Pakistan National PKI

ECAC TLS Subordinate CAs Certificate Practice Statement

Version control

Version	Date	Description / Status	Responsible
V2.0	25/11/2024	Initial version after the changes in the PKI hierarchy and ECAC's intermediate CAs /NTC CAs termination for review & approval	ECAC
V2.1	20/02/2025	Introducing the Multi-Perspective Issuance Corroboration	ECAC
V2.2	25/02/2025	Extend ECAC's certificate issuance scope to include commercial domains.	ECAC
V2.3	21/04/2025	Amended to align with the requirements of Root Store programs and incorporate feedback received from auditors	ECAC

Document Signoff

Version	Date	Responsible	Validated By	Reviewed and Approved By
V2.3	/ /2025	ECAC	ECAC (PMA)	ECAC (PMA)

Table of Contents

1 Introduction

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

This CPS addresses the technical, procedural, and organizational policies of the TLS Subordinate CAs that are established and operated by ECAC under the Pakistan national PKI hierarchy, with regards to the complete lifetime of certificates issued by these CAs.

In this document, the word "Subordinate CAs" refer to the ECAC TLS Subordinate CAs intended to issue organization validation (OV) certificates and extended validation (EV) SSL certificates in accordance with CA/Browser Forum BR and EV guidelines

This CPS complies with the formal requirements of the Internet Engineering Task Force (IETF) RFC 3647 with regards to format and content. While certain section titles are included according to the structure of RFC 3647, the topic may not necessarily apply in the implementation of the ECAC TLS Subordinate CAs. Such sections are denoted as "Not applicable". Additional information is presented in subsections of the standard structure where required.

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

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

- WebTrust Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities - SSL Baseline
- WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL
- WebTrust Principles and Criteria for Certification Authorities – Network Security

The ECAC's Policy Management Authority (PMA) is committed to maintain this CPS in conformance with the current versions of the requirements below published at 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

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

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

1.1 Overview

The Pakistan National PKI aims to provide digital certification and trust services to government and 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[1] are:

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

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

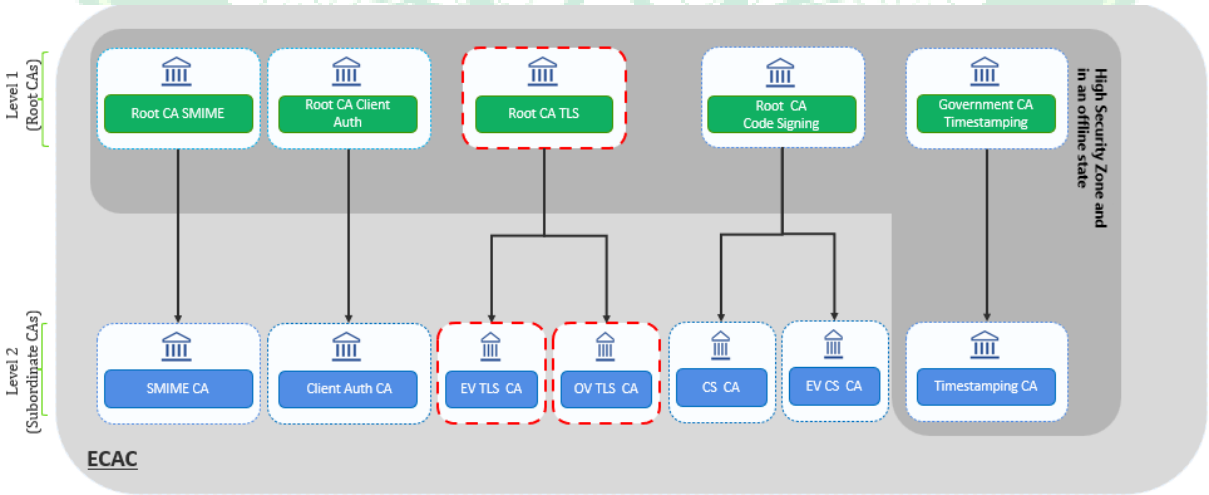

Figure 1 - Pakistan national PKI hierarchy

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

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

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

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

1.1.1 Overview of ECAC Policy Management Authority (PMA)

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

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

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

- **Responsible for the operations of the NR-CAs and their Subordinate CAs (owned by ECAC):** The ECAC runs the Registration Authority (RA) function as well as the technical operations of the NR-CAs and their Subordinate CAs under 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-known WebTrust accreditation. With this accreditation, the Pakistan national PKI (NR-CAs) would be eligible for enrollment into the "commercial" root programs (e.g., browsers and operating systems).
- **Driving PKI Promotion in Pakistan:** The ECAC PMA contributes to awareness programs, collaboration working groups, and supporting taskforces.
- **Contributing to PKI Laws and Decrees:** The ECAC PMA contributes to improving the local laws and decrees in relation to PKI and Trust Services leveraging its practical experience with TSPs as well as its exposure to international regularity authorities, service providers and "commercial" root-signing programs.
- **Oversees the Commercial & Government TSPs in Pakistan:** The ECAC PMA manages the licensing of Commercial and Government TSPs under the national TSP accreditation framework. It accordingly approves, maintains, and publishes the list of approved TSPs/TS under the national TSP accreditation framework.

1.2 Document Name and Identification

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

The ECAC CAs will use the OID **1.3.6.1.4.1.59337.1.4** to identify this document.

1.3 PKI Participants

1.3.1 Certification Authorities

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

These CAs provides the following certification services:

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

- **Certificate Validity Status Service —** it provides certificate validity status information to relying parties based upon certificate revocation lists and an OCSP responder service. The status information always reflects the current status of the certificates issued by these CAs.

1.3.2 Registration Authorities

A Registration Authority (RA) is the entity that performs the identification and authentication of certificate applicants for end-user certificates, initiates, or forwards revocation requests, and approves applications for certificate issuance and renewal on behalf of the CA.

ECAC operates its own Registration Authority (RA) function and does not rely on Delegated Third Parties for RA functions. The RA function primarily processes TLS certification requests for certificates issued to the legal organizations.

The RA function falls within the PKI operations structure. The RA officers are responsible for identity validation and certificate request management for legal entities according to the procedures outlined in section 4.2.

The RA function includes but not limited to:

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

ECAC does not delegate the validation process of domain ownership or control to any third-party RA. This process is performed only by RA officers' team of ECAC.

1.3.3 Subscribers

Subscribers are the legal representatives of legal entities, including government and non-government entities, as well as ECAC itself under Pakistan jurisdiction, with sufficient powers of attorney. They apply for OV SSL and/or EV SSL certificates from the corresponding Subordinate CAs and commit to adhering to the applicable Subscriber Agreement.

1.3.4 Relying Parties

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

1.3.5 Other Participants

Other Participants include:

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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

1) **Web Server TLS certificates**:
   a) **(Organization validated) OV Certificates:** Used for server authentication and session data encryption with a moderate level of trust compared to EV certificates, suitable for business websites and portals.
   b) **(Extended validated) EV Certificates:** Used for server authentication and session data encryption with the highest level of trust, making it ideal for banking, e-commerce, and other sites handling sensitive transactions.
2) **OCSP Responder Certificates –** used to sign the Online Certificate Status Protocol (OCSP) responses for certificates issued by these CAs.

1.4.2 Prohibited Certificate Uses

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

1.5 Policy Administration

1.5.1 Organization Administering the Document

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

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

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

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

1.5.2 Contact Person

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

Policy Management Authority
Electronic Certification Accreditation Council (ECAC),
5th Floor NTC HQ Building, G-5/2,
Islamabad, Pakistan
Tel: +92 51 9245739
Email: ecac.certification.info@pki.gov.pk

The ECAC PMA accepts comments regarding the present document only when they are addressed to the contact above.

Certificate Problem Report

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

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

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

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS Approval Procedures

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

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

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

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

1.6 Definitions and Acronyms

1.6.1 Definitions

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

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under commoncontrolwith another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. In context of this CPS, Subordinate CAs issue certificates exclusively to legal entities.

Applicant Representative – A natural person 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 a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA. In the context of this CPS, the applicant representative is in charge of submitting certificate requests and certificate revocation requests on behalf of the applicant. The words Applicant representative and requester are used interchangeably.

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 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).

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

Authorization DomainName: The FQDN used to obtain authorization for a given FQDN to be included in a Certificate. The CA may use the FQDN returned from a DNS CNAMElookupasthe FQDN for the purposes of domain validation. If a Wildcard Domain Name is to be included in a Certificate, then the CA MUST remove "*." from the left-most portion of the Wildcard Domain Nametoyield the corresponding FQDN. The CA may prune zero or more Domain Labels of the FQDN from left to right until encountering a Base Domain Name and may use any one of the values that were yielded by pruning (including the Base Domain Name itself) for the purpose of domain validation.

Authorized Ports: One of the following ports: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Base Domain Name: The portion of an applied-for FQDN that is the first Domain Name node left of a registry-controlled or public suffix plus the registry-controlled or public suffix (e.g. "example.co.uk" or "example.com"). For FQDNs where the right-most Domain Name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base DomainName.

CAA: From RFC 8659 (https://tools.ietf.org/html/rfc8659): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify one or more Certification Authorities (CAs) authorized to issue certificates for that domain name. CAA Resource Records allow a public CA to implement additional controls to reduce the risk of unintended certificate mis-issue."

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 Data: Certificate requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates

Certificate Policy (CP) – A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report – Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Revocation List – A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

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

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

Certificate Profile – A set of documents or files that define requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g. Section 7 in the present document provides a list of the certificate profiles defined within it.

Control – "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

Country – Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations.

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

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

DNS CAA EmailContact: The email address defined in Appendix A.1.1 of the Basline Requirements.

DNS CAA Phone Contact: The phone number defined in AppendixA.1.2. of the Basline Requirements.

DNS TXT Record Email Contact: The email address defined in Appendix A.2.1. of the Basline Requirements.

DNS TXT Record Phone Contact: The phone number defined in Appendix A.2.2. of the Basline Requirements.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contact (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Label: From RFC 8499(https://tools.ietf.org/html/rfc8499): "An ordered list of zero or more octets that makes up a portion of a domain name. Using graph theory, a label identifies one node in aportion of the graph of all possible domain names."

DomainName: An ordered list of one or more Domain Labels assigned to a node in the Domain NameSystem.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with:

i. the Internet Corporation for Assigned Names and Numbers (ICANN),
ii. a national Domain Name authority/registry, or
iii. a Network Information Center (including their affiliates, contractors, delegates, successors, or assignees

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

Fully-Qualified Domain Name: A Domain Name that includes the Domain Labels of all superior nodes in the Internet Domain Name System.

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

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database

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

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC)

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.

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

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.

LDH Label: From RFC5890(https://tools.ietf.org/html/rfc5890): "A string consisting of ASCII letters, digits, and the hyphen with the further restriction that the hyphen cannot appear at the beginning or end of the string. Like all DNS labels, its total length must not exceed 63 octets."

Legal Entity – An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

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

Multi-Perspective Issuance Corroboration: A process by which the determinations made during domain validation and CAA checking by the Primary Network Perspective are corroborated by other Network Perspectives before Certificate issuance.

NetworkPerspective: Related to Multi-Perspective Issuance Corroboration. A system (e.g., a cloud-hosted server instance) or collection of network components (e.g., a VPN and corresponding infrastructure) for sending outbound Internet traffic associated with a domain control validation method and/or CAA check. The location of a Network Perspective is determined by the point where unencapsulated outbound Internet traffic is typically first handed off to the network infrastructure providing Internet connectivity to that perspective.

Non-Reserved LDH Label: From RFC 5890(https://tools.ietf.org/html/rfc5890): "The set of valid LDH labels that do not have '--' in the third and fourth positions."

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.

Onion Domain Name: A Fully Qualified Domain Name ending with the RFC 7686 ".onion" Special-Use Domain Name. For example, 2gzyxa5ihm7nsggfxnu52rck2vv4rvmdlkiu3zzui5du4xyclen53wid.onion is an Onion

Domain Name, whereas torproject.org is not an Onion Domain Name.

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.

Primary Network Perspective: The Network Perspective used by the CA to make the determination of 1) the CA's authority to issue a Certificate for the requested domain(s) or IP address(es) and 2) the Applicant's authority and/or domain authorization or control of the requested domain(s) or IP address(es)

Private Key – The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key – The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure – A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Publicly Trusted Certificate – A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor – A natural person or Legal Entity that meets the requirements of Section 8.2.

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

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

Registration Authority (RA) – Any Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA. In the context of this CPS, the RA function is operated by ECAC.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

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

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

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

Request Token: A value, derived in a method specified by the CA which binds this demonstration of control to the certificate request. Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; or (ii) a hash of the Subject Public Key Info [X.509]; or (iii) a hash of a PKCS#10 CSR

Reserved IP Address: An IPv4 or IPv6 address that is contained in the address block of any entry in either of the following IANA registries: https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

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.

Short-lived Subscriber Certificate: For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 7 days (604,800 seconds).

Subject – The entity, or organization defined in the "Subject" field in a Certificate.

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 CPS, the Subordinate CAs, are signed by TLS Root CA.

Subscriber – A Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

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

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.

Test Certificate: This term is no longer used in these Baseline Requirements.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Unregistered DomainName: A Domain Name that is not a Registered Domain Name

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

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

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

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPSwebsite.

Wildcard Certificate: A Certificate containing at least one Wildcard Domain Name in the Subject Alternative Names in the Certificate.

XN-Label: From RFC 5890 (https://tools.ietf.org/html/rfc5890): "The class of labels that begin with the prefix "xn--" (case independent) but otherwise conform to the rules for LDH labels."

See EV guideline for additional definitions.

1.6.2 Acronyms

AICPA	American Institute of Certified Public Accountants
ADN	Authorization Domain Name
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain

CICA	Canadian Institute of Chartered Accountants
CCTV	Closed Circuit TV
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	DomainNameSystem
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
CSR	Certificate Signing Request
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
NIST	(US Government) National Institute of Standards and Technology
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
VoIP	Voice Over Internet Protocol

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 – Network Security
- 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
- 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.

ECAC hosts test Web pages that allow application developers to test their developed software with Subscriber Certificates. Below are test Web pages for valid, revoked, and expired certificates:

OV certificates	EV Certificates
Valid certificates: https://good.pki.gov.pk Revoked certificates: https://revoked.pki.gov.pk Expired certificates: https://expired.pki.gov.pk	Valid certificates: https://ev-good.pki.gov.pk Revoked certificates: https://ev-revoked.pki.gov.pk Expired certificates: https://ev-expired.pki.gov.pk

2.3 Time or Frequency of Publication

The PMA reviews this CPS at least once annually and makes appropriate changes so that the Subordinate CAs' operations remain fully aligned to the requirements listed in section 1 of this CPS. In instances where no changes are required, the CPS version number is incremented, and a dated changelog entry is included to document the review.

Modified versions of the CPS and agreements (Subscriber and Relying party) are published within five days after the PMA approval.

2.3.1 CA Certificates

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

2.3.2 CRLs

This Subordinate CAs maintain and publish CRLs as follows:

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

This subordinates CAs continues issuing CRLs until one of the following conditions is met:

- all Subordinate CA Certificates containing the same Subject Public Key are expired or revoked; OR
- the corresponding Subordinate CA Private Key is destroyed

2.4 Access Controls on Repositories

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

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

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

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

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

3.1.1.1 ECAC's TLS Subordinate CAs

The DN format allowed for the ECAC TLS subordinate CAs are:

OV TLS CA certificate

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

Table 1 – ECAC OV TLS Distinguished Name

EV TLS CA certificate

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

Table 1 – ECAC EV TLS Distinguished Name

3.1.1.2 Subscriber certificates

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

OV certificates

Attribute	Value
Country – "C"	PK
S (optional if L is present, otherwise mandatory)	which is the state or province of the organization's place of business.
L (optional if S is present, otherwise mandatory)	which is the city or locality of the organization's place of business.
O	full registered name of the organization to which the certificate is issued

EV certificate

Attribute	Value
Country – "C"	PK
S (optional if L is present, otherwise mandatory)	the province where the organization is established
L (optional if S is present, otherwise mandatory)	name of the locality where the organization is established
O	full registered name of organization to which the certificate is issued
businessCategory	subject business category as defined in EV guideline
jurisdictionCountryName	PK
jurisdictionStateOrProvinceName (Optional)	MUST be specified using the full name of the applicable jurisdiction.
jurisdictionLocalityName (Optional)	MUST be specified using the full name of the applicable jurisdiction.
serialNumber	Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme. As defined in EV guideline.

3.1.1.3 OCSP certificates

OV TLS CA OCSP

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

EV TLS CA OCSP

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

3.1.2 Need for Names to be Meaningful

The Certificates issued pursuant to this CPS are meaningful only if the names that appear in the Certificates can be understood and used by Relying Parties. Distinguished Names (DN) are used to identify both the subject and the issuer of the certificate in a meaningful way. Hence, the Subordinate CAs issues certificates to subscribers (subjects) that

demonstrate legitimately ownership and control on the domain names, IP addresses, mentioned in the Subject DN.

For EV TLS Certificates: The FQDN for an EV SSL Certificate cannot be an IP Address or a Wildcard Domain Name.

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

3.1.3 Anonymity or Pseudonymity of Subscribers

This CPS does not permit anonymous or pseudonymous subscribers.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

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.

Uniqueness is enforced through the use of registered public DNS name (FQDNs) or public IP addresses. the Subject Alternative Name (SubjectAltName) extension must be used to define the applicable domain and one or more additional domain names for the certificate. The usage of internal domain names and reserved IP addresses[2] is prohibited.

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

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

3.1.6 Recognition, Authentication, and Role of Trademarks

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

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

[2] The FQDN for an EV SSL Certificate cannot be an IP Address or a Wildcard Domain Name.

3.2 Initial Identity Validation

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

The RA verifies and authenticates the identity and other attributes of an Applicant prior to inclusion of these attributes in a Certificate. RA may refuse to issue a certificate at its sole discretion if identity validation is not successful

3.2.1 Method to Prove Possession of Private Key

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

3.2.2 Authentication of Organization Identity

3.2.2.1 Organization Identity

Authentication of an organization identity is performed pursuant to current Pakistan legislation through the validation processes specified below, by which the RA officer performs initial identity validation of the organization and its representatives and enrols the organization in the Web RA portal.

The RA ensures that any obtained validation data will be recollected and validated not more than 398 days after the last performed verifications.

For OV TLS certificate:

The applicant's organizational identity is verified using reliable and authoritative data sources. These sources are expected to provide detailed information about the entity, including its legal name, address, and the authorized representative's information.

The ECAC RA officer verifies the organization's legal existence, identity, legal name, organization identifier, address, and a reliable method of communication. This information may be verified using one of the following validation methods:

- For government entities: ECAC will rely on the Government Gazette, Law, Ordinance, Regulations, or Rules of Business, which are regarded as reliable data sources for verifying and validating the information provided in the applicant's submitted documentation.
- For non-government entities: ECAC will consider official documentation provided by the entity and use the Securities and Exchange Commission of Pakistan (SECP) (https://eservices.secp.gov.pk/eServices/NameSearch.jsp) and the Federal Board of Revenue (https://Iris.fbr.gov.pk) databases , which is periodically updated and considered a reliable data source in Pakistan.

Additionally, the RA officer may conduct a site visit to verify the entity's address.

The RA officer also validates the applicant's right to use the domain name(s) listed in the certificate by following the procedures outlined in Section 3.2.2.4.

To verify the association with the certificate subject, the RA officer ensures that the information provided in the application form matches exactly with the details to be inserted into the certificate.

Furthermore, the RA officer takes reasonable steps to establish that a certificate request made on behalf of an organization is legitimate and duly authorized. The authority of the person requesting the certificate is verified in accordance with Section 3.2.5.

For EV TLS certificate:

For EV TLS certificate, the RA officer conducts additional verifications related to legal, physical and operational existence of the organization according to section 3.2.2 of the EV guidelines, where the following will be determined:

- Applicant's Existence and Identity
  - Applicant's legal existence and identity.
  - Applicant's physical existence (business presence at a physical address).
  - Applicant's operational existence (business activity).
- Applicant's control, of the Domain Name(s) to be included in the EV Certificate
- Verified Method of Communication with the Applicant
- Applicant's authorization for the EV Certificate, including:
  - The Name, Title, and Authority of Contract Signer and Certificate Approver, and certificate requester.
  - Signature on Subscriber Agreement and EV Certificate Requests
- Approval of EV Certificate Request.

3.2.2.2 DBA/Tradename

The use of DBA or Tradename in the Subject Identity Information is not supported by the Subordinate CAs.

3.2.2.3 Verification of country

These Subordinate CAs issues certificates only to legal entity established in Pakistan. The RA officer verifies that the value of the "country" field of the Subject Identity Information is set to "**PK**"

3.2.2.4 Validation of Domain Authorization or Control

For each domain name to be included in the Certificate Subject, the RA verifies the Applicant's control of the domain name in accordance with the Baseline Requirements, Section 3.2.2.4. The RA also maintains a record of the method used for verification,

including relevant BR version number, he used to validate every domain. This verification is performed using one of the following approved methods for each Fully Qualified Domain Name (FQDN):

- Email validation consisting of sending an e-mail with a random, unique value (valid for no more than 30 days from its creation) to an administrative e-mail address associated with the domain name (i.e. admin@organization.pk). This validation may be performed using following e-mail addresses: admin@, administrator@, webmaster@, hostmaster@, postmaster@. (BR Section 3.2.2.4.4)
- Domain Name Service (DNS) change by confirming the presence of a unique random value or request token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character. (BR Section 3.2.2.4.7).
  This method must be executed from a primary network perspective (the same network set as CA operations) and from a remote network perspective (a different network set than CA operations) as part of the implementation of Multi-Perspective Issuance Corroboration (as specfied in 3.2.2.9). For the remote network perspective to be considered corroborating and to serve as permission to issue certificates, the RA officer MUST observe the same challenge information (e.g., Random Value or Request Token) as the primary network perspective.

ECAC don't issue TLS certificates to ".onion" domains.

3.2.2.5 Authentication for an IP Address

For OV TLS certificates

Ownership of the IP Address (es) to be added in the certificate is verified through the following methods:

- **Agreed-Upon Change to Website:** Having the Applicant demonstrate control over the requested IP Address (es) by confirming the presence of a Random Value within a file under the "/well-known/pki-validation" directory on an Authorization IP Address that is accessible by the CA via HTTP/HTTPS over an Authorized Port. (BR Section 3.2.2.5.1).
  This method must be executed from a primary network perspective (the same network set as CA operations) and from a remote network perspective (a different network set than CA operations) as part of the implementation of Multi-Perspective Issuance Corroboration (as specfied in 3.2.2.9). For the remote network perspective to be considered corroborating and to serve as permission to issue certificates, the RA officer MUST observe the same challenge information (e.g., Random Value or Request Token) as the primary network perspective.

- **Reverse Address Lookup**: Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name using the supported methods. (BR Section 3.2.2.5.3).

This method must be executed from a primary network perspective (the same network set as CA operations) and from a remote network perspective (a different network set than CA operations) as part of the implementation of Multi-Perspective Issuance Corroboration (as specfied in 3.2.2.9). To count as corroborating, a Network Perspective MUST observe the same FQDN as the Primary Network Perspective.

For EV TLS certificates

IP addresses are not permitted for EV Certificates.

3.2.2.6 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in the CN or subjectAltName, the following validations apply:

1. Wildcard SSL Certificates include a wildcard asterisk character as the first character in the Common Name (CN) attribute of the Subject field and or in the SubjectAltName extension;
2. The wildcard asterisk character must not fall within the label immediately to the left of a registry-controlled or public suffix;
3. Certificate issuance is accepted only if the applicant proves its rightful control of the entire Domain Namespace. (e.g. the RA officer MUST NOT issue "*.co.pk" or "*.local", but MAY issue "*.example.pk" to Example entity).

Wildcard domain names are not permitted for EV certificates.

3.2.2.7 Data Source Accuracy

Prior to using any data source as a Reliable Data Source, ECAC evaluates the source for its reliability, accuracy, and resistance to alteration or falsification. Criteria for this evaluation shall include:

- The age of the information provided
- The frequency of updates to the information source
- The data provider and purpose of the data collection
- The public accessibility of the data availability, and
- The relative difficulty in falsifying or altering the data

3.2.2.8 CAA records

The CAA is a special DNS record that a domain owner can configure to specify which CA is allowed to issue a certificate for that domain.

For each domain that is included in the subjectAltName extension, the ECAC RA officer checks that a CAA record exists:

- if existent whether the 'issue' and 'issuewild' tags contain "ecac.pki.gov.pk", the ECAC RA officer ensures that the certificate is issued within the Time to Live (TTL) of the CAA record, or 8 hours, whichever is greater,

- If it the CAA record exists while it does not contain the "ecac.pki.gov.pk", then the ECAC RA officer will never issue a certificate for this domain.
- processes but does not act on iodef property tag (i.e., ECAC RA officer does not use iodef property tag of the CAA record for communicating with the contact(s) stipulated in the CAA iodef record(s)).

Some methods relied upon for validating the Applicant's ownership or control of the subject domain(s) (see Section 3.2.2.4) or IP address(es) (see Section 3.2.2.5) to be listed in a certificate require CAA records to be retrieved and processed from additional remote Network Perspectives before Certificate issuance (see Section 3.2.2.9). To corroborate the Primary Network Perspective, a remote Network Perspective's CAA check response MUST be interpreted as permission to issue, regardless of whether the responses from both Perspectives are byte-for-byte identical.

Additionally, the ECAC RA officer MAY consider the response from a remote Network Perspective as corroborating if one or both of the Perspectives experience an acceptable CAA record lookup failure, as defined in this section.

The ECAC RA officer MAY check CAA records at any other time.

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

3.2.2.9 Multi-Perspective Issuance Corroboration

Multi-Perspective Issuance Corroboration attempts to corroborate the determinations (i.e., domain validation pass/fail, CAA permission/prohibition) made by the Primary Network Perspective from multiple remote Network Perspectives before Certificate issuance.

ECAC uses different sets of Network Perspectives when performing MultiPerspective Issuance Corroboration for the required:

1. Domain Authorization or Control and
2. CAA Record checks

The set of responses from the relied upon Network Perspectives provides ECAC with the necessary information to allow it to affirmatively assess: -**a**. The presence of the expected: 1) Random Value; 2) Request Token; 3) IP Address; or 4) Contact Address, as required by the relied upon validation method specified in Sections 3.2.2.4 and 3.2.2.5 of this CP/CPS; and -**b**. ECAC's authority to issue to the requested domain(s), as specified in Section 3.2.2.8

Results or information obtained from one Network Perspective will not be reused or cached when performing validation through subsequent Network Perspectives (e.g., different Network Perspectives cannot rely on a shared DNS cache to prevent an adversary with control of traffic from one Network Perspective from poisoning the DNS cache used by other Network Perspectives).

The network infrastructure providing Internet connectivity to a Network Perspective MAY be administered by the same organization providing the computational services required to operate the Network Perspective. All communications between a remote Network Perspective and ECAC will take place over an authenticated and encrypted channel relying on modern protocols (e.g., over HTTPS).

A Network Perspective can use a recursive DNS resolver that is not co-located with the Network Perspective. However, the DNS resolver used by the Network Perspective will fall within the same Regional Internet Registry service region as the Network Perspective relying upon it. Furthermore, for any pair of DNS resolvers used on a Multi-Perspective Issuance Corroboration attempt, the straight-line distance between the two DNS resolvers will be at least 500 km. The location of a DNS resolver is determined by the point where unencapsulated outbound DNS queries are typically first handed off to the network infrastructure providing Internet connectivity to that DNS resolver.

ECAC may immediately retry Multi-Perspective Issuance Corroboration using the same validation method or an alternative method (e.g., ECAC can immediately retry validation using “Email to DNS TXT Contact” if “Agreed-Upon Change to Website - ACME” does not corroborate the outcome of Multi-Perspective Issuance Corroboration). When retrying Multi-Perspective Issuance Corroboration, ECAC must not rely on corroborations from previous attempts. There is no stipulation regarding the maximum number of validation attempts that may be performed in any period of time.

The "Quorum Requirements" Table describes quorum requirements related to Multi-Perspective Issuance Corroboration. If ECAC does not rely on the same set of Network Perspectives for both Domain Authorization or Control and CAA Record checks, the quorum requirements will be met for both sets of Network Perspectives (i.e.,the Domain Authorization or Control set and the CAA record check set). Network Perspectives are considered distinct when the straight-line distance between them is at least 500 km. Network Perspectives are considered "remote" when they are distinct from the Primary Network Perspective and the other Network Perspectives represented in a quorum.

ECAC may reuse corroborating evidence for CAA record quorum compliance for a maximum of 398 days. After issuing a Certificate to a domain, remote Network Perspectives may omit retrieving and processing CAA records for the same domain or its subdomains in subsequent Certificate requests from the same Applicant for up to a maximum of 398 days.

Quorum Requirements Table

# of Distinct Remote Network Perspectives Used	# of Allowed non-Corroborations
2-5	1
6+	2

Remote Network Perspectives performing Multi-Perspective Issuance Corroboration must rely upon networks (e.g., Internet Service Providers or Cloud Provider Networks) implementing measures to mitigate BGP routing incidents in the global Internet routing system for providing internet connectivity to the Network Perspective.

For TLS Certificates issued on or after March 15th, 2025, ECAC will require Multi-Perspective Issuance Corroboration using at least two (2) remote Network Perspectives. ECAC MUST ensure that the requirements defined in QuorumRequirements Table are satisfied. If the requirements are not satisfied, then the ECAC will NOT proceed with the issuance of the Certificate.

3.2.3 Authentication of Individual Identity

The Subordinate CAs do not issue certificates to individuals.

3.2.4 Non-verified Subscriber Information

All fields constituting the subscriber information written in the certificate are verified by the ECAC RA officer.

3.2.5 Validation of Authority

The organization's authorized representative nominates a certificate requester from the organization who undergoes the certificate request process with the RA officer. The Authorization of certificate requester is performed as follows with:

1. The RA officer conducts an identity proofing through an in-person identity verification of the Requester against his/her government government-issued ID Card. The actual ID card (not a copy) is presented by the Requester,
2. The RA officer uses the proof of employment (Attestation letter) received as part of the certificate application to validate the association between the Requester and the entity.
3. The RA officer 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,
4. The RA officer verifies the authority of the authorized representative through an authoritative source using a formal communication with the legal entity.

For EV certificates, the RA officer conducts additional verifications related to validation of Authority according to section 3.2.2.8 of the EV guidelines. This includes:

- Verification of Name, Title, and Authority of the authorized representative,
- Verification of Signature on Subscriber Agreement and EV Certificate Requests,
- Verification of approval of EV certificate request.

3.2.6 Criteria for Interoperation

No Stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Identification and authentication for re-keying is performed as initial registration, in addition to the below rules:

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

3.3.2 Identification and Authentication for Re-key after Revocation

Identification and authentication procedures for re-key after revocation is same as during initial certification.

3.4 Identification and Authentication for Revocation Request

The identification and authentication procedures of revocation requests involves a formal request from the authorized representative of the entity to which the certificate is issued. A revocation procedure is enforced by the RA officer. It encompasses:

- The signature of a revocation request form by an appropriately authorized representative.
- The verification of the identity of the requesters against the information available to the RA officer (provided during the subscriber registration)
- Communication with the entity to provide reasonable assurances that the entity's official representative authorized the revocation operation. Such communication, depending on the circumstances, may include one or more reliable method of communication such as telephone, e-mail or courier service.

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

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

The authorized certificate Requester can submit certificate requests on behalf of the organization or entity. The Requester is responsible for the accuracy of information submitted as part of the certificate application. The RA officer ensures the entity official representative approves the certificate request by signing and stamping the certificate request form and the appended subscriber agreement.

ECAC's Subordinate CAs does not issue Certificates to entities on an internal blacklist[3] of organizations from whom it will not accept certificate requests. This blacklist is queried by the RA officer whenever it receives any certificate request.

Additionally, ECAC's Subordinate CAs do not issue certificates to entities that appear on a government denied list maintained by Pakistan or that is located in a country with which the laws of Pakistan prohibit doing business.

For OCSP responder certificate: the RA officer and an authorized PKI administrator in trusted role oversee the execution of an internal operational ceremonies through which these certificates can be issued. They engage the PMA for approving the operational ceremony documentation and for validating the embedded certificate templates and naming conventions against the provisions of this CPS. The PMA authorizes the ceremony and confirms the list of involved trusted role staff.

4.1.2 Enrollment Process and Responsibilities

The CAs require each Applicant to submit a Certificate request and application information prior to issuing a Certificate. The RA officer authenticates all communication from an Applicant and ensures that the application form is filled and signed as expected.

- The applicant downloads the certificate application form with the subscriber agreement from the ECAC public repository.
- The certificate application form is filed and signed by the authorized representative of the entity (likewise, the subscriber agreement must be ratified);
- The relevant technical team from the entity generates a key pair according to the requirements of this CPS then create a Certificate Signing Request (CSR) using the approved certificate fields in the application form (e.g., DN attributes, key size, key type etc.). This CSR is handed over to the authorized certificate requester.
- The requester authenticates to the web RA portal (using multi-factor authentication) and submits the certificate application including:
    - Scanned copy of properly filled and signed application form.
    - The information and documents required for identification and authorization of the subject request.

[3] An internal blacklist in where the RA logs previously rejected certificate requests due to suspected or fraudulent usage and revoked certificate requests from entities.

- Certificate Signing Request (CSR) file.

- The RA officer reviews and validates the integrity and authenticity of all the submitted documents in addition to vetting the applicant identity as specified in section 3.2.2.
- The RA officer checks the blacklist of organizations from whom it will not accept certificate requests. This blacklist is queried by the RA officer whenever it receives any certificate request.
- The RA officer processes the certificate request. Refer to section 4.2.

For Extended Validation Certificates, separation of duties requires two members of the RA team to approve the request.

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

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Applicable Requirements for TLS certificates applications:

a) A unique ID is assigned to each certificate application record,

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

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

d) The RA officer conducts a blacklist check against its own blacklist. If the applicant is in the blacklist, the certification application is rejected,

e) The RA officer sends to the applicant the necessary information including the documentation required for identity verification and the subscriber agreement once the request is initiated by the applying entity.

f) The Requester fills-in the Organization registration form as follows:

   a. Organization Information
      i. Organization's Legal Name
      ii. Official Address
      iii. Main telephone number
   b. Authorized representatives Information:

i. applicant representative information such as phone, official email address, position.

c. Requester information

i. Name of and contact information of the Requester (the representative authorized to submit certificate management requests on behalf of the entity).

g) The applicant representative signs and ratifies a dedicated subscriber agreement.

h) An attestation letter issued by the entity HR establish the association between the Requester and the entity,

i) The Requester submits the signed registration form, the attestation letter as well as other validation documentation to the RA via email,

j) The RA officer performs the following verification for each certificate request without relying on previously performed verifications:

- Validates the organization's identity as described in section 3.2.2.1
- Validate the entity authorized representative as described in section 3.2.2.1,
- Verify the authorization of certificate Requestor as specified in section 3.2.5,
- Verify the phone number of the organization by making a random call.

If all the above validations are passed, the RA officer initiated a process on the Web RA Portal through which the entity and the Requester are registered on the portal based on the collected information. At this point the requester would be able to login to the Web RA Portal and submit certificate requests on behalf of his entity.

Once the certificate request has been submitted, the RA officer can proceed as follows:

k) Verify ownership of the domain names or IP addresses as specified in sections 3.2.2.4 and 3.2.2.5 of this CPS.

l) Corroborate the results of domain validation from multiple Network Perspectives, in accordance with section 3.2.2.9.

m) Verify the subject DN format (from CSR) and ensure that:

- The organization field value matches precisely the name of the entity as it was enrolled by the RA officer.
- A least one FQDN or IP address[4] is included in the certificate's SubjectAltName extension.

n) In case of wildcard certificates, conduct a Wildcard Domain Validation as specified in section 3.2.2.6 of this CPS,

[4] IP address and wildcard domain names are not permited for EV certificates.

o) Check for valid domain TLD that must be ".PK" For each domain that is included in the certificate request,
p) Verify the validity of TLD against the IANA published lists of valid TLD and gTLD (https://data.iana.org/TLD/tlds-alpha-by-domain.txt),
q) Check CAA records for the domain as specified in section 3.2.2.8 of this CPS.
r) Corroborate the results of CAA checks from multiple Network Perspectives, in accordance with sections 3.2.2.8 & 3.2.2.9.

Re-identification of the Applicant is not required for re-keying applications, provided that the previously submitted identification evidence remains valid and applicable. However, previously validated data may only be reused for a maximum of three hundred ninety-eight (398) days. After this period, the data must be revalidated as initial registration.

For OCSP responder certificate: The RA and an authorized PKI administrator in trusted role oversee the execution of PKI internal operational ceremonies through which any of these certificates can be issued. The PMA approves the operational ceremony documentation and validates the embedded certificate templates and naming conventions against the provisions of this CPS. The PMA authorizes then the ceremony and confirms the list of involved trusted role ceremony staff. The ceremony is executed under the supervision of the RA officer that reviews the CSR before its processing by the CA

4.2.2 Approval or Rejection of Certificate Applications

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

- Successful identification and authentication of all required Subscriber information according to Section 3.2.2
- Domain/IP ownership verification,
- Proof of association between the requesting organization and the subject to which the certificate will be issued,
- Proof of possession of private key,
- Identification and Authorization of the certificate request.

This CA does not issue publicly trusted SSL certificates to internal server name or reserved IP addresses

4.2.2.1 For EV certificates:

Prior to a determination of whether to approve or reject an application for an EV Certificate, the RA conducts other verification checks required by the EV Guidelines, known as:

4.2.2.1.1 Final Cross-Correlation and Due Diligence:

The approval of EV certificate issuance requires two RA officers. The second RA officer cannot be the same individual who collected the authentication documentation and originally approved the EV Certificate. The second RA officer reviews the collected information and documents for discrepancies or details that require further explanation. If the second RA officer has any concerns about the application, he may require additional

explanations and documents. If satisfactory explanations and/or additional documents are not received within a reasonable time, the RA officer will reject the EV Certificate request and notify the Applicant accordingly.

- The RA officer rejects any certificate application that he cannot verify. He may also reject a certificate application if he believes that issuing the certificate could damage ECAC's business.
- The RA Team performs the requirements of Final Cross-Correlation and Due Diligence through employees under its control and having appropriate languages skills, training, experience, and judgment in confirming organizational identification and authorization.
- When some or all of the documentation used to support the application is in a language other than English, and the RA employees do not possess the necessary language skills, the RA relies on language translations of the relevant portions of the documentation provided by a qualified Translator.
- Following successful completion of all required validations of a certificate application, the RA officer will approve an application for an EV Certificate.

The Subordinate CAs do not issue publicly trusted SSL certificates to internal server name or reserved IP addresses.

For OCSP certificates: A certificate application is approved by the PMA as part of the overall ECAC authorized internal operational ceremony.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Once all the validation is done as described in section 4.2.1, the RA team uses the web RA portal to initiate certificate issuance from the Subordinate CAs based on the CSR received from the applicant.

The Certification Authority (CA) will validate the format and structure of the Certificate Signing Request (CSR) and generate a corresponding pre-certificate. The pre-certificate will undergo linting using industry-standard tools to assess its technical conformity and compliance (of each to-be-signed artifact prior to signing it), with applicable standards. Following successful validation, the final certificate will be generated in accordance with the predefined configured certificate template and made available for download from the web RA portal. The CA issues the certificate in "**Active**" state.

Furthermore, TLS certificates are logged in two or more Certificate Transparency databases.

For OCSP responder certificate: The issuance and management of these certificates happen as part of operational ceremonies that are approved by at least two members of the PMA. These approvals establish the following: (1) authorizing the ceremony execution, (2) approving the list of ceremony attendees involving the RA officer, a

member of the PKI operations management, and designated administrators from the PKI operations team, (3) validating embedded certificate templates and naming conventions against the provisions of this CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The certificate is made available for download to the subscriber on his Web RA portal account.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Requester downloads the certificate from the web RA portal then validates its content against the certificate application/CSR. In case of any discrepancies, the Requester initiates a discussion with the ECAC's RA officer which may lead to certificate revocation to issue a corrected certificate.

The certificate is considered accepted by the organization if no complaints are raised by the Requester to the ECAC's RA within 10 business days of receiving the email notification of certificate generation.

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

4.4.2 Publication of the Certificate by the CA

The Subordinate CAs does not publish end-user certificates apart from sharing it with the requester.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The subscribers adhere to the following obligations:

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

Refer to section 9.6.3 of this CPS for complementary details.

4.5.2 Relying Party Public Key and Certificate Usage

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

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

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

4.6 Certificate Renewal

Certificate Renewal is the act of issuing a new certificate with a new validity period while the identifying information and the public key from the old certificate are duplicated in the new certificate. Certificate renewal is not supported by the Subordinate CAs. Only certificate re-key is supported.

4.6.1 Circumstance for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-Key

Certificate re-key refers to the issuance of a new certificate with a new subject public key for a subject to whom a certificate has previously been issued by the Subordinate CAs. Subject attributes and other certified attributes can be updated.

4.7.1 Circumstance for Certificate Re-Key

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

same type for the subscriber within a maximum of 5 business days from the issuance of the new certificate.

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 Subordinates 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 wants to get a new certificate, the Subscriber shall apply for a certificate re-key.

4.8.1 Circumstance for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

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

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

4.9.1 Circumstances for Revocation

4.9.1.1 Circumstances for Subscriber certificates revocation

Subordinate CAs does not support the revocation of Short-lived subscriber certificates.

With the exception of Short-lived Subscriber Certificates, Subordinate CAs revokes a certificate within 24 hours and use the corresponding CRLReason if one or more of the following occurs:

1. The Subscriber requests in writing, without specifying a CRLreason, that the CA revoke the Certificate (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
2. The subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization (CRLReason #9, privilegeWithdrawn).
3. The CA obtains reasonable evidence that the subscriber's private key, corresponding to the public key in the certificate suffered a key compromise (CRLReason #1, keyCompromise).
4. The CA obtains evidence that the validation of domain authorization or control for any FullyQualified Domain Name or IP address in the Certificate should not be relied upon (CRLReason #4, superseded).
5. The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate including but not limited to those identified in Section 6.1.1.2, (CRLReason #1, keyCompromise);

With the exception of Short-lived Subscriber Certificates, the Subordinate CAs may revoke a certificate within 24 hours and use the corresponding CRL Reason if one or more of the following occurs:

6. Obtaining evidence that the certificate no longer complies with the requirements of sections 6.1.5 and 6.1.6 (CRLReason #4, superseded).
7. Obtaining evidence that the certificate was misused (CRLReason #9, privilegeWithdrawn).
8. Knowing that a subscriber has violated one or more of its material obligations under the subscriber Agreement (CRLReason #9, privilegeWithdrawn).

9. Coming across any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name) (CRLReason #5, cessationOfOperation)
10. Knowing that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name (CRLReason #9, privilegeWithdrawn);
11. Made aware of a material change in the information contained in the Certificate (CRLReason #9, privilegeWithdrawn).
12. Discovering that the certificate was issued in a manner not in accordance with the procedures of this CPS and with the Baseline Requirements (CRLReason #4, superseded).
13. Knowing that any of the information contained in the certificate is inaccurate (CRLReason #9, privilegeWithdrawn).
14. This CA right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless this CA has planned to continue maintaining the CRL/OCSP Repository (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
15. Revocation is required by this CPS for a reason that is not otherwise required to be specified in this section 4.9.1 (CRLReason "unspecified (0)" which results in no reasonCode extension being provided in the CRL);
16. Discovering that there is a demonstrated or proven method that exposes the Subscriber's Private Key to compromise or if there is clear evidence that the specific method used to generate the Private Key was flawed (CRLReason #1, keyCompromise);

4.9.1.2 Circumstances for Subordinate CA revocation

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

1. The revocation is requested in writing;
2. Subordinate CAs notifies the Issuing CA (i.e., Root CA) that the original certificate request was not authorized and does not retroactively grant authorization;
3. Subordinate CAs obtains evidence that the CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Section 6.1.5 and Section 6.1.6;
4. The Issuing CA (i.e., Root CA) obtains evidence that the Subordinate CAs Certificates was misused;

5. The Issuing CA (i.e., Root CA) is made aware that the Subordinate CAs Certificates was not issued in accordance with or that Subordinate CAs has not complied with this document.
6. The Issuing CA (i.e., Root CA) determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. Subordinate CAs ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. Subordinate CAs ' right to issue Certificates under these Requirements expires or is revoked or terminated, unless the (i.e., Root CA) has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's (i.e., Root CA) Certificate Policy and/or Certification Practice Statement.

4.9.2 Who Can Request Revocation

Revocation can be requested by the following entities:

- The ECAC's RA in the cases described in section 4.9.1
- The Subscriber may submit a revocation request for his own certificate,
- ECAC at its own discretion (if for instance a compromise is known for the CA key),

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

4.9.3 Procedure for Revocation Request

Revocation of certificates is done as follows:

- The RA officer assigns a unique ID to the revocation request. The RA officer records the submitted documents under the assigned ID,
- The RA officer authenticates the requester's identity as described in section 3.4;
- The RA officer validates the certificate information in the revocation request form;
- The RA officer performs any required investigation within the applicable time constraints (as listed in section 4.9.1 of this CPS). This may include any required communication with the certificate subscriber,
- The RA team execute the certificate revocation.
- The Subordinate CsA revokes the certificate, and the certificate status is updated[5].
- The RA officer notifies via email the subscriber/the entity requested the revocation of the completion of the certificate revocation operation.
- The RA officer updates his internal blacklist with the details of the revoked certificate, circumstances for revocation and based on this information, potentially changes the risk profile of the applicant in the internal blacklist. Such

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

information will be queried by the RA officer prior to processing future certificate requests for the applicant.

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

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

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

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

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

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

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

If ECAC deems appropriate, it may forward the revocation reports to law enforcement.https://ecac.pki.gov.pk/repository/Certificate_Problem_Report.html

4.9.4 Revocation Request Grace Period

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

4.9.5 Time Within Which CA Must Process the Revocation Request

Certificate revocation requests are processed within 24 hours.

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

communication on the certificate problem is sent to the Subscriber and to the originator of the problem report.

The RA officer performs further investigations involving the PMA, the subscriber and other relevant authorities (e.g. law enforcement) to decide on the action to be taken on the subject certificate.

If the investigations results led to one of the certificate revocation circumstances listed in section 4.9.1, then the certificate will be revoked within the timeframe set forth in Section 4.9.1.

Based on the revocation circumstance, RA officer may agree with subscriber on a plan to issue a new certificate.

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 CRL Issuance Frequency (If Applicable)

CRLs is issued as per Section 2.3 of this CPS.

4.9.8 Maximum Latency for CRLs (if applicable)

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

4.9.9 On-Line Revocation/Status Checking Availability

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

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

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

4.9.10 On-Line Revocation Checking Requirements

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

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds

For the status of Subscriber Certificates:

- OCSP responses have a validity interval greater than or equal to eight hours;
- OCSP responses have a validity interval less than or equal to ten days;

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

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

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

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

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

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements Re Key Compromise

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

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

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

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

4.9.13 Circumstances for Suspension

Not Applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

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

4.10.1 Operational Characteristics

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

The Subordinate CA's OCSP responder exposes an HTTP interface that is also publicly available to relying parties.

Revocation entries in a CRL or OCSP response[6] remains until after the revoked certificate's Expiry Date.

4.10.2 Service Availability

The public repository where certificate information and CRLs are published is accessible 24 hours a day and 7 days a week and guarantees an uptime for at least 99.5% over one year period.

The ECAC's Subordinate CAs 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's Subordinate CAs 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.

[6] In the current implementation of the OCSP, the ''ArchiveCutoff'' extension is included in OCSP responces only for certificates that have expired

4.11 End of Subscription

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

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow is not supported by the Subordinate CAs.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not Applicable.

5 Facility, Management, and Operational Controls

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

ECAC's security program includes 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 ECAC has in place to counter such threats.

Based on the Risk Assessment, ECAC develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan also takes into account available technology and the cost of implementing the specific measures and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical Security Controls

The ECAC PMA ensures that appropriate physical controls are implemented at the Subordinate 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 Subordinate CAs' systems.

5.1.2 Physical Access

The Subordinate 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 Subordinate 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 Subordinate CAs' equipment continuously operate within the manufacturers' range of operating temperatures and humidity.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

The ECAC Subordinate 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 activated in the case of fire, and can be manually activated, if necessary.

5.1.6 Media Storage

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

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

5.1.7 Waste Disposal

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

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

5.1.8 Off-Site Backup

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

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

Adequate back-up facilities ensure that backup copies are transferred to the disaster recovery location where they are stored with the same physical, technical and procedurals controls that apply to the primary facility.

5.2 Procedural Controls

The ECAC PMA follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the ECAC Subordinate 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 Subordinate CAs:

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

5.2.2 Number of Persons Required per Task

The ECAC operations team follows rigorous control procedures to ensure the segregation of duties, based on job responsibility, to prevent single trusted personnel to perform sensitive operations.

The most sensitive tasks such as the following require the presence of two or more persons:

- Physical access to the secure enclave where the CA systems are hosted,
- Access to and management of CA's 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
- System administrators issue the necessary ICT system credentials for ECAC Subordinate CAs staff to perform their respective functions.

5.2.4 Roles Requiring Separation of Duties

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

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

For EV certificates, To approve certificate issuance, as outlined under "Final Cross-Correlation and Due Diligence" in Section 4.2.2.1, the participation of two individuals is required. One RA officer reviews and verifies all Applicant information, while another RA officer approves the issuance of the EV Certificate.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Prior to engagement of a 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 the Subordinate CAs personnel.

The training program encompasses a diverse range of topics and is delivered by a combination of experienced Subordinate 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 Subordinate CAs services. The topics covered in the training are:

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

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

5.3.4 Retraining Frequency and Requirements

The training curriculum is delivered to all ECAC Subordinate 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 Subordinate 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 Subordinate 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 Subordinate 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 Subordinate CAs staff.

The ECAC PMA shall also ensure that the key operational documentation is made available to the relevant staff members. This includes, at a minimum, this CPS document, security policies, operational guides and technical documentation relevant to every trusted role.

5.4 Audit Logging Procedures

Audit logging procedures include event logging and systems auditing, implemented for the purpose of maintaining a secure environment. This covers activities such as key life cycle management, including key generation, backup, storage, recovery, destruction and the management of cryptographic devices, the CA and OCSP responder.

Security audit log files for all events relating to the security of the CA, RA and OCSP responders shall be generated and preserved.

These logs shall be reviewed by the security officer team and are also subject to review as part of the regular internal audits performed by the ECAC PMA compliance function on the Subordinate CAs operations.

5.4.1 Types of Events Recorded

Audit logs are generated for all events relating to the security and services of the Subordinates CAs systems. ECAC records events related to its actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved.

ECAC makes these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements

At a minimum, each audit record includes the following:

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

4. Description of the event.

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

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

1. Subordinates CAs certificates and key life cycle events, including:
    1. Key generation, backup, storage, recovery, archival and destruction;
    2. Cryptographic device life-cycle management events.
    3. Certificate requests, renewal, and re-key requests, and revocation;
    4. Approval and rejection of Certificate requests;
    5. Generation of CRLs;
    6. Signing of OCSP responses; and
    7. Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
2. Subscriber Certificate life-cycle management events, including:
    1. Certificate requests, renewal, and re-key requests, and revocation;
    2. All verification activities stipulated in this CPS (e.g. date, time, calls, persons communicated with);
    3. Approval and rejection of certificate requests;
    4. Issuance of certificates;
    5. Multi-Perspective Issuance Corroboration attempts from each Network Perspective, minimally recording the following information:
        1. An identifier that uniquely identifies the Network Perspective used;
        2. The attempted domain name and/or IPaddress; and
        3. The result of the attempt (e.g., “domain validation pass/fail”, “CAA permission/prohibition”)
    6. Multi-Perspective Issuance Corroboration quorum results for each attempted domain name or IP address represented in a Certificate request.
3. Security events, including:
    1. Successful and unsuccessful PKI system access attempts;
    2. PKI and security system actions performed;
    3. Relevant router and firewall activities (as described in Section 5.4.1.1); and
    4. Security profile changes;

5. System platform issues (e.g. crashes), hardware failures, and other anomalies
6. Installation, update and removal of software on a Certificate System;
7. Entries to and exits from the CA facility.

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

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

5.4.1.1 Router and firewall activities logs

Router and firewall activities logged include:

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

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

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

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

5.4.2 Frequency of Processing Log

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

- Audit and Security of the online CA systems (Ex. OCSP responder) are reviewed by the Security Officer's on monthly basis to validate the integrity of the logging processes and to test/confirm the daily monitoring function is being operated properly,
- Physical access logs and the user management on the PKI systems are reviewed by the Security Officer's team on quarterly basis to validate the physical and logical access policies,
- The PMA audit and compliance function executes an internal audit on the Subordinate CAs operations on yearly basis. Samples of the log review reports and

collected audit logs since the last audit cycle is requested by the PMA as part of this internal audit.

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

5.4.3 Retention Period for Audit Log

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

1. CA certificate and key lifecycle management event records (as set forth in Section 5.4.1(1)) after the later occurrence of:
    1. the destruction of the CA Private Key; or
    2. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509 v3 basic Constraints extension with the CA field set to true and which share a common Public Key corresponding to the CA Private Key,
2. Subscriber Certificate lifecycle management event records (as set forth in Section 5.4.1(2)) after the revocation or expiration of the Subscriber Certificate,
3. Any security event records (as set forth in Section 5.4.1(3)) after the event occurred.

5.4.4 Protection Of Audit Log

Audit logs are protected by a combination of physical, procedural, and technical security controls as follows:

- The ECAC Subordinate CAs systems generates cryptographically protected audit logs
- The security of audits logs is maintained while these logs transit by the backup system and when these logs are archived
- The access control policies enforced on the ECAC Subordinate 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 Subordinate CAs operations personnel.

5.4.5 Audit Log Backup Procedures

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

- Backup media are stored locally in the ECAC Subordinate 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 Subordinate 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 Subordinate 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 Subordinate CAs core and supporting PKI system. This regular self-assessment activity is executed by security personnel part of the Subordinate CAs operations team.

On an annual basis, and after infrastructure or application upgrades or modifications that the Subordinate CAs determines are significant, the ECAC PMA coordinates a third-party independent vulnerability assessment and penetration testing is conducted on the Subordinate CAs systems.

The outcome of the regular assessments and identified issues are 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 Subordinate 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 Subordinate CAs personnel.

5.5 Records Archival

5.5.1 Types of Records Archived

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

1. Documentation related to the security of CA systems, and
2. 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 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 seven (7) years:

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

5.5.3 Protection of Archive

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

5.5.4 Archive Backup Procedures

Only one version of each digital archive is maintained in the primary and disaster recovery facilities of the ECAC Subordinate CAs. The Subordinate 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 Subordinate CAs systems is synchronized with the time source of a GPS clock. The time-stamping services setup reaches an accuracy of the time of +/-1s or better with respect to UTC.

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

5.5.6 Archive Collection System (Internal or External)

The EAC Subordinate 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 Subordinate CAs operations team uses the ECAC Subordinate 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 Subordinate CAs' key shall be changed with a frequency that ensures the Subordinate CAs shall have a validity period greater than the maximum lifetime of Subordinate CA's certificates.

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

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

To support revocation management of issued certificates, the old CA private keys are maintained until all the Certificates signed with the Private Key have expired.

5.7 Compromise And Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If a potential hacking attempt or other form of compromise to the ECAC Subordinate 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 implements the necessary measures to ensure full recovery of the ECAC Subordinate CAs' services in case of a disaster, corrupted servers, software, or data. That is subject to the PMA authorization to trigger incident recovery procedures.

The ECAC disaster recovery and business continuity document specifies the circumstances imply triggering of incident recovery procedures that may involve the disaster recovery location if required.

The ECAC disaster recovery and business continuity plan is tested at least once a year, including failover scenarios to the disaster recovery location.

5.7.3 Entity Private Key Compromise Procedures

For Subscribers key compromise, see section 4.9.

Compromise of the ECAC Subordinate 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 Subordinate CAs required operational capabilities, in a timely fashion. In particular, the plan targets the recovery of the following services, either on the primary location, or the disaster recovery location:

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

Failover scenarios to the ECAC disaster recovery location are made possible considering the ECAC Subordinate 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:

1. The conditions for activating the plan,
2. Emergency procedures,
3. Fallback procedures,
4. Resumption procedures,
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans.
10. The Subordinate CAs' plan to maintain or restore the Subordinate CAs' business operations in a timely manner following interruption to or failure of critical business processes
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the main site; and

15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either ate the original or a remote site.

ECAC does not disclose business continuity plans to Subscribers, Relying Parties, or to Application Software Suppliers, but will provide business continuity plan and security plans to the auditors upon request.

5.8 CA or RA Termination

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

- Ensure that any disruption caused by the termination of the Subordinate CAs is minimized as much as possible
- Ensure proper arrangements for the retention of archived logs, as specified in Section 5.5
- Ensure proper arrangements for maintaining the validation status service URLs specified in certificates that remain valid for the applicable period after termination,
- Ensure prompt notification of termination is provided to Subscribers, Authorized Relying Parties, Application Software Providers, and other relevant stakeholders. This notification should be published in daily newspapers or communicated through other mediums and methods as determined by the PMA
- Where applicable, ensure communication with relevant parties and facilitate the transfer of archived Subordinate CAs' records to an appropriate custodian
- Ensure the development and execution of a plan to assist, as much as possible, Subordinate CAs' subscribers in transitioning to another TSP,
- ensure that a process for revoking all Digital Certificates issued by the Subordinate CAs at the time of termination is maintained.

6 Technical Security Controls

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

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 ECAC's Subordinate 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 a Qualified Auditor (see section 8 Compliance Audit and Other Assessments)
- Proper distribution of secrets/activation data/key shares to the trusted operatives and key custodians
- A video of the entire key generation ceremony will be recorded and stored securely for audit purposes

6.1.1.2 Subscriber's Key Pair Generation

The subscriber keys are generated according to the below requirements:

Certificate type	Key generation requirements
OV & EV SSL server certificates	The key pair are generated using the key generation utility provided with the web server software.

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

1. The Key Pair does not meet the requirements set forth in 6.1.5 and/or 6.1.6;
2. There is clear evidence that the specific method used to generate the Private Key was flawed;
3. The Subordinate CAs are aware of a demonstrated or proven method that exposes the Private Key to compromise.
4. The Subordinate CAs has previously been made aware that the Subscriber's Private Key has suffered a Key Compromise, such as through the provisions of Section 4.9.1.1;

5. The Subordinate CAs is aware of a demonstrated or proven method to easily compute the Private Key based on the Public Key in the certificate, including but not limited to those identified in Section 6.1.1.3(5) of the Baseline Requirement.

The Subordinate CAs will not generate a Key Pair on behalf of a Subscriber and will not accept a Certificate request using a Key Pair previously generated by the Subordinate CAs.

6.1.2 Private Key Delivery to Subscriber

ECAC does not generate Subscribers' private keys for publicly trusted SSL certificates, nor does it perform key escrow, recovery, or backup.

If ECAC detects or suspects that the Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then ECAC revokes all Certificates that include the Public Key corresponding to the communicated Private Key.

6.1.3 Public Key Delivery to Certificate Issuer

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

6.1.4 CA Public Key Delivery to Relying Parties

The Subordinate CAs public key certificates are published on the ECAC public repository.

6.1.5 Key Sizes

The Subordinate CAs's keys size are 4096-bit RSA.

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

6.1.6 Public Key Parameters Generation and Quality Checking

6.1.6.1 Subordinate CAs

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

6.1.6.2 Subscribers

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

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

For the creation and storage of the ECAC Subordinate 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 Subordinate CAs hosting facility.

ECAC encrypts its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

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

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

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

6.2.4 Private Key Backup

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

Backup operations are executed as part of the ECAC Subordinate CAs' key generation ceremonies. The ECAC Subordinate 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 Subordinate 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 Subordinate CAs' key ceremony procedure. Dedicated personnel in

trusted roles participate in the transport operation, which is escorted by security guards. Provisions stipulated in Section 6.2.2 are also considered during the transportation

6.2.5 Private Key Archival

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

6.2.6 Private Key Transfer into or from a Cryptographic Module

The ECAC Subordinate 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 Subordinate 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

6.2.8.1 Subordinate CAs

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

6.2.8.2 Subscribers

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

6.2.9 Method of Deactivating Private Key

6.2.9.1 Subordinate CAs

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

6.2.9.2 Subscribers

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

6.2.10 Method of Destroying Private Key

6.2.10.1 Subordinate CAs

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

The CA keys are destroyed through documented procedures involving individuals in trusted roles. These procedures enforces the principle of multi-person control and split

knowledge. The procedures also ensures that the CAs keys are destroyed by removing permanently from any hardware modules the keys are stored on.

6.2.10.2 Subscribers

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

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

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Refer to Section 5.5 for archival conditions.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

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

The maximum duration of a Subscriber end entity certificate doesn't exceed 398 days. For the purpose of calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, shall represent an additional day. For this reason, Subscriber Certificates should NOT be issued for the maximum permissible time by default, in order to account for such adjustments.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 Subordinate CAs

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

6.4.1.2 Subscribers

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

6.4.2 Activation Data Protection

6.4.2.1 Subordinate CAs

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

6.4.2.2 Subscribers

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

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

In particular, the ECAC subordinate 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 Subordinate CAs systems and end-point protection
- Backup and recovery mechanisms for ECAC Subordinate CAs operations
- Hardening of ECAC Subordinate 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 Subordinate CAs operational processes
- The ECAC Subordinate 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 in implementing the required ECAC Subordinate 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 Subordinate CAs' operations team.

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

6.6.2 Security Management Controls

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

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

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

6.6.3 Life Cycle Security Controls

Refer to Section 6.5.1 for details.

6.7 Network Security Controls

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

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

The ECAC PMA ensures regular vulnerability testing is conducted on the ECAC Subordinate CAs' online services. The ECAC PMA also ensures that at least once a year,

penetration testing is conducted on the ECAC Subordinate CAs connected systems, by an independent third-party.

6.8 Timestamping

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

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profiles

OV TLS 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 + **[72]** Months	Suggested validity for the subordinate certificate is up to 06 years
Subject	False				
CountryName		M	S	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Electronic Certification Accreditation Council	UTF8 encoded
CommonName		M	S	ECAC OV TLS CA G1	UTF8 encoded

SubjectPublicKeyInfo	False	M	D		
AlgorithmIdentifier		M	D	RSA (OID: 1.2.840.113549.1.1.1) NULL	
SubjectPublicKey		M	D	Key length: 4096	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M	D		Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Root CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M	S		
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.gov.pk	OCSP responder URL
AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		M	S	http://repository-ecac.pki.gov.pk/repository/cert/tls_root_ca.p7b	Root CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	M	S		

DistributionPoint		M	S	http://repository-ecac.pki.gov.pk/repository/crl/tls_root_ca.crl	CARL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M	S		
keyCertSign, cRLSign		M	S	True	
Policy Properties					
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.23.140.1.2.2	CA/B BR Reserved Certificate Policy for OV TLS Certificates
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	1.3.6.1.4.1.59337.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://ecac.pki.gov.pk/repository/cps	
Extended Key Usage Properties					
extKeyUsage	False	M	S		
clientAuth, serverAuth		M	S	True	
Basic Constraints Properties					

basicConstraints		True	M	S		
	cA		M	S	True	
	pathLenConstraint		M	S	0	

EV TLS 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 + **[72]** Months	Suggested validity for the subordinate certificate is up to 06 years
Subject	False				
CountryName		M	S	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Electronic Certification Accreditation Council	UTF8 encoded

CommonName		M	S	ECAC EV TLS CA G1	UTF8 encoded
SubjectPublicKeyInfo	False	M	D		
AlgorithmIdentifier		M	D	RSA (OID: 1.2.840.113549.1.1.1) NULL	
SubjectPublicKey		M	D	Key length: 4096	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M	D		Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Root CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M	S		
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.gov.pk	OCSP responder URL
AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		M	S	http://repository-ecac.pki.gov.pk/repository/cert/tls_root_ca.p7b	Root CA Certificate/Chain download URL over HTTP

crlDistributionPoints	False	M	S		
DistributionPoint		M	S	http://repository-ecac.pki.gov.pk/repository/crl/tls_root_ca.crl	CARL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M	S		
keyCertSign, cRLSign		M	S	True	
Policy Properties					
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.23.140.1.1	CA/B BR Reserved Certificate Policy for EV TLS Certificates
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	1.3.6.1.4.1.59337.1.1	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://ecac.pki.gov.pk/repository/cps	
Extended Key Usage Properties					

extKeyUsage	False	M	S		
clientAuth, serverAuth		M	S	True	
Basic Constraints Properties					
basicConstraints	True	M	S		
cA		M	S	True	
pathLenConstraint		M	S	0	

OV TLS Certificate

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

Field	CE	O/M	CO	Value	Comment
Certificate		M			
TBSCertificate		M			See 4.1.2 of RFC 5280
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	The issuing Subordinate CA Signature (i.e, OV TLS CA).	The issuing Subordinate CA's signature value
TBSCertificate					
Version	False	M			
Version		M	S	2	Version 3
SerialNumber	False	M			
CertificateSerialNumber		M	D		At least 64 bits of entropy validated on duplicates.
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M		<Subordinate Issuing CA's Subject>	The issuer field is defined as the X.501 type "Name"
CountryName		M	S	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
OrganizationName		M	S	Electronic Certification Accreditation Council	UTF8 encoded

CommonName		M	S	ECAC OV TLS 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 + **[397]** days	Maximum 397 days validity allowed (Baseline Requirement)
Subject	False				
CountryName		M	D	Country Name	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
stateOrProvinceName		M/O	D	State Or Province	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
localityName		M/O	D	Locality	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
OrganizationName		M	D	Organization name of the legal entity	UTF8 encoded
SubjectPublicKeyInfo	False	M			
AlgorithmIdentifier		M	D	RSA (OID: 1.2.840.113549.1.1.1)	

				NULL	
	SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions						
Authority Properties						
AuthorityKeyIdentifier		False	M			Mandatory in all certificates except for self-signed certificates
	KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate Issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess		False	M			
	AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
	AccessLocation		M	S	http://ocsp.pki.gov.pk	OCSP responder URL
	AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
	AccessLocation		M	S	http://ocsp.pki.gov.pk/repository/certs/ov_tls_ca.p7b	Subordinate Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints		False	M			
	DistributionPoint		M	S	http://ocsp.pki.gov.pk/repository/crl/ov_tls_ca.crl	CRL download URL.
Key Usage Properties						
keyUsage		True	M			

digitalSignature		M	S	True	RSA
Policy Properties					
certificatePolicies	False	M			
PolicyIdentifier		M	S	2.23.140.1.2.2	CA/B BR Reserved Certificate Policy for OV Certificates
certificatePolicies	False	M			
PolicyIdentifier		M	S	1.3.6.1.4.1.59337.1.4	
policyQualifiers:policyQualifierId		M	S	id-qt 1	
policyQualifiers:qualifier:cPSuri		M	S	https://ocsp.pki.gov.pk/repository/cps	
certificatePolicies	False	M			
PolicyIdentifier		M	S	1.3.6.1.4.1.59337.3.3.1	
Extended Key Usage Properties					
extKeyUsage	False	M			
serverAuth,		M	S	True	
clientAuth		O	S	True	
Subject Alternative Name Properties					
subjectAlternativeName	False	M			
dNSName or iPAddress		M	D	dNSNames with verified ownership or IPv4 or IPv6 address with verified ownership	Contains either a Fully-Qualified Domain Name or Wildcard Domain Name or Contains an IPAddress
SCT List Properties					
SignedCertificateTimestampList	False	M	D		

	sctList		M	D	List of submission logs	

EV TLS Certificate

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

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 = OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	The issuing Subordinate CA Signature (i.e, EV TLS CA).	The issuing Subordinate 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	<Subordinate Issuing CA's Subject>	The issuer field is defined as the X.501 type "Name"
CountryName		M	S	PK	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)

OrganizationName		M	S	Electronic Certification Accreditation Council	UTF8 encoded
CommonName		M	S	ECAC EV TLS 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 + up to **[365]** days	Maximum 12 months validity allowed (EV Guideline Requirement)
Subject	False				
CountryName		M	D	Country Name	Encoded according to "ISO 3166-1-alpha-2 code elements". PrintableString, size 2 (rfc5280)
stateOrProvinceName		M/O	D	State Or Province	UTF8 encoded. Mandatory if the localityName field is not present, optional if the localityName is present.
localityName		M/O	D	Locality	UTF8 encoded. Mandatory if the stateOrProvinceName field is not present, optional if the stateOrProvinceName is present.
OrganizationName		M	D	Organization name of the legal entity	UTF8 encoded
businessCategory		M	D	Subject's business category	as defined in EV guideline.

jurisdictionCountryName		M	D	Subject's jurisdictionCountryName	As defined in EV Guideline
jurisdictionStateOrProvinceName		O	D	Subject's jurisdictionStateOrProvinceName	As defined in EV Guideline
jurisdictionLocalityName		O	D	Subject's jurisdictionLocalityName	As defined in EV Guideline
serialNumber		M	D	Subject's serial number	As defined in EV Guideline
SubjectPublicKeyInfo	False	M	D		
AlgorithmIdentifier		M	D	RSA (OID: 1.2.840.113549.1.1.1) NULL	
SubjectPublicKey		M	D	Public Key Key length: 2048 or 4096 (RSA)	
Extensions					
Authority Properties					
AuthorityKeyIdentifier	False	M	D		Mandatory in all certificates except for self-signed certificates
KeyIdentifier		M	D	160-bit SHA-1 Hash of the Subordinate Issuing CA public key	When this extension is used, this field MUST be supported as a minimum
AuthorityInfoAccess	False	M	S		
AccessMethod		M	S	*Id-ad-2 1 id-ad-ocsp OID i.e.,1.3.6.1.5.5.7.48.1 (ca ocsp)*	OCSP Responder field
AccessLocation		M	S	http://ocsp.pki.gov.pk	OCSP responder URL

AccessMethod		M	S	*Id-ad-2 2 id-ad-caIssuers OID i.e.,1.3.6.1.5.5.7.48.2 (ca cert)*	CA Issuers field
AccessLocation		M	S	http://ocsp.pki.gov.pk/repository/certs/ev_tls_ca.p7b	Subordinate Issuing CA Certificate/Chain download URL over HTTP
crlDistributionPoints	False	O	S		
DistributionPoint		M	S	http://ocsp.pki.gov.pk/repository/crl/ev_tls_ca.crl	CRL download URL.
Subject Properties					
SubjectKeyIdentifier	False	M	D		
KeyIdentifier		M	D	160-bit SHA-1 hash of SubjectPublicKey	When this extension is used, this field MUST be supported as a minimum
Key Usage Properties					
keyUsage	True	M	S		
digitalSignature		M	S	True	RSA
Policy Properties					
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	2.23.140.1.1	CA/B BR Reserved Certificate Policy for EV Certificates
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	1.3.6.1.4.1.59337.1.4	
policyQualifiers:policyQualifierId		M	S	id-qt 1	

policyQualifiers:qualifier:cPSuri		M	S	https://ocsp.pki.gov.pk/repository/cps	
certificatePolicies	False	M	S		
PolicyIdentifier		M	S	1.3.6.1.4.1.59337.3.3.5	
Extended Key Usage Properties					
extKeyUsage	False	M	S		
serverAuth,		M	S	True	
clientAuth		O	S	True	
Subject Alternative Name Properties					
subjectAlternativeName	False	M	D		
dNSName		M	D	dNSNames with verified ownership	Contains a Fully-Qualified Domain Name. No Wildcard Domain Name is allowed.
SCT List Properties					
SignedCertificateTimestampList	False	M	D		
sctList		M	D	List of submission logs	

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

Subordinate CAs comply with RFC 5280 and Baseline Requirements in all certificates it issues.

The Subordinate CAs and end entity certificates include an Extended Key Usage extension containing key usage purposes id-kp-serverAuth and id-kp-clientAuth.

AnyExtendedKeyUsage KeyPurposeId cannot be included in the certificates.

7.1.3 Algorithm Object Identifiers

Certificates are issued with algorithms indicated by the following OIDs

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

7.1.4 Name forms

7.1.4.1 Name Encoding

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

7.1.4.2 Subject Information - Subscriber Certificates

The applicable subject information for each type of TLS Certificates is specified in the table below.

OV TLS CA issues TLS Certificates where the entries of the Subject Alternative Name Extension and the contents of the Subject DN fields are compliant with their respective definitions stated in section 7.1.4 of the Baseline Requirements. In addition, subject Attributes will not contain only metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

For EV specific fields the corresponding section in the EV Guideline must be referred.

TLS Certificate Type	Subject DN	Subject Alternative Name
OV TLS Certificates	• countryName • stateOrProvinceName Or • localityName • organizationName	dNSName, iPAddress
EV TLS Certificates	• countryName • stateOrProvinceName Or • localityName	dNSName[7]

[7] No IP address or Wildcard Domain Name is allowed for EV certificates.

	• organizationName • businessCategory • jurisdictionCountryName • jurisdictionStateOrProvinceName (if required) • jurisdictionLocalityName (if required) • serialNumber	

7.1.4.3 Subject Information – Subordinate CA Certificates

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

7.1.5 Name Constraints

ECAC follows the requirements of section 7.1.5 of the Baseline Requirements for publicly trusted TLS certificates .

7.1.6 Certificate Policy Object Identifier

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

Following Object Identifiers are also used:

End entity certificate policies	
2.23.140.1.2.2	CAB BR Reserved Policy for OV TLS Certificates
2.23.140.1.1	CAB BR Reserved Policy for EV TLS Certificates

7.1.7 Usage of Policy Constraints Extension

No Stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

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

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No Stipulation.

7.2 CRL Profile

OV TLS CA CRL

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

Field	CE	O/M	CO	Value	Comment
CertificateList		M			
TBSCertificate					
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	The signature of the CA issuing the CRL.	The signature of the authority issuing the CRL.
TbSCertList					
Version	False	M			
Version			S	1	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	PK	
OrganizationName		M	S	Electronic Certification Accreditation Council	
CommonName		M	S	ECAC OV TLS 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

EV TLS CA CRL

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

Field	CE	O/M	CO	Value	Comment
CertificateList		M			
TBSCertificate					
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
SignatureValue		M	D	The signature of the CA issuing the CRL.	The signature of the authority issuing the CRL.
TbSCertList					
Version	False	M			
Version			S	1	Version 2
Signature	False	M			
AlgorithmIdentifier		M	S	OID = 1.2.840.113549.1.1.11	SHA256 with RSA Encryption
Issuer	False	M			
CountryName		M	S	PK	
OrganizationName		M	S	Electronic Certification Accreditation Council	
CommonName		M	S	ECAC EV TLS 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 Subordinate CAs support X509 v2 CRLs.

7.2.2 CRL and CRL Entry Extensions

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

7.2.2.1 reasonCode (OID 2.5.29.21)

The reasonCode feild may be used for revoked Certificates. The reasonCode indicated must not be unspecified (0) and if reasonCode unspecified (0) is used, the CA will omit the reasonCode entry in the CRL.

This extension must not be marked critical. The most appropriate reason must be selected by the Subscriber or the CA from one the following:

(i) **keyCompromise** (1), Indicates that it is known or suspected that the Subscriber's Private Key has been compromised.

(ii) **affiliationChanged** (3), Indicates that the Subject's name or other Subject Identity Information in the Certificate has changed, but there is no cause to suspect that the Certificate's Private Key has been compromised.

(iii) **superseded** (4), Indicates that the Certificate is being replaced because: the Subscriber has requested a new Certificate, the CA has reasonable evidence that the validation of domain authorization or control for any fully-qualified domain name or IP address in the Certificate should not be relied upon, or the CA has revoked the Certificate for compliance reasons such as the Certificate does not comply with the CAB/Forum Baseline Requirements or this CPS.

(iv) **cessationOfOperation** (5), Indicates that the website with the Certificate is shut down prior to the expiration of the Certificate, or if the Subscriber no longer owns or controls the Domain Name in the Certificate prior to the expiration of the Certificate.

(v) **privilegeWithdrawn** (9), Indicates that there has been a subscriber-side infraction that has not resulted in keyCompromise, such as the Certificate Subscriber provided misleading information in their Certificate Request or has not upheld their material obligations under the Subscriber Agreement or Terms of Use.

The default revocation reason is **unspecified** (0) which results in no reasonCode being provided in the CRL. The CA will not use reasonCode **certificateHold** (6).

The **priviledgeWithdrawn** (9) reasonCode is not made available to the Subscriber.

If ECAC obtains evidence of Key Compromise for a Certificate whose CRL entry does not contain a reasonCode extension or has a reasonCode extension with a non-keyCompromise (1) reason, then ECAC may update the CRL reasonCode to keyCompromise (1).

7.2.2.2 issuingDistributionPoint (OID 2.5.29.28)

The CRLs do not support the Issuing Distribution Point extension.

7.3 OCSP Profile

OV TLS 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 OV TLS 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 OV TLS 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			

EV TLS 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 EV TLS 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 EV TLS 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			

OCSP response format

The below profile describes OCSP response according to RFC 6960.

Field	Value	Comment
responseStatus	"0" Response has valid confirmations	Result of the query. If the value of responseStatus is other than "0", the responseBytes field is not set.
responseBytes		
responseType	id-pkix-ocsp-basic	
BasicOCSPResponse		
tbsResponseData		
version	1	Version of the response format
responderID	C = PK O = <The full registered name of the subject> CN = <A name commonly used by the subject to represent itself>	Distinguished name of the OCSP responder. The information MUST correspond to the certificate that was used to sign the response.
producedAt		The time at which the OCSP responder signed this response.
responses		
certID		In accordance with RFC 6960
hashAlgorithm	Depending on the hash algorithm used in request	hashAlgorithm is the hash algorithm used to generate the issuerNameHash and issuerKeyHash values. Supported hash algorithms are SHA-1, SHA-256, SHA-384 and SHA-512.
issuerNameHash		Hash of issuer's DN
issuerKeyHash		Hash of issuer's public key
SerialNumber		CertificateSerialNumber
certStatus		Status of the certificate: • Good – certificate issued and has not been revoked. • Revoked – certificate is revoked. • Unknown – the certificate is unrecognized by this OCSP responder.
thisUpdate		The most recent time at which the status being indicated is known by the responder to have been correct.
nextUpdate	ThisUpdate + 8 hours	The time at or before which newer information will be available about the status of the certificate
ArchiveCutoff[8]	the CA's certificate "notBefore" time and date value	According to RFC 6960 clause 4.4.4. "archive cutoff" date set to the CA's certificate "notBefore" time and date value According to ETSI EN 319 411-2 / CSS-6.3.10-10.

[8] In the current implementation of the OCSP, the ''ArchiveCutoff'' extension is included in OCSP responces only for certificates that have expired

extended-revoked definition	Null	the responder supports the extended definition of the "revoked" status to also include non-issued certificates
signatureAlgorithm	Sha256withRSAEncryption	Signing algorithm
signature		signature value
certs		Certificate corresponding to the private key used to sign the response. Only OCSP responder certificate is included in the OCSP response.

7.3.1 Version Number(s)

As per the OCSP certificate profile, section 7.3.

7.3.2 OCSP Extensions

As per the OCSP certificate profile, section 7.3.

8 Compliance Audit and Other Assessments

The procedures outlined in this CPS are intended to align with the requirements specified in Section 1 and cover all applicable elements of current PKI standards relevant to the industry sectors in which ECAC operates.

8.1 Frequency or Circumstances of Assessment

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

8.2 Identity/Qualifications of Assessor

The external WebTrust audits will be performed by qualified auditors that fulfil the following requirements:

1. Independence from the subject of the audit
2. Ability to conduct an audit that addresses the criteria specified in WebTrust for Certification Authorities
3. 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
4. Licensed by WebTrust
5. Bound by law, government regulation or professional code of ethics
6. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

For internal audit, the ECAC PMA has its own audit function that is independent of the ECAC PKI operations team.

External auditors are independent third party WebTrust practitioners.

8.4 Topics Covered by Assessment

The ECAC 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 – Network Security.

8.5 Actions Taken as a Result of Deficiency

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

Regarding compliance audits of Subordinate 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.

Annual WebTrust Audit Reports are made publicly available no later than three (3) months after the end of the audit period. If there is a delay greater than three (3) months, ECAC will provide an explanatory letter signed by the Qualified Auditor. ECAC's WebTrust audit reports can be found at: https://ecac.pki.gov.pk/repository/index.html

8.7 Self-audit

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

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Not Applicable.

9.1.2 Certificate Access Fees

No fees will be charged to access the certificates issued.

9.1.3 Revocation Or Status Information Access Fees

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

9.1.4 Fees for Other Services

Not Applicable.

9.1.5 Refund Policy

Not Applicable.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

ECAC carries at least $2 million in Commercial General Liability insurance coverage and Professional Liability/Errors & Omissions insurance, with policy limits of at least $5 million in coverage, including coverage for

(i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and

(ii) (ii) Claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

Insurance is carried through companies rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated.

9.2.2 Other Assets

The ECAC maintains sufficient financial resources to maintain operations and fulfill duties of the ECAC Subordinate 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 is 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 Subordinate CAs systems. This shall include:

- The communications between the RA systems and the subscribers.
- The communications between the RA and the CA systems.
- Sessions to deliver certificates

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

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

Unless otherwise stated in this 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 Subordinate CAs digital certificates and any other publication originating from the ECAC PMA, including this CPS.

The Subordinate 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 Subordinate 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 CPS, and that any certificates issued under this document are in accordance with the stipulations specified.

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

- The Subscriber that is a party to the Subscriber Agreement;
- All Application Software Suppliers with whom the Pakistan National Root 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 OV TLS CA has complied with the Baseline Requirements and its CPS in issuing and managing the certificate.

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

- **Right to Use Domain Name or IP Address:** That, at the time of issuance, the OV TLS CA **(**i). implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii). Followed the procedure when issuing the Certificate; and (iii). accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- **Authorization for Certificate**: That, at the time of issuance, the OV TLS CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;
- **Accuracy of Information**: That, at the time of issuance, the OV TLS CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;
- **Identity of Applicant**: That, if the Certificate contains Subject Identity Information, the OV TLS CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2 and 11.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;
- **Subscriber Agreement**: That, if the OV TLS CA and Subscriber are not Affiliated, the Subscriber and OV TLS CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the OV TLS CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
- **Status**: That the OV TLS CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates;
- **Revocation:** That the OV TLS CA will revoke the Certificate for any of the reasons specified in these Requirements.

ECAC represents and warrants to Certificate Beneficiaries for EV SSL Certificates that, during the period when the Certificate is valid, ECAC has followed the Guidelines and its

Certification Practice Statement in issuing and managing the Certificate and in verifying the accuracy of the information contained in the EV SSL Certificate:

- **Legal Existence**: EV TLS CA has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the Certificate was issued, the Subject named in the Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration.
- **Identity:** EV TLS CA has confirmed that, as of the date the Certificate was issued, the legal name of the Subject named in the Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business.
- **Right to Use Domain Name:** EV TLS CA has taken all steps reasonably necessary to verify that, as of the date the Certificate was issued, the Subject named in the Certificate has the right to use all the Domain Name(s) listed in the Certificate.
- **Authorization for EV Certificate:** EV TLS CA has taken all steps reasonably necessary to verify that the Subject named in the Certificate has authorized the issuance of the EV Certificate.
- **Accuracy of Information**: EV TLS CA has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued.
- **Subscriber Agreement:** The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with the CA that satisfies the requirements of these Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use.
- **Status:** EV TLS CA will follow the requirements of the EV Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and
- **Revocation:** EV TLS CA will follow the requirements of the EV Guidelines and revoke the Certificate for any of the revocation reasons specified in the EV Guidelines.

9.6.2 RA Representations and Warranties

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

9.6.3 Subscriber Representations and Warranties

The ECAC implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. A separate Agreement is used for each certificate request. The Subscriber Agreement or Terms of Use contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its

principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to the RA officer, both in the certificate request and as otherwise requested by ECAC.
2. **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
3. **Acceptance of Certificate:** An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate:** When certificates are requested, an obligation and warranty to use the Certificate and associated Private Key only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
5. **Reporting and Revocation:** An obligation and warranty to:
   a. promptly requests revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
   b. promptly requests revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate
6. **Termination of Use of Certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. **Responsiveness:** An obligation to respond to ECAC instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. **Acknowledgment and Acceptance:** An acknowledgment and acceptance that the ECAC is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by this CPS,

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 a certificate provides adequate assurances for its intended use.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers Of Warranties

Within the scope of the law of Pakistan, and except in the case of fraud, or deliberate abuse, the ECAC cannot be held liable for:

- The accuracy of any information contained in certificates except as it is warranted by the Subscriber that is the party responsible for the ultimate correctness and accuracy of all data transmitted to the ECAC with the intention to be included in the certificate.
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificates or digital signatures.
- Wilful misconduct of any third-party participant breaking any applicable laws in 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 Subordinate CAs services.
- Any form of misrepresentation of information by Subscriber or relying parties on information contained in this CPS or any other documentation made public by the PMA and related to the ECAC services.

9.8 Limitations of Liability

In cases where ECAC has issued and managed the EV Certificate in compliance with the Guidelines and this CPS, ECAC shall not be liable to the EV Certificate Subscriber, Relying Parties or any other third parties for any losses suffered as a result of use or reliance on such EV Certificate.

Otherwise, in cases where ECAC has not issued or managed the EV Certificate in compliance with the EV Guidelines and this CPS, ECAC's liability to the Subscriber for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV Certificate shall not exceed $2,000. Likewise, liability to Relying Parties or any other third parties for legally recognized and provable claims for losses or damages suffered as a result of the use or reliance on such EV Certificate shall not exceed $2,000.

Except for liability with respect to the EV Certificate, in no event shall ECAC be liable for any indirect, incidental, special, or consequential damages, or for any loss of profits, loss of data or other indirect, incidental, consequential damages arising from or in connection with the use, delivery, reliance upon, license, performance or non-performance of

certificates, digital signatures or any other transactions or services offered or contemplated by this CPS.

9.9 Indemnities

Not Applicable.

9.10 Term And Termination

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

When changes are required to be done on this CPS. The ECAC PMA will incorporate any such change into a new version of this document and, upon approval, publish the new version. The new document will carry a new version number.

9.12.1 Procedure for Amendment

Refer to Section 9.12.

9.12.2 Notification Mechanism and Period

Upon publishing on the ECAC repository, the newer version of the CPS becomes effective. The older versions of this document are archived on the ECAC public repository.

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

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

9.12.3 Circumstances under which OID Must Be Changed

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

9.13 Dispute Resolution Provisions

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

9.14 Governing Law

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

9.15 Compliance with Applicable Law

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

- Electronic Transaction Ordinance, 2002

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

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

9.16.3 Severability

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

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

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

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

9.17 Other Provisions

No stipulation.

Document Approval

Reviewed By:

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

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

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

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

Approved By:

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

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

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

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