Pakistan National PKI

Certificate Policy (CP) for Trust Services Providers (TSPs)

Version control

Version	Date	Description / Status	Responsible
V1.0	08/12/2022	Initial version for review & approval	ECAC
V1.1	26/12/2022	Corrected the URLs, Email Addresses, Object IDs	ECAC
V1.2	22/02/2023	Accommodated comments by ECAC Design Authority	ECAC
V1.3	19/02/2024	No Changes. Policy Review Activity.	ECAC

Document Signoff

Version	Date	Responsible	Validated By	Reviewed and Approved By
V1.3	19/02/2024	ECAC	ECAC (PMA)	ECAC (PMA)

Table of Contents

1 Introduction

The present document is the Certificate Policy (hereinafter, the CP) indorsing requirements applicable to the provision of certification services offered the Trust Services Providers (TSP) issuing publicly trusted certificates to end-entities in Pakistan.

Trust Services Providers are established and operated in Pakistan under the Pakistan national PKI accreditation framework and the applicable laws in Pakistan. The ECAC is mandated to operate the national PKI accreditation framework and hence it is responsible for authorizing TSPs offering certification services in Pakistan.

This CP addresses the technical, procedural, and organizational policies of the CAs operated by the TSPs with regard to the complete lifetime of certificates issued by these CAs.

The provisions of the present CP regarding practices, level of services, responsibilities and liability bind TSPs, its CAs, subscribers and relying parties.

This CP 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 TSPs' CAs. Such sections are denoted as "Not applicable". Additional information is presented in subsections of the standard structure where required.

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

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

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

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

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

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

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

Further information with regard to this CP can be obtained from the ECAC PMA, using contact information provided in clause 1.5.

1.1 Overview

The Pakistan National PKI comprises two separate PKI hierarchies for each of the Government and Commercial domains, both hierarchies are established under the Pakistan National Root CA (hereinafter, NR-CA). This setup provides a resilient framework to support variance in requirements between government and non-government sectors regarding the offering and consumption of certification and other trust services.

The Pakistan National PKI offers certification services to support the following use cases:

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

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

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

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

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

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

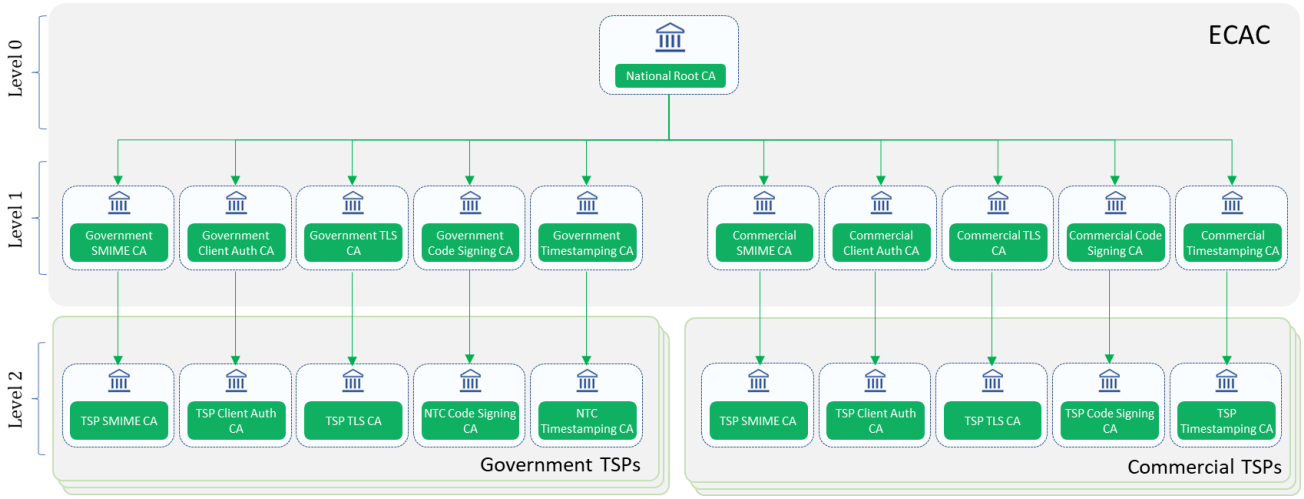

Figure 1 - Pakistan national PKI hierarchy

1.2 Document Name and Identification

This document is the "Certificate Policy (CP) for Trust Services Providers (TSPs)" by the ECAC Pakistan, and it was approved by the ECAC Policy Management Authority (PMA) for the publication.

This CP document is published at https://ecac.pki.gov.pk

The OID **1.3.6.1.4.1.59337.2.1** is used to identify this document.

TSPs shall include the above mentioned OID in the CP extension of their CAs to indicate compliance with the present CP. TSPs shall represent, in its applicable CPS, that all certificates containing the above OID indicating compliance with this CP and are issued and managed in accordance with this CP.

1.3 PKI Participants

Several parties make up the participants of a TSP CA, including:

- The NR-CA,
- The direct superior CA that signed the TSP CA, that could be either:
  - An ECAC Government/Commercial intermediate CA
- The TSP CA itself, i.e. the certification authority of the TSP,
- Registration Authorities (RA) used by the TSP to register end-entities to which end-entity certificates are issued,
- Subscribers,
- Relying parties.

These participants, collectively called PKI participants, and their roles are described in the following sections.

1.3.1 Certification Authorities

National Root Certification Authority

The NR-CA is opened and operated by the ECAC. The NR-CA is at the top-level of the Pakistan national PKI hierarchy.

Government Intermediate Certification Authorities

The Government SMIME CA, Government Client Auth CA, Government TLS CA, Government Code Signing CA and the Government Timestamping CA that are certified by the NR-CA. As indicated in the name of each the CAs, each is dedicated for a specific certificate usage under the Government PKI domain.

The ECAC owns and operates the Government Intermediate CAs and offers related trust services to the government TSPs.

Commercial Intermediate Certification Authorities

The Commercial SMIME CA, Commercial Client Auth CA, Commercial TLS CA, Commercial Code Signing CA and the Commercial Timestamping CA that are certified by the NR-CA. As indicated in the name of each the CAs, each is dedicated for a specific certificate usage under the Commercial PKI domain.

The ECAC owns and operates the Commercial Intermediate CAs [offline] and offers related trust services to the Commercial TSPs.

TSP Certification Authority

A TSP CA is a subordinate issuing CA operated by a TSP based in Pakistan, and which is approved for inclusion in the Governmental PKI domain or in the Commercial PKI domain according to the Pakistan national PKI accreditation framework.

A TSP CA is either certified by one of the NR-CA's intermediate CAs.

A TSP CA shall be operated in accordance with a Certification Practice Statement (CPS) that defined by the TSP in compliance with the present CP. This CP is subject to the approval by the ECAC PMA. Approval activities covers:

- Evaluation of the specified practices of the TSP CA, including but not limited to:
  - types of end-entity certificates issued by the TSP-CA and the related certificate life-cycle management procedures (e.g. vetting and registration procedures, revocation procedures),
  - processes and controls in place to maintain logical, physical and environmental security,
  - cryptographic systems and products used to generate, store and manage cryptographic keys.
- Provisions regarding level of services, responsibilities and liability of the TSP, its CA(s), subscribers and relying parties.

The TSP CAs are technically constrained to restrict the issuance of digital certificates through constraints such as length of certification paths, extended key usage, name constraints, and inclusion of certificate policy OIDs.

TSPs may undergo an independent WebTrust audit in addition to complying with the national accreditation framework indorsed by the ECAC.

The main obligations of a TSP with regards to the operation of a TSP CA are:

- Identification and authentication of subscriber information (Ex. during application and revocation phases) in accordance with the applicable certificate profile requirements,
- Publication of certificates (where applicable) to a public repository,
- Life-cycle management of issued certificates, including but not limited to all aspects related to application, issuance, and revocation,
- Provision and maintenance of certificate validity status information services through publicly available Certificate Revocation Lists (CRL) and Online Certificate Status Protocol (OCSP) responders,
- Inform, without delays, the ECAC PMA about:
    - any significant change to the provision of its certification services,
    - any incident or compromise related to the provision of its certification services,
    - intention to cease the provision of its certification services.

1.3.2 Registration Authorities

The TSP shall set up or delegate the RA function according to this CP. The RA function consists in Registration Authority Officer (RAO), operators, products, systems, and procedures used by the TSP CA to validate the identity of subscribers requesting the issuance of certificates.

In case of delegating the RA function to a third-party organization that may offer this service by law, the TSP remains fully responsible and accountable for the operations performed by the delegated RA.

The RA responsibilities are:

- Authenticating, approving or rejecting certificate application and revocation requests,
- Identify certified entities as per the naming conventions defined in this CP, so that each subscriber is uniquely and unambiguously identified,
- Process certificate issuance and revocation requests with the TSP 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 CP,
- Implementing other operational controls as specified in this CP,

- Processes and stores information according to the requirements defined in this CP (particularly, in section 9).

The personnel involved in the RA function shall meet and follow the requirements set forth in Sections 4.2 and 5.3.

1.3.3 Subscribers

Subscribers of the TSPs can be:

- Natural persons,
- Legal Persons or organizations or departments thereof, or
- Devices.

For any certificate, the subscriber shall sign a subscriber agreement, agreeing on the terms and conditions as set forth by the TSP.

1.3.4 Relying Parties

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

1.3.5 Other Participants

None.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The TSP CA shall restrict the use the certificates it issues using appropriate certificate extensions with regards to key usage and extended key usage, which shall be configured according to the certificate type.

The TSP CPS shall specify, in accordance with the present CP and in particular its section 7, the appropriate certificate usage that apply to each type of certificate it issues. A TSP CA may issue one or more types from the following pre-defined certificate types:

- Natural person certificates for electronic signatures,
- Natural person certificates for authentication,
- Natural person certificates for email Protection (S/MIME),
- Legal person (or organization) certificates for electronic seal (eSeal),
- Legal person (or organization) certificates for code signing,
- Device certificates (Client authentication) for general identification, authentication, or session data encryption purposes,
- TLS certificates for general identification, authentication or session data encryption purposes,
- VPN certificates for general identification, authentication or session data encryption purposes [VPN],

1.4.2 Prohibited Certificate Uses

The TSP CPS shall specify the certificate usage restrictions that apply to each type of certificate it issues.

Any usage of the certificate inconsistent with these restrictions, with the appropriate usage or with the contents of this CP and TSP CPS shall not be authorized.

1.5 Policy Administration

1.5.1 Organization Administering the Document

This CP document is administered by the ECAC PMA.

1.5.2 Contact Person

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

Policy Management Authority

Electronic Certification Accreditation Council (ECAC),

5th Floor NTC HQ Building, G-5/2,

Islamabad, Pakistan

Tel: +92 51 9245739

Email: ecac.certification.info@pki.gov.pk

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

1.5.3 Person Determining CPS Suitability for the Policy

The TSP is responsible for ensuring that its CPS conforms to this CP.

The ECAC PMA is responsible for assessing the actual CPS suitability for the present CP. This process may be supported by a Conformity Assessment Report (CAR) from an auditor as supported in the national accreditation framework.

The final decision on confirming this suitability belongs to the ECAC PMA.

1.5.4 CPS Approval Procedures

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

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

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

1.6 Definitions and Acronyms

1.6.1 Definitions

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

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

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

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

Attestation Letter – A letter attesting that Subject Information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information. In the context of this CP, attestation letters are signed by Human Resource teams of government entities.

Audit Period – In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA)

CA Key Pair – A Key Pair where the Public Key appears as the Subject Public Key Info in one or more Root CA Certificate(s) and/or Subordinate CA Certificate(s).

Certificate – An electronic document that uses a digital signature to bind a public key and an identity

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

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

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

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

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

Certificate Profile – A set of documents or files that defines requirements for Certificate content and Certificate extensions in accordance with Section 7 of the Baseline Requirements. e.g., a Section in a CA's CPS or a certificate template file used by CA software.

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

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

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

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

EV Certificate – A certificate that contains subject information specified in these Guidelines and that has been validated in accordance with the EV Guidelines.

EV Certificate Request – A request from an Applicant to the CA requesting that the CA issue an EV Certificate to the Applicant, which request is validly authorized by the Applicant and signed by the Applicant Representative.

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

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

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

Key Compromise – A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Generation Script – A documented plan of procedures for the generation of a CA Key Pair.

Key Pair – The Private Key and its associated Public Key.

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

Object Identifier – A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder – An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol – An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder.

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

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

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

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

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

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

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

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

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

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

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

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

Subordinate CA – A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

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

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

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

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

Validity Period – The period of time measured from the date when the Certificate is issued until the Expiry Date.

1.6.2 Acronyms

AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CCTV	Closed Circuit TV
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CV	Curriculum Vitae
DN	Distinguished Name
ECAC	Electronic Certification Accreditation Council
EV	Extended Validation
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol

IETF	Internet Engineering Task Force
ISO	International Standards Organization
NTC	National Telecom Corporation
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Information Number
PKCS#10	Certification Request Syntax Specification
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RSA	Rivest-Shamir-Adelman (The names of the inventors of the RSA algorithm)
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SSL	Secure Sockets Layer
TSA	Timestamping Authority
TLS	Transport Layer Security
TSP	Trust Service Provider (collective term for TCs and PSCEs)
UPS	Uninterruptible Power Supply
URI	Universal Resource Identifier, a URL, FTP address, email address, etc.
URL	Universal Resource Locator
VPN	Virtual Private Network

1.6.3 References

This document refers to the following:

- RFC3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
- RFC5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- AICPA/CPA Canada WebTrust for Certification Authorities Principles and Criteria
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL
- AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Code Signing Baseline Requirements

- Electronic Transaction Ordinance 2002 of Pakistan for Digital Signature and Electronic Certification

2 Publication and Repository Responsibilities

2.1 Repositories

The TSP shall publish and maintain applicable CPS(s), relevant policies, and agreements (Ex. subscriber, RA and relying party agreements), the TSP CA(s) certificates, the TSP CA OCSP responder certificates, TSP CA CRLs and other applicable status information and any other related public documents it issues via an online and publicly accessible website (hereinafter, the TSP public repository).

2.2 Publication of Certification Information

The TSP shall publish a copy of the TSP CA certificate, the TSP CA OCSP responder certificate, as well as this CP on the TSP public repository.

The TSP may also retain other documents that make certain disclosures about its PKI's policies, practices, and procedures as part of the public repository.

The TSP shall publish certificate validity status information in frequent intervals as indicated in this CP. The provision of the certificate validity status information shall be 24/7 available service offered as follows:

- CRLs including any changes since the publication of the previous CRL, at regular intervals. The TSP CA shall 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 TSP CA shall add the OCSP URL in the AIA extension of the Subscribers' certificates.

2.3 Time or Frequency of Publication

Updates of this CP are published within five days of the ECAC PMA approval.

2.3.1 Certificates

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

2.3.2 CRLs

Online (issuing) TSP CAs shall maintain and publish CRLs as follows:

- CRLs shall be refreshed no later than every 24 hours, even if no changes have occurred since the last CRL issuance.
- CRLs lifetime shall be set to 26 hours.

Offline (Intermediary) TSP CAs shall maintain and publish CRLs as follows:

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

2.4 Access Controls on Repositories

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

The TSP shall implement 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 TSP CAs follow the standard X.500 distinguished names. The names must be unique and meaningful.

The tables below specify the DN structures that the TSP shall follow for each of the support certificate types.

3.1.1.1 For Certificates issued to Legal persons:

Attribute	Value
SerialNumber (for EV Code Signing only)	The organization's registration number that is verified according to the EV guidelines. For Government Entities that do not have a Registration Number or readily verifiable date of creation, the TSP SHALL enter appropriate language to indicate that the Subject is a Government Entity
CN	full organization registered name
OU (optional)	unit name within the organization
O	organization's legal name
BusinessCategory (for EV Code Signing only)	The organization's business category that is verified as per the EV guidelines
L (optional if S is present, otherwise mandatory)	organization's locality name
S (optional if L is present, otherwise mandatory)	the state/province that the organization belongs to
Country – "C"	PK

3.1.1.2 For Certificates issued to Natural persons:

Attribute	Value
givenName (optional)	Individual's authenticated given name
surname (optional)	Individual's authenticated surname
SERIALNUMBER (optional)	unique identifier for each individual as constructed by the RA
CN	concatenation of given name and surname separated by a "space" character
OU (optional)	organizational unit name within a legal entity associated with the natural person
O	organization name of a legal entity associated with the natural person
L (optional if S is present, otherwise mandatory)	person's locality name
S (optional if L is present, otherwise mandatory)	the state/province that the person belongs to
Country – "C"	PK

3.1.1.3 Device authentication certificates:

Attribute	Value
CN	system unique common name, unique device identifier or IP address that are applicable
OU (optional)	unit name within the organization
O	organization's legal name
L (optional if S is present, otherwise mandatory)	organization's locality name
S (optional if L is present, otherwise mandatory)	the state/province that the organization belongs to
Country – "C"	PK

VPN certificates:

Attribute	Value
subjectAltName	System unique common name, unique device identifier or IP address that are applicable
CN (optional)	System unique common name, unique device identifier or IP address that are applicable
OU (optional)	unit name within the organization
O	organization's legal name
L (optional if S is present, otherwise mandatory)	organization's locality name
S (optional if L is present, otherwise mandatory)	the state/province that the organization belongs to
Country – "C"	PK

TLS/SSL certificates:

Attribute	Value
SerialNumber (for EV only)	The organization's registration number that is verified according to the EV guidelines. For Government Entities that do not have a Registration Number or readily verifiable date of creation, NTC SHALL enter appropriate language to indicate that the Subject is a Government Entity
subjectAltName	public IP or FQDNs or authenticated domains that are under the control of the Subscriber
CN (optional)	FQDN(s) or public IP address, potentially linked to the subjectAltName
OU (optional)	unit name within the organization
O	organization's legal name
BusinessCategory (for EV only)	The organization's business category that is verified as per the EV guidelines
L (optional if S is present, otherwise mandatory)	organization's locality name

S (optional if L is present, otherwise mandatory)	the state/province that the organization belongs to
Country – "C"	PK

OCSP:

Attribute	Value
CN	friendly name of the TSP CA OCSP service
OU (optional)	unit name within the organization
O (mandatory)	organization's legal name (TSP name)
L (optional if S is present, otherwise mandatory)	organization's locality name
S (optional if L is present, otherwise mandatory)	the state/province where the OCSP operates
Country – "C"	PK

3.1.2 Need for Names to be Meaningful

All end-entity certificates issued by the TSP CA shall be meaningful and shall uniquely identify the subject.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous or pseudonymous subscribers are not permitted.

3.1.4 Rules for Interpreting Various Name Forms

The naming convention used by the TSP CA shall be based on ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.5 Uniqueness of Names

The TSP shall enforce the controls that are necessary to guarantee that subject Distinguished Names (DN) are unique. Minimum controls enforced:

- For certificates issued to natural and legal persons, the TSP shall enforce a convention for a meaningful representation uniquely identifying the person.
- Certificates issued to devices shall uniquely identify the device. Options include using the registered public DNS name or public IP addresses.

3.1.6 Recognition, Authentication, and Role of Trademarks

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

Names can only contain trademarks in case the subscriber has the legal right to use the trademark in question.

For EV TLS Certificates, TSPs shall not allow including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific person or Legal Entity unless it has verified in accordance with the Identity Validation requirements of this document, and the EV Guidelines

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

The TSP RA shall validate the proof of possession of private key by subscribers

3.2.2 Authentication of Organization Identity

3.2.2.1 Identity

The TSP RA shall validate the identity and related information of the organization through a reliable authoritative source that allows the verification of the organization's presence, legal name, authorize representatives, and address. Such sources could be:

- for Government entities: the *Official* Government *Gateway*, and
- for non-Government entities: *"Securities and Exchange Commission of Pakistan" or "Federation of Pakistan Chambers of Commerce & Industry"*

Organization identity validation requirements can be summarized as follows:

1. Verification of presence and legal standing:
   1.1. Verify the existence of the Organization using an authoritative source that provides information on the formation of organization including its legal name, address and a reference of the decree or law issued to establish the organization under its designated name. The TSP RA shall also conduct a site visit to the organization's site to validate the address unless there are other trusted means of verifying the organization's address, that shall be approved by the ECAC PMA.
   1.2. Verify the organization's authorized representative approving the certification request. This can be established either based on the organization's record at the authoritative source or an approved a formal communication between the TSP and the organization, the type and requirements of such communication need to be approved by the ECAC PMA.
2. Verification of association with the certificate subject: The TSP RA shall verify that the organization name to be inserted in the certificate matches the legal name of the organization requesting the certificate. The full organization's name of an abbreviated version can be included in the certificate.

For EV TLS & Code Signing certificates, TSPs shall conduct additional verifications related to legal, physical and operational existence of the organization according to section 11 of the EV guidelines.

3.2.2.2 Authentication of Domain name

For SSL/TLS certificates, the control or ownership of the domain name(s) which is/are specified in the certificate application shall be verified.

Control or ownership of the domain portion of email addresses shall be verified before delegating the issuance of S/MIME certificates.

3.2.3 Authentication of Individual Identity

3.2.3.1 Tools and mechanisms for Authentication of Individual Identity

This section defines tools and types of mechanisms that can be used for identification and authentication of an individual's identity.

3.2.3.1.1 Types of evidences:

Primary Evidences:

Primary evidences are defined as governmental authoritative sources including secure photo ID evidence, issued with robust identity proofing, issuance and management processes. Examples of Primary evidences are: passports, (electronic) citizen identity cards, (electronic) resident identity cards, (international) driving license, civil servant cards, police forces identification cards.

Secondary Evidences:

Secondary evidences are government authoritative sources that are supported by moderate identity proofing, issuance and management processes. Examples of Secondary evidences are: professional corporation card (e.g. Bar association, Healthcare professional association), population register excerpts, tax register excerpts, social security register excerpts.

3.2.3.1.2 Authoritative source

An authoritative source is any source, irrespective of its form, that is nationally trusted to provide valid and accurate data, information and/or evidence that can be used to prove the identity of an individual. A source may only be authoritative for the data provided by it.

It is important to ensure that an information claimed to be provided by a claimed authoritative source is authentic, i.e. that it originates from a known authoritative source, is genuine and its integrity has been verified.

Examples of authoritative sources can include:

- National Population registers for information on person's identity data,
- Government registers which have associated governing processes to ensure reliable and correct data such as passport registers, driving license databases, tax registers, social security registers,
- Official identity documents such as passports and identity cards.

3.2.3.2 Identity validation requirements

Certificate type	Identity validation requirements

• Natural person certificates for A**dvanced** electronic signatures
• Natural person certificates for authentication
• Natural person certificates for email protection
	The TSP shall verify the applicant's identity lawfulness as follows:
	• Verify that the applicant's email address exists, and that the subscriber has control over an existing email address (i.e. ownership and control of email)
	• Verify a Primary or Secondary pieces of evidence of the following
	  ○ Applicant's full name, and date and place of birth,
	  ○ Linkage between the identity of the Subject of the certificate and a legal

	person (organization, corporation) identity when the subject is a natural person who is identified in association with a legal person • Validate the authenticity of submitted evidence to establish that: - They are valid pieces of evidence: Checking should rely on national guidance on how to verify the authenticity and security features of national official identity documents. With regards to foreign identity documents, checking may rely on the guidance provide on PRADO (Public Register of Authentic travel and identity Documents Online)1 or any similar database or guidance on how to verify some of the most important security features of official documents issued around the world. - The identity is not that of a deceased person (individual).
	The TSP shall verify the link between the claimed identity and the claimant through the following mechanisms: • By an RA office through authentication credentials exchanged with the claimant using his verified email address and/or a mechanism that involves live video session with the claimant that involves the presentation of a "Primary evidence" or "Secondary evidence" used earlier. • Existing authentication credentials from accepted Identity Providers in Pakistan provided that the following requirements are met: - Existence of ID proofing artifacts substantiate the antecedent verification outcome - Mechanisms are in place that bind the individual to the asserted identity
• Natural person certificates for **Qualified** electronic signatures	**The TSP shall verify the applicant's identity lawfulness as follows**: • Verify that the applicant's email address exists, and that the subscriber has control over an

[1] https://www.consilium.europa.eu/prado

	existing email address (i.e. ownership and control of email)
	• Primary and Secondary pieces of evidence of the following
	  ○ Applicant's full name, and date and place of birth,
	  ○ Linkage between the identity of the Subject of the certificate and a legal person (organization, corporation) identity when the subject is a natural person who is identified in association with a legal person
	• Validate the authenticity of submitted evidences to establish that:
	- They are valid pieces of evidence: Checking should rely on national guidance on how to verify the authenticity and security features of national official identity documents. With regards to foreign identity documents, checking may rely on how to verify some of the most important security features of official documents issued around the world.
	- The identity is not that of a deceased person.
	The TSP shall verify the link between the claimed identity and the claimant through the following mechanisms:
	TSPs shall verify the link between the claimed identity and the claimant as part of a physical in-person interview or equivalent via one of following methods:
	- Visual face-matching by an RA office through a video session with the claimant that involves the presentation of "Primary evidence",
	- Biometric verification involving face matching and liveness detection according to standards related to Presentation Attack Detection.

3.2.4 Non-verified Subscriber Information

All information included in the DN shall be checked and authenticated by the TSP RA.

3.2.5 Validation of Authority

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

1. The TSP RA receives a legible copy of a valid government-issued photo ID for the certificate requester. The ID copy shall be inspected for indication of alteration or falsification,
2. The TSP RA receives a completed and signed certificate request form from the requestor. The form is signed by the authorized representative, that attests the authority of the requestor,
3. The TSP RA verifies the authority of the authorized representative through an authoritative source or an approved formal communication with the organization,
4. The TSP RA validate the identity of certificate Requester using similar methods to those specified in section 3.2.3.2.

For EV TLS & Code Signing certificates, TSPs shall conduct additional verifications related validation of Authority according to section 11 of the EV guidelines.

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 shall be performed as in initial registration.

3.3.2 Identification and Authentication for Re-key after Revocation

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

3.4 Identification and Authentication for Revocation Request

The TSP RA shall enforce identification and authentication for revocation requests.

The TSP RA shall validate the revocation request and the identity of the revocation request applicant.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

For Government TSPs, certificate applications can be submitted by Government employees.

For Commercial TSPs, certificate applications can be submitted by the community for such TSPs (that shall be limited to the TSP's employees (and contractors)) or to a user base that a TSP is authorize to service by law.

Further details and restrictions shall be specified in the applicable TSP CPS.

4.1.2 Enrollment Process and Responsibilities

For any requested certificate, the subscriber shall ratify a dedicated subscriber agreement.

Further details on the enrolment process shall be specified in the applicable TSP CPS.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Detailed vetting procedures shall be documented as part of the overall certificate application in the applicable TSP CPS. The TSPs' vetting procedures shall conform with the following requirements:

1. General requirements for all certificate applications:
    a. The RA shall assign a unique ID to each certificate application record,
    b. The RA shall store 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 shall be added to a blacklist, the blacklist shall include the necessary details to avoid ambiguously in identifying future malicious requests,
    d. The RA shall conduct a blacklist check against the RA's own blacklist. If the applicant is in the blacklist, the certification application is rejected,
    e. The applicant shall sign or ratify a dedicated subscriber agreement.
2. Requirements specific to applicant/certificate type:
    a. For natural person certificates:
        i. The RA shall validate the applicant's identity as described in section 3.2.3, In case of negative outcome, the verification procedure stops, otherwise, the vetting procedure continues,
        ii. The RA shall validate the Linkage between the identity of the Subject of the certificate and a legal person (organization, corporation) identity when the subject is a natural person who is identified in association with a legal person,
    b. For eSeal/Code Signing certificates

i. The RA validates the organization's identity as described in section 3.2.2. In case of negative outcome, the verification procedure stops, otherwise, the vetting procedure continues,
ii. Establish government entity authorized representative as described in section 3.2.2,
iii. Identify authorized certificate requestor as specified in section 3.2.5.
iv. For EV Code Signing, the Applicant is required to demonstrate control of any email address to be included in a Certificate.

c. For SSL/TSL/VPN certificates:
   i. The RA shall validate the organization's identity, authorized representatives and certificate requestor as mentioned in point (b) above,
   ii. In case of having the wildcard character (*) in the CN or subjectAltName, the following restrictions shall 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 rejected unless the applicant proves its rightful control of the entire Domain Namespace.
   iii. The RA shall verify the validity of TLD included in the certificate request,
   iv. The RA shall verify for any of the domains to be included in the certificate is a high-profile domain, if yes then the certificate application is rejected,
   v. The RA shall check the CAA records for the domain(s) to verify the authority of the CA to issue a TLS certificate for that domain(s),
   vi. The RA shall verify ownership of the domain name using any of the approved methods under section 3.2.2.4 of the CA/Browser Forum Baseline Requirements,
   vii. The RA shall verify the ownership of the domain name using any of the approved methods under section 3.2.2.5 of the CA/Browser Forum Baseline Requirements.

d. For device authentication certificates:
   i. The RA shall validate the organization's identity, authorized representatives and certificate requestor as mentioned in point (b) above,
   ii. The RA shall verify the IT system/device and the control by certificate requester as follows:
      1. Identify the IT system/device for which certificate(s) shall be issued. The IT system/device must be part of the IT infrastructure of the organization that the requester belongs to,
      2. Verify that the requester is a legitimate sponsor or authorized device or system administrator of the device or system for which certificate(s) shall be issued.

4.2.2 Approval or Rejection of Certificate Applications

The certificate application approval shall be contingent to the following:

- Subject and applicant identity verification,
- Proof of possession of private key,
- Proof of ownership of the device, when applicable,
- Proof of association with an organization, when applicable,
- Any other conditions or constraints such as defined in the CPS.

The TSP CPS shall describe further details on the criteria of approval or rejection of applications.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The TSP CA shall process a certificate issuance as follows:

- Verify that the certificate request initiated from an authorized RA,
- Issue the certificate with required type identified by a Policy OID identified in the TSP CPS. The issued certificate shall include the information provided in the certificate request.

The TSP shall specify further details on the CA actions as part of the applicable TSP CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The TSP CPS shall specify further details on notifications.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The subscriber shall be given a mechanism to verify that the issued certificate contains required information as per the certificate application. The TSP shall define a criterion of declaring certificate acceptance by the subscriber.

The TSP CPS shall specify further details on certificate acceptance.

4.4.2 Publication of the Certificate by the CA

The TSP CA may publish the issued certificates on the TSP public repository as specified in section 2.2.

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 shall adhere to the following obligations:

- Use the private key and corresponding certificate only for their intended usage as per this CP and the applicable TSP CPS,
- Cease using a private key following expiration or revocation of the corresponding certificate,
- Inform the RA, without any delay, in the event of private key compromise.

4.5.2 Relying Party Public Key and Certificate Usage

A party relying on a certificate issued by the TSP CA shall:

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

4.6 Certificate Renewal

Certificate Renewal is the 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 shall not be supported.

4.6.1 Circumstance for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-Key

Certificate Re-key is the process of issuing of a new certificate to the subscriber with a new public key and validate period while the other information in the certificate may remain same.

4.7.1 Circumstance for Certificate Re-Key

Certificate re-key may happen while the certificate is still active, after it has expired, or after a revocation.

The certificate re-key shall invalidate any existing active certificates of the same type.

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

This CP does not specify provisions for certificate modification outside the context of certificate re-key, which results in the generation of a new certificate with the same identification information. Refer to section 4.7 for further details.

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

4.9.1 Circumstances for Revocation

The TSP CA shall revoke an issued certificate under the following circumstances:

- Upon request from the subscriber or a representative
- Knowing that the information on the certificate is no longer accurate
- Discovering that the certificate was issued in a manner not materially in accordance with the procedures required by this CP / the applicable TSP CPS
- Determination that the certificate was issued to a subject other than the one named as the subject of the certificate
- The subscriber has been declared legally incompetent
- Obtaining an evidence that the certificate was misused
- Obtaining or discovering evidence that subscriber's private key, corresponding to the public key certificate, has been compromised or that there is a demonstrated or proven method that exposes the subscriber's private key to compromise
- Receiving a lawful order from a law enforcement organization in Pakistan to revoke a certificate
- The subscriber has been declared legally incompetent

The TSP CPS shall specify additional relevant revocation circumstances in full compliance with applicable requirements.

This CP does not specify circumstances for revoking an OCSP certificate or other certificates belong to the TSP CA itself apart from the compromise of the related key pair, which shall be considered by the TSP as a disaster and treated as such in conformance with its disaster recovery and business continuity procedures.

The following sub-sections focus only on the revocation provisions that apply to end-entity certificates issued by the TSP CA.

4.9.2 Who Can Request Revocation

The subscriber shall be able to request the revocation of his/her certificate.

The RA shall be allowed to revoke subscriber certificates.

Only authorized revocation requests shall be accepted by the RA.

The TSP CPS shall specify further details on who can request revocation.

4.9.3 Procedure for Revocation Request

The TSP CPS shall specify further details on the revocation procedure.

4.9.4 Revocation Request Grace Period

There should not be a grace period for revocation. However, the TSP may specify a grace period based on further provisions in section 4.91 of the applicable TSP CPS.

4.9.5 Time Within Which CA Must Process the Revocation Request

Certification revocation requests and problem reports shall be processed within 24 hours from their reception.

4.9.6 Revocation Checking Requirement for Relying Parties

Certificate revocation information is offered to relying parties through CRLs published on a publicly available repository or through its OCSP responder.

Relying parties shall use any of these methods while processing a certificate issued by a TSP CA.

4.9.7 CRL Issuance Frequency (If Applicable)

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

4.9.8 Maximum Latency for CRLs (if applicable)

Not stipulation.

4.9.9 On-Line Revocation/Status Checking Availability

The TSP OCSP responders shall conform to RFC 6960.

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

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

4.9.10 On-Line Revocation Checking Requirements

The TSP OCSP responders shall support both HTTP GET and HTTP POST methods.

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

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

4.9.11 Other Forms of Revocation Advertisements Available

Not stipulation.

4.9.12 Special Requirements related to Key Compromise

Not stipulation.

4.9.13 Circumstances for Suspension

Certificate suspension shall not be supported.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

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

OCSP responder exposes an HTTP interface accessible to relying parties.

4.10.2 Service Availability

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

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

The TSP CPS shall specify the conditions for ending the subscriptions from the TSP subscribers.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Key escrow shall not be supported.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Session key encapsulation shall not be supported.

5 Facility, Management, and Operational Controls

This section specifies the minimum physical and procedural security controls that need to be implemented by TSPs.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

All critical components of the TSP PKI solution shall be housed within a dedicated secure enclave either in a facility owned by TSP or rented from a reliable service provider in Pakistan.

Physical access controls shall protect the infrastructure, management systems and related operational activities of the TSP PKI solution

5.1.2 Physical Access

Physical security controls shall be enforced so that access of unauthorized persons is prevented through at least four tiers of physical security.

Physical security controls include security guard-controlled building access, biometric access, and CCTV monitoring shall protect the CA systems from unauthorized access, these controls are monitored on a 24x7x365 basis. Further, access to the secure enclave where the PKI systems are hosted shall be enabled only if two trusted employees are present to open the enclave's door.

5.1.3 Power And Air Conditioning

The secure enclave shall be equipped with a UPS, heating ventilating and air conditioning (HVAC) sufficient to maintain the computer equipment within the manufacturers' recommended range of operating temperatures and humidity.

5.1.4 Water Exposures

The TSP shall take reasonable precautions to minimize the impact of water exposure on the TSP PKI hosting facility.

5.1.5 Fire Prevention and Protection

The TSP PKI hosting facility shall follow leading practices and applicable safety regulations in Pakistan, monitored 24x7x365 and equipped with fire and heat detection equipment.

5.1.6 Media Storage

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

Audit and backup storage media shall be stored in a secure fire-proof safe and duplicated and stored in a secure offsite 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

System backups must provide sufficient recovery information to allow the recovery from system failure(s).

Backups shall be made on a daily basis and copies shall be transferred to a secure offsite location on a periodic basis.

Facilities used for offsite backup and archives shall have the same level of security as the TSP CA main site.

5.2 Procedural Controls

The TSP CA shall follow personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the CA staff members, and the satisfactory performance of their duties in the field of PKI governance, operations, and service delivery.

5.2.1 Trusted Roles

All members of the staff operating the key management operations, administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position (i.e., trusted operatives).

The TSP shall conduct a clearance check of all members of staff who are candidates to serve in trusted roles as a due diligence attempt to determine their trustworthiness and competence.

5.2.2 Number of Persons Required per Task

The TSP shall maintain and enforce rigorous control procedures to ensure the segregation of duties, based on job responsibility, to prevent single trusted personnel to perform sensitive operations.

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

- Physical access to the secure enclave where the CA systems are hosted,
- Access to and management of CA cryptographic hardware security module (HSM),
- Validate and authorize the issuance of certificates.

5.2.3 Identification and Authentication for each Role

Before exercising the responsibilities of a trusted role:

- The TSP confirms the identity and history of the employee by carrying out background and security checks
- The TSP issue access credentials to the designated personnel who need to access equipment located in the secure enclave.

- The TSP provide the necessary credentials that allow designated personnel to conduct their functions.

5.2.4 Roles Requiring Separation of Duties

The TSP shall ensure separation of duties among the following work groups:

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

5.3 Personnel Controls

The TSP shall ensure implementation of security controls regarding the duties and performance of the members of the CA staff members.

These security controls shall be documented in an internal policy, yet it shall include the areas below.

5.3.1 Qualifications, Experience, and Clearance Requirements

The TSP 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

The TSP shall make the relevant checks on prospective staff members by means of status reports issued by a competent authority or third-party statements.

5.3.3 Training Requirements

The TSP shall make available relevant technical training for their staff members to perform their functions.

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

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

5.3.4 Retraining Frequency and Requirements

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

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

The TSP shall sanction personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems for the purpose of imposing accountability on the TSP CA staff, as it might be appropriate under the circumstances and as per the prevailing HR Policy and Country Law.

5.3.7 Independent Contractor Requirements

Independent contractors and their personnel are subject to the same background checks as the CA 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 TSP shall make available documentation to the CA staff describing their duties and the operational processes they are fulfilling.

5.4 Audit Logging Procedures

Details on the audit logging procedures shall be defined in the TSP CPS.

This CP specifies minimum requirements on audit logging procedures as per the following sections.

5.4.1 Types of Events Recorded

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

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

Following events occurring in relation to the TSP CA operations shall be recorded:

- CA key life cycle management events, including:

- Key generation, backup, storage, recovery, archival and destruction
- Cryptographic device life-cycle management events

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

5.4.2 Frequency Of Processing Log

The TSP shall ensure that the designated personnel reviews log files at regular intervals to validate log integrity and ensure timely identification of anomalous events.

Designated personnel shall report and perform follow-up of these events and any issues affecting audit log integrity.

Evidence of audit log reviews, outcome of the review process, and executed remediation actions shall be collected and archived

5.4.3 Retention Period for Audit Log

The TSP CA shall retain the following, for at least two (2) years:

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

While these Requirements set the minimum retention period, the TSP may choose a greater value as more appropriate to be able to investigate possible security or other types of incidents that will require retrospection and examination of past audit log events.

5.4.4 Protection Of Audit Log

Audit logs shall be protected by a combination of physical, procedural and technical security controls.

5.4.5 Audit Log Backup Procedures

The following rules apply for the backup of the TSP CA audit log:

- Backup media are stored locally in the TSP CA main site, in a secure location
- A second copy of the audit log data and files are stored in an offsite location that provides similar physical and environmental security as the main site

5.4.6 Audit Collection System (Internal vs. External)

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 TSP shall determine 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 TSP shall perform annual risk assessments on their CA systems to cover the following scope:

- Identification of potential internal and external threats that could result in the compromise of the CA systems and assets
- Assessment of the likelihood and potential damages of the identified threats
- Review of the residual risks considering the implemented controls in place
- Definition of new arrangements/controls as applicable to mitigate the residual risks
- Alignment with the TSP management on a plan to implement the new arrangements/controls

5.5 Records Archival

5.5.1 Types of Records Archived

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

A. Documentation related to the security of CA systems, and Delegated Third Party Systems (Ex. RAs), and
B. Documentation related to their verification, issuance, and revocation of certificate requests and Certificates.

5.5.2 Retention Period for Archive

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

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

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

While these Requirements set the minimum retention period, the TSP may choose a greater value as more appropriate in order to be able to investigate possible security or other types of incidents that will require retrospection and examination of past records archived.

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

The TSP CPS or related documentation shall provide details on how archive records are backed up.

5.5.5 Requirements for Timestamping of Records

All recorded events by the TSP CA shall include the date and time of when the event took place, based on the time of the operating system.

The TSP CPS shall specify further details including the controls in place to ensure that all CA systems rely on and are synchronized with a reliable time source.

5.5.6 Archive Collection System (Internal or External)

Only authorized and authenticated personnel shall be allowed to handle archived material.

5.5.7 Procedures to Obtain and Verify Archive Information

Only TSP staff members with a clear hierarchical control and a definite job description may obtain and verify archived information. The TSP shall retain records in electronic or paper-based format.

5.6 Key Changeover

The TSP may periodically changeover its CA keys.

Private keys may be maintained until such time as all relying certificates have expired.

5.7 Compromise And Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

The TSP shall specify applicable incident, compromise reporting and handling procedures as part of its business continuity and disaster recovery plan.

The TSP shall specify 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 TSP and all other PKI Participants (other than Subscribers and Relying Parties) shall establish the necessary measures to ensure full recovery of the TSP CA services in case of a disaster, and corrupted servers, software, or data.

The TSP shall implement:

- Disaster recovery solution in a location sufficiently distant from the CA main site,
- Reliable communication between the two sites (for data replication etc.),
- Disaster recovery infrastructure and procedures shall be fully tested at least once a year.

5.7.3 Entity Private Key Compromise Procedures

For Subscribers key compromise, see section 4.9.

In the event of a key compromise of a TSP CA, the following actions shall be taken by the TSP:

- The ECAC PMA shall be notified as soon as there is an indication of suspected compromise. The TSP shall work together with the ECAC PMA on deciding whether to continue TSP CA activities or cease operations. If it is decided to revoke the TSP CA certificate:
    - The subscribers holding active end-entity certificates shall be notified,
    - The ECAC PMA shall decide with the TSP whether a new certificate is going to be issued to the TSP CA.
- A TSP CA compromise notice shall be published toward relevant relying parties.

5.7.4 Business Continuity Capabilities after a Disaster

The TSP shall establish the necessary measures to ensure full recovery of the CA services in case of a disaster, corrupted servers, software or data. These measures shall be specified in the TSP business continuity and disaster recovery plan, to be implemented to ensure business continuity following a natural or other disaster.

The TSP business continuity and disaster recovery plan shall define at least the following:

- Conditions for activating the plan
- Fall-back and resumption procedures
- The responsibilities of the individuals involved in the plan execution
- Recovery time objective (RTO)
- Recovery procedures

- The plan to maintain or restore the business operations in a timely manner following interruption to or failure of critical business processes
- Key termination plan (in case of TSP CA key compromise)
- Procedures for securing the main facility to the extent possible during the period following a disaster and up to recovery of operations in a secure environment in either the main, or secondary site.

5.8 CA or RA Termination

If the TSP and/or the ECAC PMA determine that termination of the TSP CA services is deemed necessary, the TSP shall initiate a termination plan that should have been agreed with the ECAC PMA as part of the TSP onboarding.

The TSP termination plan shall cover the below minimum aspects:

a. Provide a written notice to the ECAC PMA of its intention to cease operating its TSP CA activities, together with a copy of the TSP's termination plan, at least ninety (90) days before:
   i. the date when it will cease to the TSP CA related activities,
   ii. expiry, when applicable, of the TSP authorization for providing its TSP CA activities, where the TSP has no intention to apply for an authorization renewal.
b. The TSP arrangement for the retention of archived logs (as set forth in Section 5.5),
c. The TSP arrangement for maintaining the validation status services URLs as mentioned in the certificates that would still be valid at the moment of termination, until expiry of the latest certificate,
d. Communications towards subscribers of its intention to terminate its TSP-CA activities within at least sixty (60) days before effective termination or the expiry of its authorization, whichever occurring first,
e. Advertisements about the TSP intention to terminate its TSP CA activities within at least sixty (60) days before effective termination or the expiry of its authorization, whichever occurring first, in daily newspapers, or by such other mediums and in the manner the ECAC PMA may determine,
f. Communications towards relevant parties and for transferring archived TSP CA records to an appropriate custodian,
g. Plan to assist (as much as possible) the TSP's subscribers with a transition to another TSP,
h. Revoke all certificates, issued by the TSP-CA, that remain unrevoked or unexpired at the end of the notice period, whether or not the subscribers have requested a revocation.
i. Undertake the necessary measures to ensure that discontinuing its operations does not cause disruption to its subscribers and relying parties.
j. Arrangements to adequately ensure the ongoing maintenance of its systems and security measures for sensitive and accurate data,

k. Addressing any other requirements set forth in the national accreditation framework.

6 Technical Security Controls

This section specifies the minimum key management requirements that need to be implemented by TSPs.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 TSP CAs:

The TSP CA key pairs shall be generated within the memory of an HSM certified as meeting the requirements of section 6.2.11.

The TSP CA Key Generation Ceremony shall be video recorded and stored securely for auditing purposes.

The TSP-CA Key Generation Ceremony shall be witnessed by an internal/external auditor with the aim to produce a report opinion that the TSP CA:

- Documented its CA key generation and protection procedures in compliance with this CP and the applicable CPS,
- Included appropriate detail in its CA Key Generation Script,
- Executed in the in presence of a quorum of authorized personnel including representatives from the ECAC PMA,
- Maintained effective controls to provide reasonable assurance that the CA key pair was generated and protected in conformity with the procedures described in this CP, the applicable CPS,
- Performed, during the CA key generation process, all the procedures required by its CA Key Generation Script.

6.1.1.2 Subscribers

Subscribers' key pairs shall be generated with sufficient security maintained during the key generation process and during the delivery of these keys and corresponding certificate to the subscriber. Subscriber keys shall be generated using [FIPS 186-4] approved methods.

6.1.2 Private Key Delivery to Subscriber

6.1.2.1 TSP CAs

The TSP CA keys shall be generated in the HSM as part of the KGC ceremony.

6.1.2.2 Subscribers

When the TSP generates subject's key pairs, these shall be generated within the memory of cryptographic devices conforming to FIPS 140 Level 2 at minimum and shall be delivered to subscribers using secure communication channel.

6.1.3 Public Key Delivery to Certificate Issuer

The TSP RA's shall only accept Public Keys from Subscribers in accordance with Section 3.2 of this CP.

6.1.4 CA Public Key Delivery to Relying Parties

The TSP shall make its TSP CA certificates available to subscribers and relying parties by publishing them at the TSP public repository.

The TSP CA's public keys will be also made available on the Trusted List.

6.1.5 Key Sizes

Subscriber keys shall be at least 2048-bit RSA, recommended 4096-bit RSA or at least 256-bit ECDSA, recommended 384-bit ECDSA.

TSPs shall ensure that the keys used for EV certificates are compliant with the requirements set forth in the EV guidelines.

6.1.6 Public Key Parameters Generation and Quality Checking

The TSP shall rely on off-the-shelf implementation of key PKI functionality including public key parameters generations. The TSP private and public keys generation shall be done in compliance to the Baseline Requirements Section 6.1.6 on quality checking.

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

Certificates issued by the TSP CA shall contain a key usage bit string in accordance with [RFC 5280].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The TSP shall generate its TSP CA key pairs and store their private keys within an HSM that is certified according to the rating specified in 6.2.11.

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

With regards to TSP CA private key shared control, the TSP shall implement technical and procedural mechanisms that implement the principles of dual control and split knowledge. These principles guarantee the participation of multiple trusted individuals for performing sensitive operations with TSP CA cryptographic hardware.

6.2.3 Private Key Escrow

Private keys of the TSP CA may not be escrowed.

6.2.4 Private Key Backup

The TSP CA private keys are backed up, stored and recovered by multiple and appropriately authorized members of the TSP CA related staff serving in trusted roles. More than one member of the TSP CA management shall authorize key backup and shall assign personnel in writing.

A back-up of the generated key material is taken and stored under the same security measures as the primary key material.

6.2.5 Private Key Archival

Not applicable.

6.2.6 Private Key Transfer into or from a Cryptographic Module

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

At no time shall the TSP CA private key 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 TSP CAs

The TSP CA private keys shall be activated using the principles of dual control and split knowledge.

The activation procedure shall involve multi-factor authentication of the HSM admins and key custodians.

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 TSP CAs

The TSP CAs' private keys shall be deactivated in situations such as:

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

6.2.9.2 Subscribers

Activation and deactivation of subscriber's private key depends on the type of certificate and their storage location. This shall be described in the TSP CA CPS and subscriber's agreement.

6.2.10 Method of Destroying Private Key

6.2.10.1 TSP CAs

Destruction of the TSP CA keys outside the context of the end of its lifetime shall be authorized by multiple members of the TSP management.

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

6.2.10.2 Subscribers

Destruction of subscriber's private key depends on the type of certificate and their storage location. This shall be described in the TSP CA CPS and subscriber's agreement.

6.2.11 Cryptographic Module Rating

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

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Refer to Section 5.5 for archival conditions.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The TSP CA Certificate validity shall be at least:

- The maximum validity of a Subscriber certificates, Plus
- the CA key usage period that shall be decided by the TSP based on a proper risk assessment, Plus
- the estimate time for planning and executing the TSP CA re-key activities.

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

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

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 TSP CAs

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

6.4.1.2 Subscribers

When the TSP is responsible for the subscribers' key generation, the activation data shall be randomly generated by the CA/RA. This activation data shall be securely delivered to the subscriber.

6.4.2 Activation Data Protection

The TSP CAs private keys and HSM activation data shall be protected from disclosure by means of cryptographic key material management procedures documented by the TSP in its applicable TSP CPS.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications shall be tested, developed and implemented in accordance with industry best practice development and change management standards.

Purchased hardware or software shall be shipped or delivered in a sealed or shrink-wrapped container and be installed by trained personnel.

6.6.2 Security Management Controls

A formal configuration management methodology shall be used for installation and on-going maintenance of the CA systems.

There shall be a mechanism for detecting unauthorized modification to the CA systems' software or configuration.

The CA software, when first loaded, is checked as being that supplied from the vendor, with no modifications, and is the version intended for use.

6.6.3 Life Cycle Security Controls

Refer to Section 6.6.1 for details.

6.7 Network Security Controls

The TSP shall ensure maintenance of network security, including managed firewalls and intrusion detection systems, to ensure that the CA systems are protected against denial of service and intrusion attacks.

The network shall be segmented into several zones, based on their functional, logical and physical relationship. Network boundaries shall be enforced to limit the communication

between systems deployed within different zones. Components shall be hardened so that only the services, protocols, ports, and communications that the CA has identified as necessary to its operations are activated.

6.8 Timestamping

The TSP CA servers' internal clock shall be synchronized with a reliable time source.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The TSP shall document the profiles of the certificates its issues in the TSP CA CPS in compliance with the requirement set forth in this section.

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

The TSP CA shall issue certificates with X.509 v3 extensions as defined in RFC 5280 in addition to extensions indorsed by the CA/Browser Forum. Section 7.1 of the applicable CPS shall specify details of the contents of the certificates issued by the TSP CA.

7.1.3 Algorithm Object Identifiers

X.509 v3 standard OIDs shall be used. Algorithm shall be RSA encryption for the subject key and SHA256 with RSA encryption for the certificate signature.

7.1.4 Name Forms

As per the naming conventions and constraints listed in section 3.1 of this CP.

7.1.5 Name Constraints

Name constraints are supported as per RFC 5280.

7.1.6 Certificate Policy Object Identifier

The TSP may use its own OID scheme in addition to other OIDs indorsed by the ECAC PMA and the CA/Browser Forum.

7.1.7 Usage of Policy Constraints Extension

Policy Constraints extension shall not be supported.

7.1.8 Policy Qualifiers Syntax and Semantics

The use of policy qualifiers defined in RFC 5280 shall be supported.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificate policies extensions must be processed as per RFC 5280.

7.2 CRL Profile

The TSP shall document the profiles of the CRL its issues in the TSP CA CPS in compliance with the requirement set forth in this section.

7.2.1 Version Number(S)

The TSP CAs shall support X509 v2 CRLs.

7.2.2 CRL and CRL Entry Extensions

The CRL extensions shall contain the CRL number (a sequential number incremented with each new CRL produced).

7.3 OCSP Profile

The OCSP profile shall comply with the requirements of RFC 6960.

OCSP response signing certificates must the use of the following extensions:

- Key usage (not critical)
- Authority key ID (not critical)
- Extended key usage (critical)
- OCSP no check (not critical)

The TSP shall document further details on the OCSP certificate profile in the applicable CPS.

7.3.1 Version Number(s)

The TSP CA shall support the v1 OCSP responses according to RFC 6960.

7.3.2 OCSP Extensions

No stipulation.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

Based on the types of certificates (certificate usage based on the EKU extension) that the TSP CA can issue, The TSP shall organize an external WebTrust covering applicable criteria to ensure that it meets applicable requirements, standards, procedures, and service levels at least on an annual basis.

The TSP accepts this auditing of its own practices and procedures and makes the audit report publicly available no later than three months after the end of the audit period. The TSP and the ECAC PMA evaluate the results of such audits before further implementing them.

In addition, the ECAC PMA may conduct the compliance verification directly on the TSP or appoint an auditor to do the verification on their behalf to cover other requirements under the national accreditation framework.

8.2 Identity/Qualifications of Assessor

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

- Independence from the subject of the audit
- Ability to conduct an audit that addresses the criteria specified in WebTrust for Certification Authorities
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and third-party attestation function
- Licensed by WebTrust
- Bound by law, government regulation or professional code of ethics
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

External auditors shall be independent third party WebTrust practitioners.

8.4 Topics Covered by Assessment

For WebTrust audits, the types of certificates (certificate usage based on the EKU extension) that the TSP CA can issue determine the combination from the following standards to be covered in the audit:

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

8.5 Actions Taken as a Result of Deficiency

Issues and findings resulting from the assessment are reported to the TSP management as well as the ECAC PMA.

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

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

8.6 Communication of Results

The overall results of audits shall be reflected by the ECAC PMA on the Trusted List.

External audits reports are published on the TSP public repository.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The TSP may charge fees for certificate issuance and renewal. Details with regard to fees shall be documented in the applicable TSP CPS.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation Or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Each PKI Participant, except the Relying Parties, will maintain appropriate insurance to meet its obligations under this CP and will maintain a sufficient amount of insurance coverage for its liabilities to other Participants, including Subscribers and Relying Parties.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The TSP shall consider the following as confidential information:

- Subscriber's personal information that are not part of certificates or CRLs
- Correspondence between and the RA function during the certificate management processing (including the collected subscriber's data)
- Contractual agreements between the TSP and its suppliers
- TSP 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 by the TSP shall be deemed public. This includes the information published on the TSP's repository.

9.3.3 Responsibility to Protect Confidential Information

The TSP shall protect confidential information through training and policy enforcement with its employees, contractors and suppliers.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The TSP shall observe personal data privacy rules and privacy rules as specified in the present CP. Refer to section 9.4.2 for the scope of private information and to section 9.4.3 for the items that are not considered as private information.

Both private and non-private information can be subject to data privacy rules if the information contains personal data.

Only limited trusted personnel are permitted to access subscriber private information for the purpose of certificate lifecycle management.

The TSP shall not release any private information without the consent of the legitimate data owner or explicit authorization by a court order. When the TSP releases private information, the TSP shall ensure through reasonable means that this information is not used for any purpose apart from the requested purposes. Parties granted access will secure the private data from compromise, and refrain from using it or disclosing it to other third parties. Also, these parties are bound to observe personal data privacy rules in accordance with the relevant laws in the Islamic Republic of Pakistan.

The TSP shall respect 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 TSP/its RA shall preserve the privacy and confidentiality of any exchanged private information. Data encryption shall be used when electronic communication channels are used with the CA systems. This shall include:

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

9.4.2 Information Treated as Private

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

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

The TSP employees, suppliers and contractors handle personal information in strict confidence under the TSP 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 TSP shall ensure that collected personal information is used for the purpose of certificate life cycle management only as consented by the subscribers.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The TSP shall 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 TSP may own and reserve all intellectual property rights associated with its own databases, web sites, the CAs' digital certificates and any other publication whatsoever originating from the PKI, including this CP.

When the TSP uses software from third party suppliers, it shall ensure that intellectual property rights of the supplier are maintained. This shall be defined in the supplier's license agreement.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The TSP shall warrant that their procedures are implemented in accordance with this CP and the corresponding TSP CPS, and that any certificates issued under the TSP CPS are in accordance with the stipulations specified.

For EV certificates, the TSPs shall adhere to representations and warranties requirements set forth in the EV Guidelines.

9.6.2 RA Representations and Warranties

The TSP shall warrant that it performs RA functions as per the stipulations specified in the TSP CPS.

9.6.3 Subscriber Representations and Warranties

The TSP shall warrant that each subscriber signs a subscriber's agreement with the TSP that lists the subscriber's obligations. The TSP shall use its own CPS to convey legal conditions of usage of certificates to subscribers.

9.6.4 Relying Party Representations and Warranties

The TSP shall use its own CPS to convey conditions of usage of certificates to be honored by relying parties.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers Of Warranties

TSPs may not disclaim any responsibilities or obligations described in this CP. Any such disclaimers of warranties shall be documented in the TSP's CPS and reviewed/validated by the ECAC PMA.

9.8 Limitations of Liability

The total liability of the TSP CAs may be limited provided that TSP operations remain compatible with the provisions of this TSP CP. Such limitations of liability shall be documented in the TSP's CPS and the ECAC PMA.

9.9 Indemnities

No stipulation.

9.10 Term And Termination

9.10.1 Term

The present TSP CP is approved by the ECAC PMA and shall remain in force until amendments are published on the ECAC repository and relevant communication towards TSPs occurred.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

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

9.11 Individual Notices and Communications with Participants

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

9.12 Amendments

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

9.12.1 Procedure for Amendment

Refer to Section 9.12.

9.12.2 Notification Mechanism and Period

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

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

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

9.12.3 Circumstances under which OID Must Be Changed

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

9.13 Dispute Resolution Provisions

The ECAC PMA shall facilitate dispute resolution between PKI participants when conflicts arise as a result of the use of certificates issued under this TSP CP.

9.14 Governing Law

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

9.15 Compliance with Applicable Law

This CP and provision of TSP CA 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

TSPs complying to the provisions of this TSP CP may not assign their rights, duties or obligations without the prior written consent of the ECAC PMA.

9.16.3 Severability

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

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

simultaneously. An appropriate change in practice, modification to this CP 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

TSPs shall not be liable for any failure or delay in their performance under the provisions of this TSP CP 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: ----------