edfb2bc02f

Commercial domain:

Attribute	Value
Commercial SMIME CA	
Common Name – "CN"	ECAC Commercial SMIME CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Serial Number	2a1fa8cc3e6bdeb25d4743425eec04c5945b3726
Commercial Client Auth	
Common Name – "CN"	ECAC Commercial Client Authentication CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Serial Number	49333f5787900990df0c4c1545b8515ef13ab224
Commercial TLS CA	
Common Name – "CN"	ECAC Commercial TLS CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Serial Number	2c54f22077fa7e28191234f38de01799da79346c
Commercial Code Signing CA	
Common Name – "CN"	ECAC Commercial Code Signing CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Serial Number	5ac2da6e334a70ffddec6a24c857f95e9f939482
Commercial Timestamping CA	

Common Name – "CN"	ECAC Commercial Timestamping CA G1
Organization Name – "O"	Electronic Certification Accreditation Council
Country – "C"	PK
Serial Number	59992794c79053a9e7fa788767a42e7b5b71b005

3.1.2 Need for Names to be Meaningful

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

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

The PMA enforces the uniqueness of each Subject name in a Certificate in a manner where name uniqueness is not violated when multiple certificates are issued to the same entity. Refer to section 3.1.1.

3.1.6 Recognition, Authentication, and Role of Trademarks

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

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

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The ECAC demands to validate the proof of possession of private key as part of the certificate request processing. The proof of possession is submitted in the form of PKCS#10 format.

3.2.2 Authentication of Organization Identity

3.2.2.1 NR-CA and its Subordinate CAs:

The ECAC's NR-CAs and their Subordinate CAs form the PKI owned and operated by the ECAC under the direct control and supervision of the ECAC PMA to serve the government domain. Consequently, the approval of certification requests for these CAs is managed internally by the ECAC PMA as part of the process of establishing these CAs. This approval is further verified through the organization and oversight of key generation ceremonies by the ECAC PMA.

3.2.2.2 Government TSPs

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

1. Verification of presence and legal standing:

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

2. Verification of association with the certificate subject: The ECAC PMA verifies that the organization name to be inserted in the certificate matches the legal name of the organization requesting the certificate. The full organization's name of an abbreviated version can be included in the certificate
3. Processing of any additional paperwork required by the ECAC PMA as part of the verification process that is required to conclude the review and validation of the TSP request by the ECAC PMA.

3.2.2.3 Commercial TSPs

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

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

3.2.3 Authentication of Individual Identity

The ECAC's NR-CAs do not issue certificates to individuals.

3.2.4 Non-verified Subscriber Information

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

3.2.5 Validation of Authority

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

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

3.2.6 Criteria for Interoperation

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

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

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

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Identification and authentication for re-keying is performed as in initial registration.

3.3.2 Identification and Authentication for Re-key after Revocation

Same provisions as those defined in sections 3.1 and 3.2 apply. This is executed only as part of a re-key operation that is approved after all investigations are performed by ECAC PMA .

3.4 Identification and Authentication for Revocation Request

For the ECAC's Subordinate CAs: Revocation requests are processed by trusted roles within ECAC, under the supervision of the PMA, as part of an authorized internal operational ceremony.

For the TSP Subordinate CAs:

The following revocation procedure is enforced by the ECAC PMA:

- Signed revocation request from an authorized representative or a formal delegate by an authorized representative,
- Verification of the identity of the form signatory based on the information collected during the registration. If the signatory was not involved during the registration, the process defined in section 3.2.5 is followed to authorize the request.

- Communication with the TSP to provide reasonable assurances on confirming the revocation. Such communication, depending on the circumstances, may include one or more of the following: telephone, e-mail, or courier service.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 The ECAC's Subordinate CAs:

Certificates applications to NR-CAs are submited by trusted roles within ECAC, under the supervision of the PMA, as part of an authorized key ceremony. The RA function, authorized by the ECAC PMA, is responsible for setting up Subordinate CAs under the NR-CAs.

4.1.1.2 Government & Commercial TSPs:

A TSP authorized representative submits the certificate application as part of the overall process through which the RA function is authorized by the ECAC PMA to set up its Subordinate CA under the NR-CAs.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 The ECAC's NR-CAs and their Subordinate CAs:

The processes related to standard certificate lifecycle (Issuance, rekey and revocation) of the NR-CAs, and their subordinate CAs are specified as part the ECAC PMA key ceremony documentation.

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

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

4.1.2.2 Government and Commercial TSPs:

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

1. The TSP downloads the Application form from the ECAC repository website https://ecac.pki.gov.pk
2. The form is filled and signed by the Official Representative of the Applicant. The applicant must provide the following information in the form:
    a. Information related to the organization:
        i. Legal Name of the entity (organization)
        ii. Official address of the entity for correspondence
        iii. Official Representative name of the entity
        iv. Applicant Representative(s) name of the entity
    b. Information related to the TSP CA Certificate
        i. Description of the planned TSP certificate usage

ii. Select the TSP certificate types if more than one certificate usage is required
iii. In the case of technically constrained Subordinate CA, TSP registered domain name(s) e.g., "example.com" if the TLS or SMIME certificates will be issued by the Subordinate CA
iv. Required certificate profiles and the values of each attribute that should be present in the Subordinate CA certificate

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

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

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

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 The ECAC's Subordinate CAs:

Identification and authentication functions are carried out by trusted roles associated with the ECAC PMA. The processing of certificate applications to NR-CAs involves

authorized representatives from the RA function, which is operated directly by the ECAC PMA.

4.2.1.2 Government and Commercial TSPs:

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

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

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

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 The ECAC's NR-CAs and their Subordinate CAs:

The ECAC's NR-CAs and their Subordinate CAs are established as part of the ECAC PMA Key Ceremony. The ECAC PMA authorizes the setup of these CAs after validating that all pre-requisites are met including the fulfilment of all compliance verifications.

4.2.2.2 Government and Commercial TSPs:

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

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

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

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

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

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

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

- The ECAC CA operators submit the certificate request to the relevant Root CA to perform a certificate signing operation,
- The ECAC CA operators and the ceremony auditor/witness, validate the issued certificate's content against the profile defined, this CP/CPS and the information submitted in the certificate application,
- The certificate is then handed over to the TSP representative / authorized representative from the RA function.

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

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Not applicable. The NR-CAs only issues certificates to Subordinate CAs.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

4.4.1.1 ECAC's Subordinate CAs:

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

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

4.4.1.2 Government and Commercial TSPs:

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

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

4.4.2 Publication of the Certificate by the CA

Following the acceptance of a certificate, ECAC publishes the issued certificates on its public Repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No other entities or organizations are notified directly of the certificate issuance. They are indirectly notified through the update of the Repository.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber is required to use the Private Key and the Certificate in accordance with CPS of the CA to be certified.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Party is required to use the Subscriber's Public Key and the Certificate in accordance with CPS of the CA to be certified.

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 NR-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 NR-CAs. Subject attributes and other certified attributes can be updated.

4.7.1 Circumstance for Certificate Re-Key

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

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

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

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

4.7.2 Who May Request Certification of a New Public Key

As per the initial certificate issuance.

4.7.3 Processing Certificate Re-Keying Requests

As per the initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per the initial certificate issuance.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per the initial certificate issuance.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per the initial certificate issuance.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per the initial certificate issuance.

4.8 Certificate Modification

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

4.8.1 Circumstance for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

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

4.9.1 Circumstances for Revocation

The NR-CAs will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. A writing revocation request is submitted to the NR-CAs.
2. The NR-CAs is notified that the Subordinate CA's original certificate request was not authorized and does not retroactively grant authorization.
3. The NR-CAs obtains evidence that the Subordinate 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. The NR-CAs obtains evidence that the Certificate was misused.
5. The NR-CAs is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certification Practice Statement.
6. The NR-CAs determines that any of the information appearing in the Certificate is inaccurate or misleading.
7. The Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate.
8. TSP did not successfully complete the regular surveillance audit as per the national TSP accreditation framework, or didn't operate continuously in accordance with the provisions of this CP/CPS and the TSP CP, leading the ECAC PMA to conclude that the identified issues cause an unacceptable risk to the Web Trust status of the Pakistan National PKI.
9. The NR-CAs or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the NR-CAs has planned to continue maintaining the CRL/OCSP Repository; or
10. Revocation is required by the present document.

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

- A certificate revocation ceremony is then planned and executed no later than seventy-two (72) hours after the Subordinate CA certificate revocation is approved,
- Publish the new CARL to reflect the certificate/service revocation and push the revocation status to the OCSP service.
- In case of ECAC's Subordinate CAs, the termination plan is activated.
- In case of government and commercial Subordinate CAs, the PMA notify the TSP and relevant stakeholders. The TSP is responsible for activating its termination plan and communicating with all affected Subordinate CAs
- Update the CCADB and communicate as required with the Root Programs,
- Record all communication, reports, and evidence in relation to the certificate revocation operation for future reference and audit processes

4.9.2 Who Can Request Revocation

The authority to revoke the ECAC's Subordinate CA certificates rests within the ECAC.

A revocation of a TSP certificate can be requested by:

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

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

4.9.3 Procedure for Revocation Request

The procedure for a Subordinate certificate revocation is as follows:

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

Certificate problems reporting:

Subscribers of the Subordinate CAs, relying parties, application software suppliers, and other third parties may submit certificate problem reports to PMA via contact details provided in section 1.5.2.

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

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate Problem Report, the PMA will investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to their Subscribers, concerned authorities and to the originator of the problem report.

After reviewing the facts and circumstances, the PMA work with their Subscribers, concerned authorities and to the originator of the problem report to establish whether or not the certificate will be revoked, and if so, a date which the PMA will revoke the certificate. The period from receipt of the Certificate Problem Report to published revocation will not exceed the time frame set forth in Section 4.9.1

Depending on the revocation circumstances and the national TPS accreditation framework, a new Subordinate CA certificate may be issued.

4.9.6 Revocation Checking Requirement for Relying Parties

The revocation information is made available to the relying parties through CRLs (i.e., CARLs) which are publicly available on the ECAC public repository and through the OCSP responders. Relying parties can use either method to validate the certificate.

4.9.7 CRL Issuance Frequency (If Applicable)

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

4.9.8 Maximum Latency for CRLs (if applicable)

Not stipulation.

4.9.9 On-Line Revocation/Status Checking Availability

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

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

4.9.10 On-Line Revocation Checking Requirements

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

The NR-CAs and its intermediate CAs update information provided via their OCSP responders

(i) every six months; and
(ii) within 24 hours after revoking a Subordinate CA Certificate.

The ECAC OCSP responders that receive a request for status of a certificate that has not been issued, shall not respond with a "good" status for such Certificates. OCSP responders for CAs which are not Technically Constrained, in line with Section 7.1.2.3 or Section 7.1.2.5 of Baseline Requirements, will not respond with a "good" status for such Certificates.

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

4.9.11 Other Forms of Revocation Advertisements Available

Not stipulation.

4.9.12 Special Requirements Re Key Compromise

Not stipulation.

4.9.13 Circumstances for Suspension

The ECAC CAs do not support the certificate suspension.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

OCSP responder exposes an HTTP interface accessible to relying parties.

4.10.2 Service Availability

The public repository where certificate information and CRLs are published 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 ECAC PMA 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 ECAC PMA 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

Not applicable. The NR-CAs only issues certificates to Subordinate CAs.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

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

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

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

5 Facility, Management, and Operational Controls

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

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

1. Physical security and environmental controls,
2. System integrity controls, including configuration and change management, patch management, vulnerability management and malware/virus detection/prevention,
3. Maintaining an inventory of all assets and managing 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 NR-CAs 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 NR-CAs 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 CAs provides UPS and backup generators with enough capability to support the CA systems operations in power failure circumstances. UPS units and stand-by generators are available for the entire facility.

A fully redundant air-conditioning system is installed in the areas hosting the CA systems. All these systems ensure that the ECAC CAs' equipment continuously operate within the manufacturers' range of operating temperatures and humidity.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

The ECAC CAs hosting facility follows leading practices and applicable safety regulations in Pakistan, monitored 24x7x365 and equipped with fire and heat detection equipment.

Fire suppression equipment is installed within dedicated areas and automatically activates in the case of fire, and can be manually activated, if necessary.

5.1.6 Media Storage

Electronic, optical, and other storage media are subject to the multi-tiered physical security and are protected from accidental damage (water, fire, electromagnetic interference).

Audit and backup storage media are stored in a secure fire-proof safe and duplicated and stored in the disaster recovery location.

5.1.7 Waste Disposal

All wastepaper and storage media created within the secure facility shall be destroyed before discarding. Paper media shall be shredded using a crosshatch shredder, and magnetic media shall be wiped by de-magnetization, or physically destroyed. HSMs and related key management devices shall be physically destroyed or securely wiped (zeroized) prior to disposal.

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

5.1.8 Off-Site Backup

A DR-site location is utilized for the storage and retention of NR-CAs backups, including software, data and private keys. These backups are created at the end of each key

ceremony, following a documented key ceremony script and transferred to the DR-Site. The facility is equipped with the same physical security measures as the primary site, offering protection against fire and unauthorized access.

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 a position. The background check shall be maintained and reviewed annually.

The following are the trusted roles for the ECAC CAs:

- **PKI Administrator:** Owning the credentials of the CA software. Responsible for configuring and maintaining the CA.
- **Security Officer:** Owning credentials that enable configuring the HSMs and PKI policies on the target systems subject to key generation during relevant key ceremony. Owner of the Administrator user on the Root CA host system.
- **RA Officer:** Authorized to conduct the vetting of the licensed TSP as part of the certification request processing.
- **M-of-N Custodians**: Owners of the HSM activation data. Custodians of the offline CAs' safes.
- **CA Domain Owner:** Owning the credential that authorizes Root CA HSM backup and restore operations.
- **HSM Auditor:** Owning the credentials for retrieving the HSM audit logs.
- **Data Center Custodians:** Personnel who has the credentials for opening the PKI datacenter while performing the Root CA operations.
- **Compliance officer:** Authorized to collect and review the audit logs generated by the Subordinate CAs' systems and regular internal compliance audits

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 member of staff who needs to physically access equipment located in the secure enclave
- ECAC CAs dedicated staff (system administrators) issue the necessary ICT system credentials for ECAC CAs staff to perform their respective functions.

5.2.4 Roles Requiring Separation of Duties

The PMA will ensure that no individual is assigned more than one Trusted Role. During Root CA operations, the role separation is enforced either by the CA equipment and/or through a defined procedure (i.e., key ceremony script). No individual is assigned more than one role when accessing or operating the CA equipment. All roles have job descriptions, with specific skills and experience requirements, defined from the viewpoint of roles fulfilled.

5.3 Personnel Controls

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

5.3.1 Qualifications, Experience, and Clearance Requirements

Prior to engagement of an NTC PKI staff member, whether as an employee, agent, or an independent contractor, the ECAC PMA ensures that checks are performed to establish the background, qualifications and experience needed to perform within the competence context of the specific job. Such checks include:

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

C. Appropriateness of references, and
D. Any clearances as deemed appropriate

5.3.2 Background Check Procedures

All employees in trusted roles are selected based on integrity, background investigations, and security clearance. The ECAC PMA ensures that these checks are conducted every two years 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 NR-CAs personnel.

The training program encompasses a diverse range of topics and is delivered by a combination of experienced NR-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 NR-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 validation specialists, 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 CP/CPS document, security policies, operational guides and technical documentation relevant to every trusted role.

5.4 Audit Logging Procedures

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. This 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 NR-CAs 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 NR-CAs operations.

5.4.1 Types of Events Recorded

Audit logs are generated for all events relating to the security and services of the ECAC CAs systems. At a minimum, each audit record includes the following:

- The date and time the event occurred
- A success or failure indicator of the event (e.g. CA signing event, revocation event, certificate validation event)
- The identity of the entity and/or operator that caused the event.
- Description of the event.

Where possible, the audit logs are automatically generated and where not possible, a logbook or paper forms are used. The audit logs, both electronic and non-electronic, are retained by the ECAC CAs operations team and may be made available during compliance audits.

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

1. Root CA key life cycle management events, including:
    - Key generation, backup, storage, recovery, archival, and destruction;
    - Cryptographic device lifecycle management events;
2. Subscriber Certificate lifecycle management events, including:
    - Certificate requests, renewal, and re-key requests, and revocation;
    - All verification activities stipulated in the present documemt.
    - Approval and rejection of certificate requests;
    - Issuance of Certificates;
    - Generation of Certificate Revocation Lists; and
    - Signing of OCSP Responses
3. Security events, including:
    - Successful and unsuccessful PKI system access attempts
    - PKI and security system actions performed.
    - Security profiles and configuration changes
    - User management operations
    - System platform issues (e.g., crashes), hardware failures, and other anomalies
    - Relevant router and firewall activities (as described in Section 5.4.1.1); and
    - Entries and exists from the CA facility.

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 ECAC PMA ensures that designated personnel review log files at regular intervals to validate log integrity and ensure timely identification of anomalous events. At a minimum, the following audit log review cycle is implemented by the ECAC PMA:

- Audit and Security logs of the CA applications are reviewed by the security officer's team every six months (since the NR-CAs are all offline),
- Physical access logs and the user management on the ECAC CAs systems shall be reviewed by the Monitoring & Compliance team on a quarterly basis to validate the physical and logical access policies
- The ECAC PMA audit and compliance function executes an internal audit on the ECAC CAs operations on a yearly basis. Samples of the log review reports and collected audit logs since the last audit cycle shall be requested by the ECAC PMA as part of this internal audit

- Evidence of audit log reviews, outcome of the review process, and executed remediation actions are collected and archived.

5.4.3 Retention Period for Audit Log

The ECAC CAs retains the following, for at least two (2) years:

A. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1(1)) after the later occurrence of:
   i. the destruction of the CA Private Key; or
   ii. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509 v3 basic Constraints extension with the CA field set to true and which share a common Public Key corresponding to the CA Private Key,

B. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1(2)) after the revocation or expiration of the Subscriber Certificate,

C. 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 ECAC CAs systems generate cryptographically protected audit logs
- The security of audits logs is maintained while these logs transit by the backup system and when these logs are archived
- The access control policies enforced on the ECAC CAs systems ensure that read access only is granted to personnel having access to audit logs as part of their operational duties
- Only authorized roles can obtain access to systems where audit logs are stored and any attempts to tamper with audit logs can be tracked to the respective ECAC CAs operations personnel.

5.4.5 Audit Log Backup Procedures

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

- Backup media are stored locally in the ECAC CAs main site, in a secure location
- A second copy of the audit log data and files are stored in the disaster recovery location that provides similar physical and environmental security as the main site.

5.4.6 Audit Collection System (Internal vs. External)

Automatic audit processes are initiated at system startup and end at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, the ECAC PMA determines whether to suspend the relevant CA's operations until the problem is fixed.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is required to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

The ECAC NR-CAs operations conduct an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes,
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the ECAC has in place to counter such threats.

The ECAC NR-CAs 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 NR-CAs core and supporting PKI system. This regular self-assessment activity is executed by security personnel part of the NR-CAs operations team.
- On an annual basis, and after infrastructure or application upgrades or modifications that the NR-CAs determines are significant, the ECAC PMA coordinates a third-party independent vulnerability assessment and penetration testing is conducted on the NR-CAs systems.
- The outcome of the regular assessments and identified issues shall be made available to the ECAC PMA and PKI operations management, who shall be responsible to organize and oversee the execution of the remediations by the respective teams.

ECAC NR-CAs 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 ECAC NR-CAs personnel.

5.5 Records Archival

5.5.1 Types of Records Archived

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

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

5.5.2 Retention Period for Archive

Archived audit logs, as 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 CAs shall retain, for at least two (2) years:

A. All archived documentation related to the security of CA Systems (as set forth in Section 5.5.1),
B. All archived documentation relating to the verification, issuance, and revocation of certificate requests and Certificates (as set forth in Section 5.5.1) after the later occurrence of:
    i. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates, or
    ii. the expiration of the Subscriber Certificates relying upon such records and documentation.

5.5.3 Protection of Archive

Records are archived in such a way that they cannot be deleted or destroyed. Controls are in place to ensure that only authorized personnel are able to manage the archive without modifying integrity, authenticity and confidentiality of the contained records.

5.5.4 Archive Backup Procedures

Only one version of each digital archive is maintained in the primary and disaster recovery facilities of the ECAC NR-CAs. The NR-CAs operations team use backup, restore, and archive procedures that document how the archive information is created, transmitted, and stored.

5.5.5 Requirements for Timestamping of Records

All recorded and archived events include the date and time of the event taking place. The time of NR-CAs systems is synchronized with the time source of a GPS clock. Further, the ECAC CAs operations team enforce a procedure that checks and corrects any clock drift.

5.5.6 Archive Collection System (Internal or External)

The EAC CAs archive collection system is internal.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized and authenticated staff shall be allowed to access the archived material. The ECAC CAs operations team use the ECAC CAs backup, restore and archive procedures that document how the archive information is created, transmitted, and stored. These procedures also provide information on the archive collection system.

5.6 Key Changeover

To minimize impact of key compromise, the NR-CAs' key shall be changed with a frequency that ensures the NR-CAs shall have a validity period greater than the maximum lifetime of Subordinate CA's certificates.

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

To support revocation management of Subordinate CA certificates, the old NR-CAs private keys are maintained until all of 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 ECAC CAs is detected by the ECAC PMA, it shall perform an investigation to determine the nature and the degree of damage:

- If a CA Private key is suspected of compromise, the procedures outlined in the ECAC's Business continuity and disaster recovery plan shall be followed. Otherwise, the scope of potential damage shall be assessed to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised,
- The ECAC PMA also specifies applicable compromise reporting and relevant communications as part of the Business continuity and disaster recovery plan,
- Apart from the circumstance of key compromise, the ECAC specifies the recovery procedures used when computing resources, software, and/or data are corrupted or suspected of being corrupted.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

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

The ECAC 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

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

Considering the criticality of such compromise situation and its impact on the Pakistan National PKI, The ECAC PMA will be invited for an emergency meeting to take decisions and handles communications as required as part of the Key compromise and CA termination plans. Refer to sections 4.9.1 and 4.9.3 for further details.

5.7.4 Business Continuity Capabilities after a Disaster

In case of a disaster, corrupted servers, software or data, the ECAC disaster recovery and business continuity plan is triggered to restore the minimum ECAC CAs required

operational capabilities, in a timely fashion. In particular, the plan targets the recovery of the following services, either in the primary location, or the disaster recovery location:

- Certification services (issuance and revocation)
- Public repository where CRLs and CAs certificates are published
- OCSP services

Failover scenarios to the ECAC CAs disaster recovery location are made possible considering the ECAC CAs backup system that enables the continuous replication of critical ECAC CAs data from the primary site to the disaster recovery site. That allows a recovery of the ECAC CAs critical services at the disaster recovery location within a maximum of twelve (12) hours RTO.

The ECAC business continuity plan defines the following:

- 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 NR-CAs' plan to maintain or restore the NR-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 NR-CAs main site; and
- Procedures for securing its facility to the extent possible during the period following a disaster and prior to restoring a secure environment either ate the original or a remote site.

5.8 CA or RA Termination

Note Applicable.

6 Technical Security Controls

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

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 ECAC's NR-CAs:

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

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

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

  A video of the entire key generation ceremony will be recorded and stored securely for audit purposes.

6.1.1.2 ECAC's Subordinate CAs

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

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

- The KGC is subject to the formal authorization of the ECAC PMA
- The KGC is conducted in presence of a combination of authorized personnel with trusted roles including representatives from the ECAC PMA
- The KGC is witnessed by the CA's Qualified Auditor (see section 8 Compliance Audit and Other Assessments)

- Proper distribution of secrets/activation data/key shares to the trusted operatives and key custodians
- A video of the entire key generation ceremony will be recorded and stored securely for audit purposes

6.1.1.3 Government and Commercial TSPs:

The ECAC PMA oversees the establishment of the Government and Commercial TSPs and approves their respective ceremonies after the completion of several verifications including the successful completion of a surveillance audit on the TSP operations. The key generation ceremonies for the TSP are also witnessed by a WebTrust qualified auditor. The security measures that are in place for key generation of the TSP Subordinate CAs are documented in their respective CPS.

6.1.2 Private Key Delivery to Subscriber

Not Applicable.

6.1.3 Public Key Delivery to Certificate Issuer

The Subordinate CA certificate request is processed as part of NR-CAs ceremony which results in the generation of the Subordinate CA certificate that is handed over to the TSP's representative / PMA's RA function representative. NR-CAs also publishes the Subordinate CA certificate on its public repository.

6.1.4 CA Public Key Delivery to Relying Parties

The NR-CAs Certificates are published as soon as they are issued on the ECAC public repository. NR-CAs also publishes in its public repository the Subordinate CA certificates that it has signed.

6.1.5 Key Sizes

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

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

For the creation and storage of the ECAC NR-CAs private keys, FIPS 140-2 Level 3 certified/compliant hardware security modules are used. The HSMs are stored within the most secure and inner zone of the ECAC NR-CAs hosting facility.

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

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

ECAC CAs personnel are assigned to the trusted roles by the ECAC PMA ensuring segregation of duties and enforcing the principles of multi control and split knowledge. Multi-person control of the ECAC CAs private keys is achieved using an "m-of-n" split key knowledge scheme. A certain number of persons 'm' (at least two (2)), out of 'n' persons (three (3) persons), the total number of key custodians, need to be concurrently present, together with HSMs administrators to activate or re-activate the ECAC CAs private key.

The ECAC PMA keeps written, auditable, records of tokens and related password distribution to trusted operatives and key custodians. In case trusted operatives or key custodians are to be replaced, it will keep track of the renewed tokens and/or password distribution.

6.2.3 Private Key Escrow

Private keys of the ECAC NR-CAs are not escrowed. Dedicated backup and restore procedures of the ECAC NR-CAs private key are implemented by the ECAC PMA.

6.2.4 Private Key Backup

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

Backup operations are executed as part of the ECAC CAs' key generation ceremonies. The ECAC CAs' keys are backed up under the same multi-person control and split knowledge as the primary key. The recovery operation of the backup key is subject to the same multi-person control and split knowledge principles.

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

Refer to Section 6.2.2 for further details.

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

The ECAC NR-CAs' key pairs shall only be transferred to another hardware cryptographic token of the same specification as described in 6.2.11 by direct token-to-token copy via trusted path under multi-person control.

At no time shall the ECAC NR-CAs' private keys be copied to disk or other media during this operation.

6.2.7 Private Key Storage on Cryptographic Module

No further stipulation other than those stated in clauses 6.2.1, 6.2.2, 6.2.4 and 6.2.6.

6.2.8 Method of Activating Private Key

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

6.2.9 Method of Deactivating Private Key

The HSMs used for the NR-CAs key ceremony are deactivated at the end of the ceremony which prevents any further use of the private keys. This activity applies to the principles of dual control and split knowledge and is always witnessed by the relevant personnel (PMA, auditor). The HSMs are safely powered off at the end of the ceremony and all material used during the ceremony is put back in their respective safes.

6.2.10 Method of Destroying Private Key

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

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

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Refer to Section 5.5 for archival conditions.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The NR-CAs self-signed certificate is valid for fifteen (15) years, with a Key Usage Period of ten (10) years.
The NR-CAs private keys are not used after the validity period of the associated public key certificates. Beyond the key usage period of the NR-CAs private keys, no Certificates will be issued (i.e., Subordinate CA certificates) except CARLs and OCSP responder certificates for the certificate validity status service.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The ECAC CAs' private keys and HSM activation data is generated during their private key generation ceremonies. Refer to Section 6.1.1 and 6.2.8 of this CP/CPS for further details.

6.4.2 Activation Data Protection

The ECAC NR-CAs' key management policy and ceremony procedures ensure that the principles of multi-person control and split knowledge are permanently enforced to

protect ECAC NR-CAs keys and HSMs activation data. During the KGCs, activation data are permanently under the custody of the designated ECAC trusted personnel. Refer to Section 6.1 and 6.2 for further details.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The ECAC ensures that computer security controls are implemented in compliance with technical standards and vendor security hardening guidelines as a minimum. Implemented computer security controls are documented as part of the ECAC CAs internal policy documentation.

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

- Separation of duties and dual controls for CA operations
- Physical and logical access control enforcement
- Audit of application and security related events
- Continuous monitoring of ECAC CAs systems and end-point protection
- Backup and recovery mechanisms for ECAC NR-CAs operations
- Hardening of ECAC NR-CAs servers' operating system according to leading practices and vendor recommendations
- In-depth network security architecture including perimeter and internal firewalls, web application firewalls, including intrusion detection systems
- Proactive patch management as part of the ECAC NR-CAs operational processes
- The ECAC NR-CAs systems enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer Security Rating

No stipulation — this section intentionally left blank.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Purchased hardware or software are to be shipped in a sealed, tamper-proof container, and installed by qualified personnel. Hardware and software updates are to be procured in the same manner as the original equipment. Dedicated trusted personnel are involved to implement the required ECAC NR-CAs' configuration according to documented operational procedures.

Applications are tested, developed, and implemented in accordance with industry leading development and change management practices. No software (or patches), or hardware is deployed on live systems before going through the change and configuration management processes enforced by the ECAC NR-CAs' operations team.

All ECAC NR-CAs' hardware and software platforms are hardened using industry best practices and vendor recommendations.

6.6.2 Security Management Controls

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

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

Refer to Section 6.6.1 for further details.

6.6.3 Life Cycle Security Controls

Refer to Section 6.5.1 for details.

6.7 Network Security Controls

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

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

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

6.8 Timestamping

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

The NTP server is available for the connected infrastructure. It is used to synchronize the time of the servers that host the OCSP responder for Root CAs.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profiles

ECAC Root CA (legacy Root CA)

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

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

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

Client Auth Root 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 Client Auth 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 + **[180]** Months	Suggested validity for the Root CA certificate is up to 15 years
Subject	False				
CountryName		M	D	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	Electronic Certification Accreditation Council	UTF8 encoded
CommonName		M	S	ECAC Client Auth Root 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					
AuthorityKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Issuer public key	MUST be identical to the subjectKeyIdentifier field
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	
Basic Constraints Properties					
basicConstraints	True	M	S		
cA		M	S	True	

Code Signing Root 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 Code Signing 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 + **[180]** Months	Suggested validity for the Root CA certificate is up to 15 years
Subject	False				
CountryName		M	D	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	Electronic Certification Accreditation Council	UTF8 encoded
CommonName		M	S	ECAC Code Signing Root 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					
AuthorityKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Issuer public key	MUST be identical to the subjectKeyIdentifier field
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	
Basic Constraints Properties					
basicConstraints	True	M	S		
cA		M	S	True	

TLS Root 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 TLS 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 + **[180]** Months	Suggested validity for the Root CA certificate is up to 15 years
Subject	False				
CountryName		M	D	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	Electronic Certification Accreditation Council	UTF8 encoded
CommonName		M	S	ECAC TLS Root 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					
AuthorityKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Issuer public key	MUST be identical to the subjectKeyIdentifier field
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	
Basic Constraints Properties						
basicConstraints		True	M	S		
	cA		M	S	True	

S/MIME Root 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 + **[180]** Months	Suggested validity for the Root CA certificate is up to 15 years
Subject	False				
CountryName		M	D	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	Electronic Certification Accreditation Council	UTF8 encoded
CommonName		M	S	ECAC SMIME Root 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					
AuthorityKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Issuer public key	MUST be identical to the subjectKeyIdentifier field
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	
Basic Constraints Properties					
basicConstraints	True	M	S		
cA		M	S	True	

TSA Root 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 TSA 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 + **[180]** Months	Suggested validity for the Root CA certificate is up to 15 years
Subject	False				
CountryName		M	D	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	D	Electronic Certification Accreditation Council	UTF8 encoded
CommonName		M	S	ECAC TSA Root 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					
AuthorityKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Issuer public key	MUST be identical to the subjectKeyIdentifier field
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	
Basic Constraints Properties						
basicConstraints		True	M	S		
	cA		M	S	True	

7.1.1 Version Number(s)

The ECAC NR-CAs issue X.509 version 3 certificates as defined in RFC 5280.

7.1.2 Certificate Extensions

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

7.1.3 Algorithm Object Identifiers

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

7.1.4 Name Forms

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

7.1.5 Name Constraints

Name constraints are not supported.

7.1.6 Certificate Policy Object Identifier

Certificate policy object identifiers are used as per RFC 3739 and RFC 5280. Furthermore, IQ-NR-CA comply to the following requirements:

- **For Code Signing Root CA:** section 7.1.6 of the Baseline Requirements for the Issuance and Management of Publicly Trusted Code Signing Certificates.
- **For S/MIME Root CA:** section 7.1.6 of the Baseline Requirements for the Issuance and Management of Publicly Trusted S/MIME Certificates.
- **For TLS Root CA:** section 7.1.2.1 & 7.1.6 of the Baseline Requirements for the Issuance and Management of Publicly Trusted TLS Server Certificates

Refer to section 7.1 of this CP/CPS for more details.

7.1.7 Usage of Policy Constraints Extension

Policy Constraints extension is not supported.

7.1.8 Policy Qualifiers Syntax and Semantics

No Stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificate policies extensions must be processed as per RFC 5280.

7.2 CRL Profile

legacy Root CA CARL

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

CRL Profile					
Field	CE[2]	O/M[3]	CO[4]	Value	Comment
CertificateList		M			
TBSCertificate					
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	CA's Signature.	CA's signature value
TbSCertList	False				
Version	False	M			
Version		M	S	2	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M	S		
CountryName		M	S	PK	
OrganizationName		M	S	Electronic Certification Accreditation Council	
CommonName		M	S	CN of the CAs	
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
thisUpdate		M	D	<creation time>	

NextUpdate		M	D	<Creation time> + **[184]** days	
RevokedCertificates	False	O			
Certificate					
CertificateSerialNumber		M	D	Serial of the revoked certificates	
revocationDate		M	D	Date when revocation was processed by the CA	UTC time of revocation
crlEntryExtension	False	O			
CRLReason		M	S	As per RFC 5280	Identifies the reason for the certificate revocation
Invalidity Date		O	S	Date when the certificate is supposed to be invalid	Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
CRLExtensions	False	M			
AuthorityKeyIdentifier	False	M	D	SHA-1 Hash	160-bit SHA-1 hash of subjectPublicKey of the issuing CA public key
CRL Number	False	M	D		Sequential CRL Number
expiredCertsOnCRL	False	O	D		< a date-time value specifies the date on or after which revoked certificates are retained on the CRL>
AuthorityInfoAccess	False	O			
AccessMethod		M	S	Id-ad-2 2 id-ad-caIssuers OID	

					i.e.,1.3.6.1.5.5.7.48.2 (ca cert)	
	AccessLocation		M	S	http://repository-ecac.pki.gov.pk/repository/cert/[root or intermediate ca].p7b	CA Certificate download URL over HTTP

Client Auth Root CA CARL

*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 Client Auth Root 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

Code Signing Root CA CARL

*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 Code Signing Root 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

S/MIME Root CA CARL

*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 Root 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

TLS Root CA CARL

*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 TLS Root 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

TSA Root CA CARL

*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 TSA Root 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 ECAC CAs support X509 v2 CRLs.

7.2.2 CRL and CRL Entry Extensions

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

7.3 OCSP Profile

legacy Root CA OCSP

OCSP Response Signing Certificate Profile					
Field	CE[2]	O/M[3]	CO[4]	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	CA's Signature.	CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False				
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M	S	<Issuing CA's Subject>	The issuer field is defined as the X.501 type "Name"
CountryName				PK	Encoded according to "ISO 3166-1-alpha-2 code elements".

					PrintableString, size 2 (rfc5280)
OrganizationName				Electronic Certification Accreditation Council	PrintableString
CommonName				CN of the ECAC CAs	PrintableString
Validity	False	M			Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
NotBefore		M	D	Certificate generation process date/time.	
NotAfter		M	D	Certificate generation process date/time + **[12]** Months	12 months
Subject	False	M	D		
CountryName		M		PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M		Electronic Certification Accreditation Council	PrintableString
stateOrProvinceName		M	S	Pakistan	PrintableString
CommonName		M		**For Gov. SMIME CA:** "ECAC Government SMIME CA OCSP - 2023" **For Gov. Client Auth CA:** "ECAC Government Client Authentication CA OCSP - 2023" **For Gov. TLS CA:**	PrintableString

				"ECAC Government TLS CA OCSP - 2023" **For Gov. Code Signing CA:** "ECAC Government Code Signing CA OCSP – 2023" **For Gov. Timestamping CA:** "ECAC Government Timestamping CA OCSP - 2023" **For Comm. SMIME CA:** "ECAC Commercial SMIME CA OCSP - 2023" **For Comm. Client Auth CA:** "ECAC Commercial Client Authentication CA OCSP - 2023" **For Comm. TLS CA:** "ECAC Commercial TLS CA OCSP - 2023" **For Comm. Code Signing CA:** "ECAC Commercial Code Signing CA OCSP - 2023" **For Comm. Timestamping CA:** "ECAC Commercial Timestamping CA OCSP - 2023"	
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	S	RSA	
SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	

Extensions		M			
Subject Properties					
SubjectKeyIdentifier	False	M			
KeyIdentifier		M	D	SHA-1 Hash	160-bit SHA-1 hash of subjectPublicKey
Policy Properties					
keyUsage	True	M			
digitalSignature		M	S	True	
nonRepudiation		M	S	True	
extKeyUsage	False	M			
id-kp-OCSPSigning		M	S	True	
id-pkix-ocsp-nocheck	False	M			
certificatePolicies	False	M			
PolicyIdentifier		M	S	1.3.6.1.4.1.59337.1.1	
policyQualifiers:policyQualifierId		O	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		O	D	https://ecac.pki.gov.pk/repository/cps	

Client Auth Root 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 Client Auth Root 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 Client Auth Root 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			

Code Signing Root 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 Code Signing Root 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 Code Signing Root 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			

S/MIME Root 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 Root 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 Root 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			

TLS Root 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 TLS Root 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 TLS Root 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			

TSA Root 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 TSA Root 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 TSA Root 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)

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

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

The PMA audit function conducts internal audits at least annually, which encompass the NR-CAs 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 planned and executed by an independent WebTrust practitioner according to the WebTrust audit scheme. The period during which the CA issues Certificates is divided into a contiguous sequence of audit periods. An audit period do not exceed 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 - SSL Baseline
- WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements
- WebTrust Principles and Criteria for Certification Authorities – Network Security
- WebTrust Principles and Criteria for Certification Authorities – S/MIME

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 NR-CAs 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

The ECAC PMA, through its compliance function, monitors and strictly controls its adherence to the procedures listed in this CP/CPS document and to the Baseline Requirements by performing self-audits at least a yearly.

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

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

9.1.5 Refund Policy

No refund will be made for any charged fee.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

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

9.2.2 Other Assets

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

9.2.3 Insurance or Warranty Coverage for End-Entities

Refer to section 9.6.1.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The ECAC considers the following as confidential information:

- Subscriber's personal information that are not part of certificates or CRLs
- Correspondence between and the RA function during the certificate management processing (including the collected subscriber's data)
- Contractual agreements between the ECAC and its suppliers
- ECAC internal documentation (business processes, operational processes, ….)
- Employees confidential information

9.3.2 Information Not within the Scope of Confidential Information

Any information not defined as confidential (refer to section 9.3.1) is deemed public. This includes the information published on the ECAC 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.

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

- Communications between the RA systems and the Subordinate CAs.
- Communications between the NR-CAs and the RA systems.
- Sessions to deliver certificates

9.4.2 Information Treated as Private

All personal information that is not publicly available in the content of a certificate or CRL are considered as private information.

9.4.3 Information Not Deemed Private

Information included in the certificate or CRL is not considered as private.

9.4.4 Responsibility to Protect Private Information

The ECAC employees, suppliers and contractors handle personal information in strict confidence under the ECAC contractual obligations that are at least as protective as the terms specified in Section 9.4.1.

9.4.5 Notice and Consent to Use Private Information

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

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

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The ECAC will not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. Refer to section 9.4.1 for more details.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

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

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

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

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

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

- All Application Software Suppliers with whom the IQ-NR-CA will enter into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
- All Relying Parties who reasonably rely on a valid certificate

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

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

- **Authorization for Certificate:** That, at the time of issuance of Subordinate CA certificate, the ECAC:
    i. implemented a procedure for verifying that the Subject authorized the issuance of the Subordinate CA Certificate, and that the TSP's Applicant

Representative is authorized to request the Certificate on behalf of the Subject,
ii. followed the procedure when issuing the Subordinate CA Certificate, and
iii. accurately described the procedure in this CP/CPS.

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

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

9.6.2 RA Representations and Warranties

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

9.6.3 Subscriber Representations and Warranties

- Note 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 Subordinate CA that is the party responsible for the ultimate correctness and accuracy of all data transmitted to the ECAC with the intention to be included in a CA certificate.
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificates or digital signatures.
- Willful misconduct of any third-party participant breaking any applicable laws in Pakistan, including, but not limited to those related to intellectual property protection, malicious software, and unlawful access to computer systems.
- For any damage suffered whether directly or indirectly because of an uncontrollable disruption of the ECAC services.
- Any form of misrepresentation of information by TSPs or relying parties on information contained in this CP/CPS or any other documentation made public by the PMA and related to the ECAC services.

9.8 Limitations of Liability

- To the extent the ECAC has issued and managed its certificates and Subordinate CAs in compliance with the present document, the ECAC shall have no liability to TSPs, Relying Parties and other third parties for any damages or losses suffered as a result of the use or reliance on such certificates issued by the ECAC.
- To the extent permitted by applicable law in Pakistan, the ECAC may only liable for damages which are the result of its legally provable negligence, fraud or willful misconduct.
- The ECAC will not incur any liability to Subordinate CAs or their Subscribers to the extent that such liability results from their negligence, fraud, or willful misconduct.
- The ECAC will not be liable to any party for any damage suffered whether directly or indirectly caused by force major events. The ECAC takes reasonable measures to mitigate the effects of force major in due time.
- TSP and their Subordinate CAs shall be responsible towards the ECAC for any damages resulting from TSPs negligence, fraud, willful misconduct and failure to meet the ECAC regulatory obligations.

- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations.

9.9 Indemnities

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

9.10 Term And Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

The ECAC PMA coordinates communications towards the 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 CP/CPS can be addressed to the ECAC PMA contact address as stated in section 1.5.

9.12 Amendments

When changes are required to be made on this CP/CPS. The ECAC PMA will incorporate such a 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 being published on the ECAC repository, the newer version of the CP/CPS becomes effective. The older versions of this document are archived on the ECAC CAs repository.

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

The ECAC PMA reserves the right to amend this CP/CPS without notification for amendments that are not material, including without limitation corrections of typographical errors or minor enhancements.

9.12.3 Circumstances under which OID Must Be Changed

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

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

- Electronic Transaction Ordinance, 2002

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate the ECAC CP/CPS or any of its rights or duties under this CP/CPS, without the prior written consent of the ECAC.

9.16.3 Severability

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

In the event of a conflict between the Baseline Requirements and any regulation in Pakistan, the ECAC may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in Pakistan. This applies only to operations or certificate issuances that are subject to that Law. In such event, the ECAC will immediately (and prior to issuing a certificate under the modified requirement) include in this section a detailed reference to the Law requiring a modification of the Baseline Requirements under this section, and the specific modification to the Baseline Requirements implemented by the ECAC. The ECAC will also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CP/CPS. Any modification to the ECAC practice enabled under this section will be discontinued if and when the Law no longer applies, or the Baseline Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to this CP/CPS and a notice to the CA/Browser Forum, as outlined above, is made within 90 days.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

The ECAC shall not be liable for any failure or delay in their performance under the provisions of this CP/CPS due to causes that are beyond their reasonable control, including, but not limited to unavailability of interruption or delay in telecommunications services.

9.17 Other Provisions

No stipulation.