2026

وحدة الاستجابة للحوادث السيبرانية للقطاع المالي والمصرفي

Jo-FinCERT

Trust Services for Domestic Financial Transactions - PKI Services

Certificate Policy/ Certification Practices Statement (CP/CPS)

Production Environment – V1.0

Central Bank of Jordan- The Unit of Financial Computer Emergency Response Team

Approval

Issue Date	Version Number	Approval
February, 2026	1.0	

Change Record

Date	Version	Preparer	Reviewer	Change Description
February, 2026	1.0	Ayat AlDwiry Amena Hayajneh	Ayat Hannoun	Creation

Table of Contents

Table of Tables

1. Introduction

1.1 Overview

The Public Key Infrastructure (PKI) for the financial sector is intended to be used when providing authentication services and the validity of the digital signatures for electronic transactions generated with the certificates issued under the provisions of the electronic transactions law No. (15) of the year 2015 as stated in section 9.14.

The main use of the services of CBJ Certificate Service Provider (CSP) is to issue and manage the lifecycle of the digital certificates used in digital signing and authentication services for electronic financial transactions, for sectors subject to the control and supervision of the Central Bank of Jordan.

The purpose of this document is to define the Certificate Policy (CP) and Certification Practice Statement (CPS) adopted by **CBJ-PKI** for issuing certificates. It provides a structured framework that ensures the security, reliability, and legal compliance of digital certificate operations. The document covers all aspects of certificate lifecycle management, including generation, issuance, revocation, publication, and compliance with relevant regulatory and international standards.

In the present document, the acronym CBJ-PKI is used to designate all CAs and related entities operating under the Central Bank of Jordan, and therefore under the Central Bank of Jordan Root CA.

This document has been developed in accordance with the European Telecommunications Standards Institute (ETSI) standards EN 319 401, EN 319 411, and local regulatory requirements set forth by the Telecommunications Regulatory Commission (TRC) of Jordan.

This document is organized in the following sections:

1. **Introductions** – This section introduces the CBJ-PKI as a Certificate Service Provider (CSP).
2. **Publication and Repositories Responsibilities –** Describes the publication policies for the certificates affected by this document, and the publication of this document itself.
3. **Identification and Authentication –** Discloses the rules for subscriber naming and required authentication policies.
4. **Certificate Life-Cycle Operational Requirements –** This section describes the different phases in the Life Cycle of certificates and their requirements.
5. **Management, Operational and Physical Controls –** Describes the controls enforced in the CBJ-PKI to provide adequate trust levels in the certificates issued under the CBJ-PKI.

6. **Technical Security Controls –** Discloses the security controls adopted in the CBJ-PKI.

7. **Certificate and CRL Profiles –** Describes the technical details of the different certificate types issued under the CBJ-PKI.

8. **Compliance Audit and other Assessment –** Discloses the audit policies followed in the CBJ--PKI to ensure that the security and quality requirements are fulfilled by the participant.

9. **Other Business and Legal Matters –** This section exposes the commercial, legal and contractual aspects involved in the usage of certificates issued in the CBJ-PKI.

1.1.1 Certificate Policy

X.509 certificates will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party (RA) to decide whether a certificate is trusted for a particular purpose. Subscriber certificates issued by CBJ RSA Root CA will identify the applicable policy in the certificate policies extension by including applicable OID(s).

1.1.2 Relationship Between the CP and the CPS

This document combines the CP and CPS documents and is thus presented as a single document. It states what assurance can be placed in a certificate issued by CBJ RSA Root CA to participants in the CBJ-PKI for the financial sector. It also states how CBJ RSA Root CA meets the requirements for policies defined in this document.

This CP/CPS establishes the policies and practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by CBJ RSA Root CA, as governed by this document and related documents which describe CBJ-PKI requirements and use of certificates.

1.1.3 Scope

The purpose of this document is to disclose the policies and practices adopted by the CBJ RSA Root CA who will only issue certificate(s) to first-level Subordinate Policy CA further referred to as Subordinate Policy CA (Policy CAs). The only exceptions are certificate(s) for infrastructure purposes e.g. CRL signing, OCSP signing, or some other internal CA operational purpose(s).

1.1.4 Interaction with Other PKIs

The Certification Authority (CA) operates independently and does not establish trust relationships, cross-certifications, or interoperability agreements with external Public Key Infrastructures (PKIs). All certificates issued under this CPS are trusted solely within the context defined by this Policy and Practice Statement.

1.2 Document Name and Identification

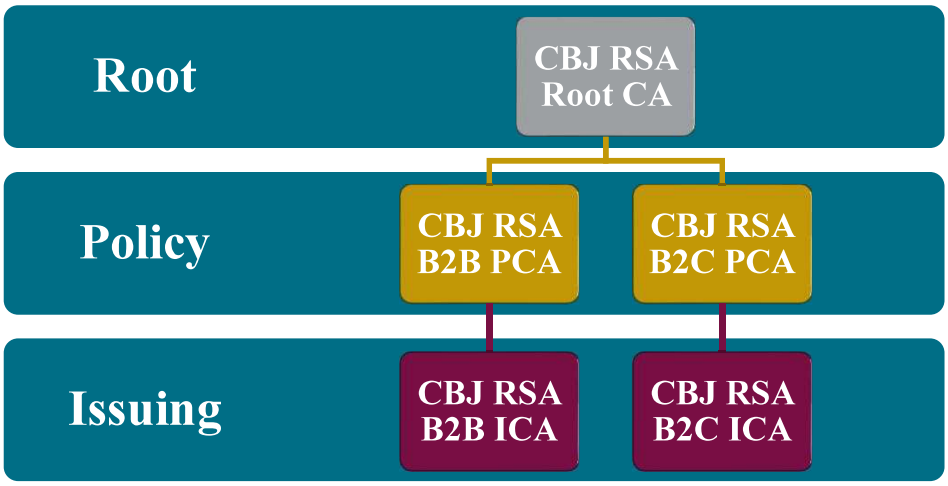

Figure 1: Certification Authorities

Name	CBJ Root CA Certificate Policy and Certification Practices Statement
Version	1.0
Status	Final
OID	1.3.6.1.4.1.56472.1.1.1.1.0
Issuance Date	Thursday, 5 February 2026
Location	This document will be published on the official Central Bank of Jordan website.

Table 1: Document Name and Identification

1.3 PKI Participants

1.3.1 Certification Authorities

The control of the Root CBJ-PKI is attributed to the Central Bank of Jordan (CBJ). The following is a graphical representation of the CBJ-PKI Certification Authorities hierarchy.

The Certification Authorities that compose the CBJ-PKI are the following:

1. **CBJ RSA Root CA:** This is the Top-level CA and the trust-anchor for the CBJ-PKI. This CA is offline and does not issue certificates to end entities or subscribers, but only to "Subordinate Policy CA" (described below). CBJ RSA Root CA Certificate contains its own Public Key and is self-signed. The certificate details of the "CBJ RSA Root CA Certificate" are included in the following table:

Distinguished Name	CN = CBJ RSA Root CA, O = Central Bank of Jordan, C = JO
SHA-1 Fingerprint	35 32 dd 59 5b 64 22 dd 60 ad ae f4 1b 21 00 07 2c 21 fb f6

Issued by	CBJ RSA Root CA
Issuance Date	September 21, 2022
Expiration Date	September 21, 2042
Location	This certificate, in the common standard formats, and can be found on the official Central Bank of Jordan website.

Table 2: CBJ RSA Root CA

2. **CBJ RSA Business-to-Business Policy CA:** expressed from now also as "CBJ RSA B2B PCA" is a subordinate Policy CA of the CBJ RSA Root CA. This CA is online and is responsible for issuing certificates to Issuing CAs dedicated to business purposes. This CA also issues certificates for OCSP responder's and TSA Servers, but it does not issue certificates to end entities or subscribers. The certificate details of the "CBJ RSA B2B PCA" is included in the following table:

Distinguished Name	CN = CBJ RSA B2B PCA 01, O = Central Bank of Jordan, C = JO
SHA-1 Fingerprint	21 11 9f a6 64 9c 8b 11 4f bc 52 e7 04 f4 de 55 29 9d 10 a2
Issued by	CBJ RSA Root CA
Issuance Date	October 3, 2022
Expiration Date	September 21, 2042
Location	This certificate, in the common standard formats, and can be found on the official Central Bank of Jordan website.

Table 3: CBJ RSA Business-to-Business Policy CA

3. **CBJ RSA Business-to-Consumer Policy CA:** expressed from now also as "CBJ RSA B2C PCA" is a subordinate Policy CA of the CBJ RSA Root CA. This CA is online and is responsible for issuing certificates to Issuing CAs dedicated to consumer purposes. This CA also issues certificates for OCSP, but it does not issue certificates to end entities or subscribers. The certificate details of the "CBJ RSA B2C PCA" is included in the following table:

Distinguished Name	CN = CBJ RSA B2C PCA 01, O = Central Bank of Jordan, C = JO
SHA-1 Fingerprint	Ea 0f dd a6 d0 c1 35 86 66 16 bc 78 e0 2a 5d a6 e2 2f 06 30
Issued by	CBJ RSA Root CA
Issuance Date	October 3, 2022
Expiration Date	September 21, 2042
Location	This certificate, in the common standard formats, and can be found on the official Central Bank of Jordan website.

Table 4: CBJ RSA Business to Consumer Policy CA

4. CBJ-PKI Issuing CAs issue subscriber certificates, depending on the characteristics of that entity (i.e. business or customer). These Issuing CAs will be permitted to issue a certain type (or types) of certificates, each conforming to a Certificate Policy/Certificate Practice Statement (CP/CPS).

1.3.2 Registration Authorities

Registration Authorities (RA) are the physical or legal persons responsible for the identification of the entities requesting a certificate (referred as "applicants" when the request is in process and "subscribers" for those in possession of a certificate). The CBJ RSA Root CA delegates to Registration Authorities the responsibility of verifying the information provided by the applicant within a certificate request, ensuring that the request and the process used to deliver the certificate to the subscriber meets the requirements of this CP/CPS. As well as the owner of an "Issuing CA" controls The Registration Authorities in the CBJ-PKI.

The responsibilities of RAs operating under the CBJ RSA Root CA are as follows:

1. Check the identity and circumstances needed to verify that the information in the certificate request is valid according to the type of certificate requested.

2. Inform the applicant, before the issuance of the certificate, about the terms and conditions related to the certificate and its usage.

3. Verify that the information contained in a certificate is accurate and complete according to this CP/CPS.

4. Ensure that the subscriber is in possession of the digital signature creation data (private keys) associated with the certificate to be issued.

1.3.3 Policy Approval Authority

The **FinCERT-PKI Operations Division** is responsible for the governance of the CBJ RSA Root CA. Its tasks include:

1. Establishing, implementing and publishing Certificate Policy/Certificate Practice Statement (CP/CPS) for CBJ RSA Root CA under CBJ-PKI. In addition, reviewing the policies, as well as updating them when necessary.

2. Review and approve the Subscriber Agreement and other related Agreements based on the CBJ RSA Root CA's specific business requirements.

3. Review the compliance of internal audits, external audits and any security assessments.

H.E the Governor of the Central Bank of Jordan is responsible for approving the policies and then officially signing them off. However, an **independent external auditor or relevant regulatory authority** ensures the adherence to applicable laws, regulations, and industry standards, and verifies compliance with these policies and standards.

1.3.4 Subscribers

In the CBJ-PKI, two different roles are defined. Depending on the status of the certificate request, these roles are named "**Applicant**" and "**Subscriber**".

An **applicant** is a physical person that requests a certificate for his own behalf or on behalf of a third party. The applicant needs to accredit his identity and ability to request a certificate. In the case of an applicant acting on behalf of a third party or legal person, they will be requested to accredit empowerment for such representation, as required by law.

A **subscriber** is a physical or legal person whose identity is linked to the digital signature creation data, or private key, and included in a digital certificate. In general, subscribers are individuals (end users), entities (organizations) or devices to whom certificates are issued and are considered the "owner" of a certificate. The subscriber of a certificate is responsible for the custody of his private key and not communicating this data in any way to any other person and legally bound by a Subscriber Agreement or Terms of use.

1.3.5 Relying Parties

All persons and entities that trust or rely on the certificates issued by certification authorities operating under the CBJ-PKI are considered to be "relying parties". These relying parties do not necessarily need to be a subscriber of a CBJ-PKI certificate. Relying parties are outside the scope of this CPS and are not controlled by the CBJ-PKI. See Relying Party Representations and Warranties in section 9.6.4.

1.3.6 Other Participants

The CBJ-PKI provides the following additional services to relying parties:

1. Directory and Publication Services.
2. Certificate Validation Services.
3. Certificate Revocation Services.

1.4 Certificate Usage

In the CBJ-PKI, the limitations for certificate usage are established by the Certificate Policy corresponding to each certificate type.

1.4.1 Appropriate Certificate Uses

Certificates under this CP/CPS are issued to be used for the following applications:

1. Validation of the signature of the CA in subject certificates used in digital signing and authentication services for electronic financial transactions, for sectors subject to the control and supervision of the Central Bank of Jordan.
2. Validation of the signature in the CRLs issued by the CA.

1.4.2 Prohibited Certificate Uses

Any use falling outside the section 1.4.1 described in this CP/CPS shall be deemed to be a prohibited use.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The Central Bank of Jordan/ FinCERT is responsible for the maintenance of this CP/CPS.

1.5.2 Contact Information

Any communication related to this CP/CPS and its related documents can be addressed to:

Name	Jo-Fin PKI Division
Email address	FinCERT.PKI@cbj.gov.jo
Address	Amman, Jordan
Telephone number	+962 6 4630301 Ext: 2766,1764, 4922

Table 5: Contact Information

1.5.3 Person Determining CPS Suitability for the Policy

TRC is the entity that determines the compliance and suitability of this CP/CPS and any supported documents.

1.5.4 CP/CPS Approval Procedures

The Central Bank of Jordan/ FinCERT defines and executes the procedures related to the approval of the CP/CPS and its subsequent amendments.

Amendments will produce a new version of the document that will be published in the CBJ-PKI Repository (specified in section 2.1 of this document).

1.6 Definitions and Acronyms

1.6.1 Definitions

This document makes use of the following defined terms:

Definitions		Description
Activation Data	:	Private data, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually held key share).
Applicant	:	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
CBJ-PKI	:	All CAs and related entities operating under the Central Bank of Jordan, and therefore under the Central Bank of Jordan Root CA.
Certificate Policy (CP)	:	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate the applicability of a type of certificate to the authentication of parties engaging in business-to-business transactions for the trading of goods or services within a given price range.
Certificate Revocation List (CRL)	:	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certification Path	:	An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Practice Statement (CPS)	:	A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.
End-Entity	:	Subscribers
Entity	:	Sectors subject to the control and supervision of the Central Bank of Jordan
Key	:	A parameter that determines the transformation from plaintext to ciphertext and vice versa.
Key Materials	:	A cryptographic key and other parameters (e.g., Initialization Vectors or domain parameters) used with a cryptographic algorithm.
Key Pair	:	Two mathematically-related keys having the properties that (1) one key can be used to encrypt a message that can only be

		decrypted using the other key, and (2) even knowing one key, it is computationally infeasible to discover the other key.
Object Identifier (OID)	:	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the CBJ-PKI OIDs are used to uniquely identify certificate policies and cryptographic algorithms.
Participant	:	An individual or organization that plays a role within a given PKI as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.
Private Key	:	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	:	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	:	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	:	An Subscriber entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by
Relying Party	:	A recipient of a certificate who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them
Root CA	:	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Subscriber	:	A subject of a certificate who is issued a certificate that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed

		in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device
Subscriber Agreement	:	An agreement between a CA and a subscriber that establishes the right and responsibilities of the parties regarding the issuance and management of certificates.
Time Stamp Authority	:	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.

[NEEDED VALID DEFINITIONS FOR DIGITAL SIGNATURES OR CERTIFICATES ACCORDING TO JORDANIAN LAW]

Table 6: Definitions

1.6.2 Acronyms

Abbreviation	Description
AIA	Authority Information Access
CA	Certification Authority
CBJ	Central Bank of Jordan
CBJ-PKI	Central Bank of Jordan- Public Key Infrastructure
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certificate Service Provider
DN	Distinguished Name
FI	Financial Institution
FinCERT	The Unit of Financial Computer Emergency Response Team
FIPS	United State Federal Information Processing Standards
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
KYC	Know Your Customer
NTP	Network Time Protocol

OCSP	Online Certificate Status Protocol
OID	Object Identifier
PCA	Policy Certification Authority
PIN	Personal identification number
PKCS	Public-Key Cryptography Standard
PKCS#10	Public Key Certificate Standard Certificate Request
PKI	Public Key Infrastructure
POC	Point of Contact
RA	Registration Authority
RFC	Request for comment
RSA	Rivest-Shamir-Adelman (encryption algorithm)
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
TRC	Telecommunications Regulatory Commission
TSA	Time Stamp Authority

Table 7: Acronyms

1.7 Statement on Compliance with CA/Browser Forum

The FinCERT, as operator of the CBJ-PKI ensures compliance with industry's best practices and security controls. In particular, FinCERT ensures compliance with the industry regulations published by ETSI Standards and TRC regulations.

2. Publication and Repository Responsibilities

This component contains the provisions regarding the publication of policies, certificates and other public information needed for the participants to interoperate with the CBJ-PKI.

2.1 Repositories

The shared repositories containing public information in the CBJ-PKI are owned by Central Bank of Jordan and are available 24 hours a day, seven days a week. In the case of interruption by cause of "force majeure", the service will be re-established in the minimum possible time.

The main repositories of the CBJ-PKI are:

1. **Policies Repository**: This repository available at the official Central Bank of Jordan website.
2. **Certificate and CRL Repositories:** services available at the URL http://csp.pki.cbj.gov.jo/cdpaia/
3. **OCSP Repository:** services available at the URL http://ocsp.csp.pki.cbj.gov.jo/ocsp/

2.2 Publication of Certificate Information

FinCERT is responsible for publication of information regarding practices, certificates, current CRLs, and the status of certificates. Issued certificates are published in the CBJ-PKI internal repository, which is accessible to authorized personnel in accordance with FinCERT policies and procedures.

All communications related to certificate life cycle in CBJ-PKI must be authenticated and protected against unauthorized modification. Communication may occur through official email address, secure file transfer protocol ls (e.g., SFTP), or other approved secure channels.

CAs shall provide relying parties with information on how to find the appropriate repository to check certificate status and OCSP within each issued certificate.

2.3 Time or Frequency of publication

This CP/CPS document will be published every time it is modified.

A certificate issued by any CA under the CBJ-PKI will be published immediately after its issuance.

In the case of revocation of a certificate, the appropriate CA will include this revocation information in the Certificate Revocation Lists (CRL) according to section 4.9.7 CRL Issuance Frequency.

2.4 Access Control on Repositories

The access for reading information in the CBJ-PKI repositories is free and unlimited.

Only FinCERT is authorized to modify the information contained in its repositories. FinCERT implements adequate controls to restrict the ability of modifying these repositories to authorized entities only.

3. Identification and Authentication

Certificates issued under the CBJ-PKI follow a set of required minimum controls that ensure the authenticity of the data included in certificates. These controls are enforced during the full lifecycle of certificates, certificate requests, and related documents.

Before issuing a certificate, FinCERT verifies the information, purpose and/or attributes of an applicant to be published in a Subordinate Policy CA certificate. This section of the CP/CPS establishes the criteria for an acceptable application for a Subordinate Policy CA Certificate.

This document reflects the common policies and controls for Identification and Authentication.

3.1 Naming

This section describes the elements regarding naming and identifying the subscribers of CBJ RSA Root CA Certificate.

3.1.1 Types of Names

All subscribers are assigned a non-null subject Distinguished Name (DN) according to the X.501 Standard. This DN is composed of a Common Name (CN), which includes a unique identification of the subscriber as described in section 3.1.5, and a structure of X.501 components as defined in section 3.1.4.

CBJ-PKI only generate and sign certificates that contain a non-null subject Distinguished Name (DN).

3.1.2 Need for Names to be Meaningful

All Distinguished Names must be meaningful, and the identification of the subscriber should be in a human readable form. This name is reviewed and confirmed by CBJ-PKI as part of the formal authorization process (Certificate Request Form or equivalent).

3.1.3 Anonymity of Subscribers and Pseudonyms

CBJ-PKI does not support anonyms and pseudonyms in Distinguished Names.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in certificates are interpreted using the (X.501) Distinguished Name (DN) standard.

Unless specified otherwise in the corresponding Certificate Policy, the common naming rule is:

Common Name (CN)	[unique identifier for the subscriber]- FinCERT may identify naming convention
Organization Unit (OU)	(optional) Organizational group of subscribers
Organization (O)	"Central Bank of Jordan" or the name of the commercial issuing CA owner
Country (C)	"JO" (for the Hashemite Kingdom of Jordan)

Table 8: Common naming of Certificate Policy

3.1.5 Uniqueness of Names

The Distinguished Names in the CBJ-PKI must be unique and never lead to ambiguity. In order to achieve this, the "Subject Name" in the certificate is formed using a format that includes one or more unique identifier (e.g. National ID, Account name…). Subject name uniqueness means that the CBJ RSA Root CA will not issue certificates with identical names to different entities.

3.1.6 Recognition, Authentication, and Role of Trademarks

The inclusion of a name in a certificate does not imply any right over that name, neither for the CBJ-PKI nor the applicant, nor the subscriber. The CBJ-PKI reserves the right to refuse a certificate request, or revoke an existing one, if a conflict is detected over ownership of a name.

In any event, the CBJ-PKI will not attempt to mediate nor resolve conflicts regarding ownership of names or trademarks.

3.2 Initial Identity Validation

"Initial Identity Validation" is the process of verifying the identity of an applicant and the authenticity of a certificate request. The registration process for entities under CBJ-PKI begins when a participant designate primary and secondary points of personnel contact officers to handle integration between CBJ and sectors subject to its control and supervision.

Only requests sent by participants designated primary or secondary points of contact, responsible for handling integration between CBJ and the sectors subject to its control and supervision (as indicated above), will be considered.

CBJ-PKI reviews the request to verify the identity and authorization of the applicant's points of contact (POCs).

Accepted requests are followed by formal documentation of responsibilities and validation (e.g., Subscriber Agreement). Once approved, CBJ-PKI proceeds with issuing the required certificate to the entity as part of the formal authorization process (Certificate Request Form or equivalent).

Sectors subject to Central Bank of Jordan control and supervision that acting as Registration Authority responsible for capturing, evidence retention and maintaining identity verification details for their customers (subjects/subscribers) through KYC.

3.2.1 Method to Prove Possession of Private Key

The Certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the certificate. The method to prove possession of a private key shall be PKCS #10 or another cryptographically equivalent demonstration. CBJ-PKI does not provide hardware tokens to CAs.

3.2.2 Authentication of Organization Identity

Participant shall designate primary and secondary points of personnel contact officers to handle integration between CBJ and sectors subject to its control and supervision who may act on behalf of the applicant during the certificate issuance process. The list of primary and secondary contacts ((Email and Phone Number) must be provided the central Bank of Jordan with it at the following email address (FinCERT.PKI@cbj.gov.jo).

CBJ-PKI issues certificates to entities upon receipt of an official Subscriber Agreement signed by the relevant authority that reflects the respective responsibilities of Participants as a Registration Authority (RA).

Each Participants need to have two types of certificates that are issued and delivered out-of-band (i.e., through agreed-upon delivery channels) as a prerequisite:

1. **Enrollment Agent (EA) Certificate:** which is used to sign all Participants clients' CSRs before submitting them down the pipe to Internal API service. To issue an EA certificate, Participants need to create an EA CSR and send it to CBJ-PKI Admins via email channel.

2. **Service Authentication Certificate (API Client):** which is used to authenticate Participants services that consume Internal API. To issue this certificate, Participants needs to create a certificate-signing request (CSR) signed by EA Certificate that the CBJ-PKI admin provided to that Participants and send it to CBJ-PKI Admins via email channel.

By this process, Participants act as a Registration Authority (RA) for their clients and hence client account management is the sole responsibility of the Participant itself and for capturing, evidence retention and maintaining identity verification details for their customers (subjects/subscribers) through KYC.

The Central Bank of Jordan must be notified of any changes to the list of authorized representatives through official channels.

3.2.3 Authentication of Individual Identity

CBJ RSA Root CA Certificate does not issue any end-entity certificates.

3.2.4 Non-Verified Subscriber Information

All information in a subscriber certificate is verified through matches all information in certificates issued information in the PKCS#10.

3.2.5 Validation of Authority

The CBJ-PKI validates individuals who are authorized to represent the Entity while authenticating the identity of the organization as detailed in Section 3.2.2.

3.2.6 Criteria for Interoperation

A Certification Authority that wishes to interoperate with the CBJ-PKI as Registration Authority is required to follow section 3.2.2.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-Key

CBJ-PKI does not renew/re-key a certificate in the traditional sense by reissuing a certificate with the same serial number or metadata. Each certificate renewal/re-keying results in the issuance of a new certificate with a unique serial number and Thumbprint. And the initial registration process is repeated as detailed in Section 3.2.

3.3.2 Identification and Authentication for Re-Key After Revocation

CBJ RSA Root CA Certificate shall not renew or re-issue Certificates that have been permanently revoked. The subscriber must apply for a new digital certificate by using the procedures for its issuance as in Section 3.2.

3.4 Identification and Authentication for Revocation Requests

The Identification Policy for revocation requests is the same as stipulated for initial registration.in Section 3.2.2.

The CBJ-PKI Certification and/or Registration Authorities can request the revocation of a certificate if there is knowledge or justified suspicion that the associated Private Key has been compromised, or reason to believe any other fact that recommends this action.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

The procedures an entity should use to apply for one or more Entity CA certificates were developed and approved by the CBJ-PKI. These procedures as follows:

1. Participant shall designate primary and secondary points of personnel contact officers to handle integration between CBJ and sectors subject to its control and supervision who may act on behalf of the applicant during the certificate issuance process.

2. The list of primary and secondary contacts ((Email and Phone Number) must be provided the central Bank of Jordan with it at the following email address (FinCERT.PKI@cbj.gov.jo).

3. CBJ-PKI reviews the request to verify the identity and authorization of the applicant's points of contact (POCs).

4. Accepted requests are followed by formal documentation of responsibilities and validation (e.g., Subscriber Agreement).

5. Once approved, CBJ-PKI proceeds with issuing the required certificate to the entity as part of the formal authorization process (Certificate Request Form or equivalent).

6. Each Participants have two types of certificates that are issued and delivered (Enrollment Agent (EA) Certificate and Service Authentication Certificate (API Client)) as detailed in Section 3.2.2.

4.1.1 Who can submit a certificate application

An authorized representative from an entity submits the certificate application to the Central Bank of Jordan, which operates the CBJ-PKI.

4.1.2 Enrolment process and responsibilities

Entities regulated by the CBJ and applying for certification under CBJ-PKI are responsible for submitting accurate and complete certificate application information, in accordance with applicable CBJ policies and procedures and the Subscriber Agreement.

All communications related to certificate enrolment and issuance between CBJ-PKI and the applying entity must be authenticated and protected against unauthorized modification. Communication may occur through official email address, secure file transfer protocols (e.g., SFTP), or other approved secure channels.

If passwords or shared secrets are used to secure communication, they must be exchanged in person or via other secure out-of-band mechanisms.

The contact information provided previously (primary and secondary points of personnel contact officers) would be used to verify the identity of the entity has authorized representative.

4.2 Certificate Application Processing

When a regulated entity under the supervision of the CBJ requests to apply for one or more Entity CA certificates, the CBJ-PKI initiates the enrollment process by CBJ-PKI procedures. These procedures as follows:

1. Entity shall designate primary and secondary points of personnel contact officers to handle integration between CBJ and sectors subject to its control and supervision which will be then an official authorized to act on behalf of the entity.

2. The list of primary and secondary contacts (Email and Phone Number) must be provided the central Bank of Jordan with it at the following email address (FinCERT.PKI@cbj.gov.jo).

3. The CBJ-PKI is responsible for validating the submitted information and verify the identity and authorization of the applicant's points of contact (POCs).

4. Formal documentation of responsibilities and validation (e.g., Subscriber Agreement) sign by regulated entity.

5. After designate primary and secondary points of personnel contact officers and signed Subscriber Agreement, issuing certificate procedure begun.

6. CSR send by email to (FinCERT.PKI@cbj.gov.jo) from primary and secondary points of personnel contact officers or by secure upload to the CBJ-PKI portal (if available).

7. The CBJ-PKI is responsible for validating the submitted information before proceeding with certificate issuance as part of the formal authorization process (Certificate Request Form or equivalent). This validation includes:

    a. **Authorized Contact Officers**; Certificate request received from designate primary and secondary points of personnel contact officers.

    b. The requester **signed the Subscriber Agreement** (for API Client Certificate Request Only).

    c. **Certificate Attributes;** Common Name (CN) Adhering to Naming convention.

    d. Request Signed by EA Certificate (CMC or PKCS#10) to ensure proof of possession of the private key.

    e. Request received to the specified email address (FinCERT.PKI@cbj.gov.jo).

    f. The subject of the email followed the format of Naming convention

    g. Email attachments encrypted.

h. Password for the attachment was sent through a different channel.

i. Confirming that the certificate request parameters (e.g., Template Name/Type of Certificate, Request Type, and other Certificate Attributes) are in line with the applicable certificate profile and CBJ-PKI policy.

j. Performing any additional technical or procedural checks required for the certificate type requested.

8. Once verification process complete successfully; the request is approved, CBJ-PKI proceeds with issuing the required certificate to the entity. The certificate is generated in the appropriate format (e.g., .cer format) and delivered securely to the authorized Point of Contact.

9. Each Participants have two types of certificates that are issued and delivered (Enrollment Agent (EA) Certificate and Service Authentication Certificate (API Client)) as detailed in Section 3.2.2.

10. All validations, decisions, and issued certificates are logged in accordance with CBJ-PKI's audit and accountability requirements.

4.2.1 Performing identification and authentication functions

The FinCERT is responsible for performing the identification and authentication of the applicant entity in accordance with the procedures defined by CBJ-PKI policies. This includes verifying the identity and authority of the entity has designated Points of Contact (POCs) as specified before in during the certificate application process.

FinCERT will only process requests sent to the specified email address (FinCERT.PKI@cbj.gov.jo) and from POCs explicitly listed before.

4.2.2 Approval or rejection of certificate applications

The FinCERT reserves the right to approve or reject any certificate application based on compliance with applicable policies, technical requirements, and verification procedures.

It is the responsibility of the requesting entity to ensure that the key pair used in the certificate request complies with the applicable certificate profile and cryptographic requirements defined by CBJ-PKI.

As CBJ-PKI only issues certificates to entities that are subject to its control and supervision, no additional validation required beyond the standard checks embedded in the enrolment and issuance process.

4.2.3 Time to process certificate applications

Upon successful identity verification and validation of all submitted information, CBJ-PKI will process and issue the certificate within 30 business days.

All issuance artifacts (e.g., signed certificates, public key details) are securely delivered to the authorized entity contact to ensure compliance with CBJ-PKI policies and to maintain trust in the issuance process. In accordance with CBJ-PKI's secure delivery procedures outlined in Section 4.1.2.

4.3 Certificate Issuance

A certificate request will only be forwarded to the CBJ-PKI Certification Authority (CA) for issuance after the Registration Authority (RA) has verified the accuracy and completeness of all information contained in the request.

CBJ-PKI is not responsible for monitoring, validating, or confirming the continued accuracy of the certificate information during the period between its issuance and renewal. It is the responsibility of the subscriber entity to promptly report any changes or inaccuracies that may affect the validity of the certificate.

4.3.1 CA Actions During Certificate Issuance

A Certification Authority adhering to the CBJ-PKI proceeds with the issuance of a certificate only after executing the necessary measures to verify that the request received by a Registration Authority is genuine as mentioned in section 4.2.

CBJ-PKI does not generate or store the private keys of subscribers; key generation and protection are the responsibility of the requesting entity.

4.3.2 Notification to subscriber by the CA of issuance of certificate

When a subscriber agreement signed and received from an authorized representative of a regulated entity and after a certificate is issued, the CA notifies the Registration Authority of the issuance and availability of the certificate and the new certificate is published to the certificate repository.

The CBJ-PKI will notify the requesting entity once the certificate is issued and will deliver the certificate through a secure and authenticated method, such email address, secure file transfer protocols (e.g., SFTP), or other approved secure channels.

By email, the certificates will be sent as encrypted email attachments in CER format, using the complex password that will be shared to designated Points of Contact (POCs) in different channel.

4.4 Certificate Acceptance

Before issuing a certificate under CBJ-PKI, an agreement must be established between the regulated entity and the CBJ (Subscriber Agreement), outlining the respective responsibilities and obligations related to the use and management of CBJ-PKI -issued certificates. The regulated entity has entitled to use the certificate, issue valid electronic signatures and end entity certificate

Once a certificate has been issued and entered into the internal CBJ-PKI repository, the regulated entity's responsibilities outlined in the Subscriber agreement and this Certification Practice Statement (CPS) take effect.

4.4.1 Conduct constituting certificate acceptance

Certificate acceptance is understood after the subscriber or his representative signs the "Subscriber Agreement", which constitutes formal acceptance of those terms. This will be considered as implicit acceptance of the certificate and its associated obligations.

4.4.2 Publication of the certificate by the CA

As specified in Section 2.2, all certificates issued under CBJ-PKI are published in the CBJ-PKI internal repository, which is accessible to authorized personnel in accordance with FinCERT policies and procedures.

4.4.3 Notification of certificate issuance by the CA to other entities

As stated in section 4.3.2, the CA only notifies the Registration Authority from which it received the request of the issuance of a certificate. For personal certificates/end entity certificates, the Registration Authority is responsible for notifying the subscriber of the availability of his certificate, by sending him a copy or by specifying how the certificate can be obtained.

CBJ-PKI will also notify authorized CBJ personnel, particularly in cases where the certificate may affect trust relationships, access controls, or system integration paths, in accordance with the same procedures.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber private key and certificate usage

CBJ-PKI does not issue subscriber (end-entity) certificates directly. Authorized Registration Authority in accordance with the policies and procedures defined in this CPS issues all subscriber certificates (end-entity).

4.5.2 Relying party public key and certificate usage

Any party effectively using the public key for any valid purpose is understood to be aware of Relying Party Representations and Warranties in section 9.6.4

Relying Parties are strongly encouraged to check certificate status via CRL or OCSP prior to trusting CBJ-PKI certificates in any transaction or authentication context.

4.6 Certificate Renewal

4.6.1 Circumstance for certificate renewal

CBJ-PKI does not support certificate renewal in the traditional sense where the same public/private key pair and metadata (e.g., serial number) are reused with an updated validity period. Instead, any request for a certificate beyond its validity period is treated as a new certificate issuance, even if subject details remain unchanged.

Entities are responsible for generating new key pairs, and for submitting new certificate signing requests (CSRs) when applying for a new certificate following expiration or key rollover.

CBJ-PKI may also initiate reissuance of certificates in the event of internal policy changes, internal key rollover, or updates to certificate profiles. In such cases, CBJ-PKI will notify the entity of the required actions.

4.6.2 Who may request renewal

CBJ-PKI does not support certificate renewal in the traditional sense, by reissuing a certificate with the same serial number or metadata. Each certificate renewal results in the issuance of a new certificate with a unique serial number and Thumbprint.

4.6.3 Processing certificate renewal requests

All renewal requests are processed using the standard certificate issuance procedures outlined in Section 4.3.1. The newly issued certificate will include a new serial number and may contain updated extensions or metadata as defined by CBJ-PKI policies.

CBJ-PKI does not permit the reuse of existing key pairs for renewal. The requesting entity is solely responsible for generating and protecting a new private key for each certificate request.

4.6.4 Notification of new certificate issuance to subscriber

As stated in section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

As stated in section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

As stated in section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

As stated in section 4.4.3.

4.7 Certificate Re-key

4.7.1 Circumstance for certificate re-key

CBJ-PKI does not support certificate re-keying as a distinct process. Instead, when a key pair is replaced, a new certificate is issued following the standard issuance procedures, with a new serial number, key pair, and updated metadata where applicable.

In such cases, coordination with the regulated entity is required to ensure appropriate handling of the revocation or expiration of the old certificate and proper deployment of the new one.

4.7.2 Who may request certification of a new public key

CBJ-PKI does not support certificate re-keying as a distinct process. When a key pair is replaced, a new certificate is issued following the standard issuance procedures, with a new serial number, key pair, and updated metadata where applicable.

In the event of an internal key rollover or changes to CBJ-PKI's own trust infrastructure, new certificates may be issued to regulated entities following standard issuance procedures and CBJ-PKI will notify the entity of the required actions.

4.7.3 Processing certificate re-keying requests

All re-keying requests are processed using the standard certificate issuance procedures outlined in Section 4.3.1. The newly issued certificate will include a new serial number and may contain updated extensions or metadata as defined by CBJ-PKI policies.

4.7.4 Notification of new certificate issuance to subscriber

As stated in section 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As stated in section 4.4.1.

4.7.6 Publication of the re-keyed certificate by the CA to other entities

As stated in section 4.4.2.

4.7.7 Notification of certificate issuance by the CA entities

As stated in section 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstance for certificate modification

CBJ-PKI does not allow the modification of certificates during their validity period. If the information contained in a certificate ceases to be valid, or the circumstances of the subscriber change in such a manner that the conditions expressed in the CPS or the CP are not met, then the only accepted procedure is the revocation and reissuance of a new certificate.

4.8.2 Who may request certificate modification

CBJ-PKI does not allow the modification of certificates. If a regulated entity identifies the need to change certificate details, an authorized Point of Contact (POC) must formally submit a request for FinCERT through approved communication channels.

CBJ-PKI will not modify existing certificates. Instead, a new certificate will be issued, and the previous certificate may be revoked based on policy or at the request of the entity.

4.8.3 Processing certificate modification requests

Under CBJ-PKI, certificate updates such as correction of errors, subject information changes, or extension adjustments are handled exclusively through certificate reissuance. A regulated entity may request reissuance by submitting a new certificate-signing request (CSR).

Typical reasons for such requests may include minor naming adjustments or correction of data entry errors.

Revocation of the previous certificate is typically performed upon successful issuance of the new one, based on policy or at the request of the entity

4.8.4 Notification of new certificate issuance to subscriber

As stated in section 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

As stated in section 4.4.1.

4.8.6 Publication of the modified certificate by the CA

As stated in section 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

As stated in section 4.4.3.

4.9 Certificate Revocation and Suspension

All Certification Authorities operating under the CBJ-PKI ensure, by establishing the necessary means, that a certificate that compromises for any reason is prevented from being used by either revoking or suspending that certificate.

CBJ-PKI issues Certificate Revocation Lists (CRLs) covering all revoked and unexpired certificates. These CRLs are published in internal CBJ-PKI repositories and are accessible via the HTTP URI included in the crlDistributionPoint (CDP) extension of each certificate. In addition, CBJ-PKI provides an OCSP service to support real-time certificate status checking.

The CBJ-PKI notified of any revocation via methods included in Section 2.2 or following emergency revocation procedures in Section 5.7. In addition, revocation requests are authenticated using CBJ-PKI-approved procedures (Certificate Revocation Form or equivalent).

4.9.1 Circumstances for revocation

CBJ-PKI may revoke a certificate under any of the following circumstances:

1. The subscriber requests revocation of his/her certificate.
2. If there is a compromise or suspected of compromise of the private key (corresponding to the public key in the certificate) or related cryptographic component, or any other emergency event that may affect the security or integrity of the CBJ-PKI environment.
3. The private key of any CA in the certification path is suspected to have been compromised.
4. When the CA has received notice or otherwise becomes aware that a subscriber has been misused of certificate or has violated one or more of its material obligations under the subscriber agreement.
5. When a certificate has been made obsolete, certificate information becomes invalid or contains inaccurate information, or a material change in the information contained in the certificate. This can occur when a modified certificate has been requested or an error is discovered in a certificate resulting in the CBJ-PKI issuing a correct certificate and revoking the certificate with the error.
6. If the subscriber fails to comply with the applicable CBJ-PKI Certificate Policy (CP) or the approved Certification Practice Statement (CPS).
7. When the privileges or mapped policies in a certificate are removed or reduced.
8. The subscriber ceases operations for any reason.
9. The CA's right to issue certificates for a particular Certificate Policy expires or is revoked or terminated.

10. CBJ-directed revocation: If CBJ, acting as the root CA operator, mandates revocation in line with oversight responsibilities.

If it is determined a private key used to authorize the issuance of one or more certificates issued by the CBJ-PKI may have been compromised, all certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise shall be revoked or verified as appropriately issued.

4.9.2 Who can request revocation

A certificate issued by CBJ-PKI may be revoked under the following conditions:

1. Upon formal direction from the Executive Manager of CBJ/FinCERT.

2. Upon an authenticated revocation request submitted by a designated Point of Contact (POC) at the regulated entity through formal channels.

3. When CBJ-PKI personnel determine that an emergency has occurred that could affect the trust or security of the certificate (see Section 4.9.1).

Revocation requests are verified by using the contact information provided previously (primary and secondary points of personnel contact officers) would be used to verify the identity of the entity has authorized representative. Moreover, validating an email or signed PDF document accompanying the request (If Any).

If a certificate is requested to be reissued due to corrections or changes, the acceptance of the new certificate by the entity constitutes implied authorization for CBJ-PKI to revoke the prior version of the certificate. No additional approval is required for that revocation.

All communications related to certificate life cycle in CBJ-PKI must be authenticated and protected against unauthorized modification. Communication may occur through official email address, secure file transfer protocol ls (e.g., SFTP), or other approved secure channels.

For the sake of speed, contacting CBJ-PKI designated personnel directly in case of Requests related to suspected private key compromise, certificate misuse, fraud, or other integrity concerns. In addition, request must be submitted through formal channels.

4.9.3 Procedure for revocation/suspension request

The CBJ-PKI will review all revocation requests to ensure that the revocation requests are legitimate and will then revoke the certificate, as follows:

1. The request must come from an officially designated point of contact (POC) provided previously.

2. Requests should be sent via methods included in Section 2.2.2 with certificate Serial Number and Reason for Revocation as one of the following **with justifications:**

    a. Key Compromise.

b. CA Compromise.

c. Cessation of Operation

d. Affiliation Changed.

e. Suspended

f. Certificate Hold.

g. Unspecified

3. Upon receipt of a revocation request, the CBJ-PKI authenticates the request by making direct contact (call back or challenge/response telephone conversation) with the Entity POC.

4. CBJ-PKI notify relevant parties that the Certificate has been Revoked Successfully or Rejected with the reason of non-compliant via methods included in Section 2.2.2.

5. In emergencies (e.g., suspected compromise), CBJ-PKI may proceed with revocation immediately and notify relevant parties post-action.

Participants act as a Registration Authority (RA) for their clients and hence client certificate revocation management is the sole responsibility of the Participant itself and for revoke certificate for their clients and verify the request.

If it is determined a private key used to authorize the issuance of one or more certificates issued by the CBJ-PKI may have been compromised, all certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise shall be revoked or verified as appropriately issued.

Revocation Notification and Publication:

1. Revoked certificates will be listed in the CRL and OCSP repositories maintained by CBJ-PKI.

2. The CRL is published at http://csp.pki.cbj.gov.jo and is updated in accordance with the publishing schedule outlined in section 4.9.7

3. Once CBJ-PKI revoke the certificate, it will be automatically generates and adds a CRL entry for that certificate.

Revocation requests communicated by other means which do not unequivocally authenticate the request will produce a temporary suspension of the certificate, as defined in sections 4.9.13 to 4.9.16.

4.9.4 Revocation request grace period

CBJ-PKI does not apply a revocation request grace period. Revocation requests are processed as soon as they are authenticated and approved in accordance with CBJ-PKI procedures.

4.9.5 Time within which CA must process the revocation request

Revocation requests initiated by entities will be processed within a maximum of 24 hours of receiving an authenticated and approved revocation request (in accordance to ETSI standard 119 495).

4.9.6 Revocation checking requirement for relying parties

CBJ-PKI requires all relying parties to verify the revocation status of any certificate issued under the CBJ-PKI at the time of each electronic signature validation.

Either may fulfill this requirement:

1. Consulting the latest Certificate Revocation List (CRL) issued by CBJ-PKI.
2. Querying the CBJ-PKI Online Certificate Status Protocol (OCSP) service.

Information necessary to locate these revocation services (e.g., CRL Distribution Point and OCSP URL) is embedded in all certificates issued by CBJ-PKI.

4.9.7 CRL (certificate Revocation List) issuance frequency

To ensure timely and reliable certificate status information, CBJ-PKI operates its issuing Certification Authority (CA) online and publishes an updated Certificate Revocation List (CRL) as the stipulated frequencies are:

CA Name	CRL Publication Interval	CRL Overlap Period	Description
CBJ RSA Root CA	3 Months	1 Week	This CRL will contain the revoked, if any, certificates for CBJ-PKI Policy CAs.
CBJ RSA B2B PCA	3 Months	1 Week	This CRL will contain the revoked, if any, certificates for CBJ-PKI Issuing CAs
CBJ RSA B2C PCA	3 Months	1 Week	
CBJ RSA B2B ICA	3 Days	3 Days	This CRL will contain the revoked, if any, certificates for CBJ-PKI Subscribers.
CBJ RSA B2C ICA	3 Days	3 Days	

Table 9: CRL Issuance Frequency

In the event of emergency certificate revocation, the updated CRL posted within 24 hours of approval, in accordance with the procedures outlined in Section 4.9.3.

New CRL replaces the previously published version in the CBJ-PKI certificate repository.

4.9.8 Maximum latency for CRLs

The CBJ-PKI operates offline Root CA; CRLs are published the same day they are generated. All CRLs are transferred securely from the offline CA and published within 4 hours of generation. This process are authenticated using CBJ-PKI-approved procedures (CRL Update Form or equivalent).

Other CRLs are posted to the repository within a reasonable time after generation (Automated).

4.9.9 On-line revocation/status checking availability

CBJ-PKI provides a 24/7 Online Certificate Status Protocol (OCSP) service that complies with RFC 2560 standards. The URL for accessing the OCSP service is included in the Authority Information Access (AIA) extension of every subscriber certificate issued by CBJ-PKI.

OCSP response practices according to RFC 6960:

1. **"Verified":** The certificate is not revoked and is known to the responder.
2. **"Revoked":** The certificate has been revoked or hold.
3. **"Unsuccessful":** The certificate has been expired.
4. **"No URLs":** The responder does not know about the certificate (e.g., non-issued or unrecognized serial number, it was never issued).

4.9.10 On-line revocation checking requirements

CBJ-PKI provides unrestricted access to its online certificate revocation services (CRL and OCSP) to all participants and relying parties within the trust framework (Participants in the PKI only).

Relying parties are expected to validate the revocation status of any certificate they rely on by checking current CRL or OCSP responses before trusting the certificate in any transaction.

4.9.11 Other forms of revocation advertisements available

CBJ-PKI Certificate Policies may, where appropriate, specify alternative methods for publishing or referencing revocation information—such as customized CRL Distribution Points (CDPs) or additional status access mechanisms.

This provision is included to support future flexibility in certificate and revocation service design.

4.9.12 Special requirements regarding key compromise

Any party that becomes aware of a suspected or confirmed key compromise within the CBJ-PKI is required to immediately report the incident to the appropriate Registration Authority (RA) or CBJ-PKI Certification Authority (CA).

In particular, subscribers must report any compromise or certificate-related issue directly to the Registration Authority that issued their certificate, using official communication channels as defined in CBJ-PKI procedures and in accordance with procedures described in Section 4.9.3.

If one of the CBJ-PKI Infrastructure CA keys is compromised, FinCERT will notify the authorized officials of Entity CAs. The compromised certificate will be added to the CRL and a CRL either with no nextUpdateTime or a nextUpdateTime of the expiration time of the certificate will be posted. Additionally, all Registration Authority with agreements to distribute the root certificate in their commercial trust stores will be notified.

A replacement CA certificate and key pair will be generated and all subordinate CAs of the compromised CBJ-PKI Infrastructure CA will be issued new certificates. The new certificate will be securely distributed to all Entity CAs.

4.9.13 Circumstances for suspension

If a revocation request does not meet the requirements for immediate revocation as outlined in Section 4.9.3, CBJ-PKI may suspend the targeted certificate as a precautionary measure until further verification is completed.

The subscriber may suspend a certificate upon request; such requests must be submitted through official channels in accordance with CBJ-PKI procedures with sufficient justification for initiating the suspension process

4.9.14 Who can request suspension

As stated in section 4.9.2.

4.9.15 Procedure for suspension request

As stated in section 4.9.3. The procedure allows subscribers to request certificate suspension

4.9.16 Limits on suspension period

There is no limits on suspension period. Suspended certificates will be permanently revoked under any of the following circumstances:

1. The subscriber or the designated Point of Contact (POC) at the regulated entity request revocation while the certificate is suspend in accordance to CBJ-PKI procedures.

2. A security incident or policy violation is identified during the suspension review, requiring revocation based on CBJ-PKI policy.

3. Revocation is explicitly directed by CBJ-PKI based on operational, legal, or regulatory grounds.

Once a certificate is revoked following suspension, it is included in the Certificate Revocation List (CRL) and cannot be reinstated.

4.9.17 Circumstances for terminating suspended certificates

The subscriber may terminating suspend a certificate upon request; such requests must be submitted through official channels in accordance with CBJ-PKI procedures with sufficient justification for initiating the terminating suspension process.

4.9.18 Procedure for terminating the suspension of a certificate

Reactivation of a suspended certificate may only be performed by the CBJ-PKI Registration Authority (RA) or Certification Authority (CA) and in accordance with procedures described in Section 4.2. This process are authenticated using CBJ-PKI-approved procedures (Un-Hold Certificate Request Form or equivalent).

4.10 Certificate Status Services

CBJ-PKI provides a highly available and reliable service for checking the status of all certificates issued.

4.10.1 Operational characteristics

Certificate status services are accessible through HTTP servers owned by CBJ-PKI certification authorities. The services can be accesses by downloading CRLs or by sending requests to OCSP servers.

The appropriate certificate revocation information service URLs are included in standard extensions within the issued certificates.

4.10.2 Service availability

The Certificate Status Services are available in a 24x7 basis.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

“End of Subscription” refers to the conclusion of a certificate’s validity due to expiration or revocation. This status applies only to the specific certificate in question and does not affect any other valid certificates or active subscriptions that the end entity may hold within the CBJ-PKI.

CBJ-PKI notifies the designated Point of Contact (POC) at the regulated entity 60 days prior to the expiration of any issued certificate and again 15 days before expiration.

If the authorized entity representative does not initiate a renewal or reissuance process before the certificate expires, the certificate is allowed to expire naturally, and the PKI relationship for that certificate is considered closed.

4.12 Key Escrow and Recovery

4.12.1 Key escrow and recovery policy and practices

CBJ-PKI does not perform any encryption key recovery functions for any certificates it issues nor does it store or manage any data encrypted using CBJ-PKI private keys that would necessitate key escrow or recovery capabilities. Therefore, key escrow and recovery is not used by the CBJ-PKI.

CBJ-PKI does not escrow digital signature keys under any circumstances.

4.12.2 Session key encapsulation and recovery policy and practices

CBJ-PKI does not perform any session key encapsulation recovery functions; no subscriber key management keys are issued or used within the CBJ-PKI.

5. Facility, Management, and Operational Controls

The CBJ-PKI asserts the importance of these controls as a fundamental basis to provide trust to subscribers and all relying parties. These controls are under surveillance and audited both internally and externally by accredited bodies.

Registration Authorities are appointed by FinCERT the Issuing CA for which the RA is related. Registration Authorities are not allowed to delegate their operations to other parties.

5.1 Physical Controls

This section describes the physical controls on the facility housing the CBJ-PKI components.

5.1.1 Site Location and Construction

The CBJ-PKI information systems are hosted in secure datacenters that ensure high levels of physical and environmental security. These datacenters operate under continuous surveillance (24/7) and are designed to mitigate critical physical risks, including unauthorized access, fire, power failure, and other environmental threats.

At all times, all personnel gaining access to the facility must pass through the building's security checkpoint using a CBJ-issued badge.

Visitors and individuals without pre-approved access must be escorted at all times and are required to sign in using an official visitor log. These facilities meet physical security standards appropriate for safeguarding high-value cryptographic infrastructure and sensitive PKI assets.

5.1.2 Physical Access

The CBJ-PKI datacenters implement diverse nested security perimeters. The access from an outer to an inner perimeter requires different security and authorization controls. Among these controls: door access and video surveillance.

5.1.3 Power and Air Conditioning

The CBJ-PKI facilities are equipped with uninterruptible power supply (UPS) systems capable of sustaining operations during power outages and protecting critical PKI components from electrical fluctuations. Redundant air conditioning systems are also in place to maintain stable temperature and humidity levels within the secure datacenter, ensuring continued performance and equipment protection.

5.1.4 Water Exposures

The facilities are located in a place where natural flooding risks are controlled and they are equipped with flooding sensors and alarms.

5.1.5 Fire Prevention and Protection

The facilities implement automated fire prevention and protection controls that is suitable for datacenters.

5.1.6 Media Storage

Sensitive information media within CBJ-PKI are securely stored in fireproof containers and high-security safes, selected based on the media type and the classification level of the information. These storage units are placed in redundant, physically separate locations to mitigate risks such as fire or water damage. Access is strictly limited to authorized personnel and governed by formal security procedures.

5.1.7 Waste Disposal

The disposal of optical or magnetic media and paper containing any information generated during CBJ-PKI operations is executed following procedures established for such purposes, including demagnetization and/or destruction processes, depending on the media type to be disposed.

5.1.8 Off-site Backup

CBJ-PKI performs daily encrypted backups of all critical information required to promote the secondary data center to operational status in the event of a disaster affecting the primary data center.

These backup copies remain encrypted at all times and are securely stored in a facility that enforces dual access control for recovery, ensuring both integrity and availability of CBJ-PKI operations under contingency scenarios.

5.2 Procedural Controls

The information systems and services incorporated in the CBJ-PKI are operated in a secure manner, following a set of predefined procedures that are enforced by the CBJ and verified through periodical auditing activities.

For security reasons the information related to these controls are classified as “CONFIDENTIAL”. Further detailed information is only disclosed to accredited auditors who are responsible for reviewing CBJ-PKI components and operations.

5.2.1 Trusted Roles

The CBJ-PKI establishes and enforces a strict security policy to control all operations performed at any level of the CBJ-PKI infrastructure. This includes the identification and control of the Persons performing those operations. These Persons are considered “Trusted Roles” and include, but are not limited to:

1. The **Administrator** role does not issue certificates for RAs and is responsible for:

a. Establishing installation, configuration, and maintenance of the OS.

b. Restarting OS and services in case of system failures.

c. Managing and publishing (APIs) through the closed network of banks.

2. The **Operator** role is responsible for:

a. Registering new Subscribers (i.e. Entity).

b. Verifying the accuracy of information included in certificates.

c. Requesting the issuance of certificates.

d. Requesting the revocation of certificates.

e. Registering certificate types that are based on certificate templates that are published on CAs

f. Carrying out the technical execution of the CRL generation process within the offline Root CA environment. Under the supervision of PKI Custodians.

3. The **Officer** role acts as a final approver, and is responsible for:

a. Executing the issuance of certificates for new subscribers.

b. Executing the revocation of certificates.

c. Generating CBJ-PKI Infrastructure CA keys.

d. Ensuring all operations comply with CBJ-PKI policies and that all requests have been properly validated by the Operator prior to execution.

4. The **Auditor** role is responsible for:

a. Performing or overseeing internal/ external compliance audits to ensure that the CBJ-PKI Infrastructure CAs are operating in accordance with this CPS and local regulatory requirements set forth by the Telecommunications Regulatory Commission (TRC) of Jordan.

b. The internal auditing shall be conducted in accordance with the approved audit plan, in addition to any tasks assigned to the Internal Audit Department, and in line with the provisions stipulated in the Internal Audit Charter.

5. **Security Officers/ Managers** role are neither key owners nor handle of key materials, they are responsible of:

a. Oversee compliance with approved policies, practices, and procedures related to key material management to ensure security policies, practices and procedures are followed.

b. Oversee physical security controls for the bank, data center, officer and server rooms where PKI services and other application, system or network components are deployed.

6. **PKI Custodians** role are not key owners but retaining a part of the key or the HSM/Smart Card media required for the operation of the CA:

   a. Participating in Offline Root CA CRL generation, key generation ceremonies and securely storing cryptographic key components.

   b. Participating in handling the activation, deactivation, and secure destruction of key materials in accordance with approved procedures.

7. Number of Persons Required per Task

The CBJ-PKI establishes the need for the segregation of duties based on job responsibility to ensure that the adequate number of Trusted Persons is required to perform sensitive tasks.

To ensure the integrity and security of CBJ-PKI, individuals may only assume one of the following roles: Officer, Operator, Administrator, or Auditor.

In CBJ-PKI, Dual- control is enforced for all sensitive CA operations (e.g. certificate issuance and revocation) to ensure that no single individual can perform critical CA functions alone. It must involve at least two trusted roles:

1. An **Operator**, who prepares and initiates the action.

2. An **Officer**, who acts as the final approver and executes the action.

The roles requiring separation of duties is stipulated in section 5.2.4.

5.2.2 Identification and Authentication for Each Role

All the persons assuming a role in the CBJ-PKI systems follow an authorization process, which entitles them to access the appropriate information and systems for their role. The authentication is achieved by using a unique credential assigned to a single individual, digital certificates and multi-factor authentication before being permitted to perform any actions.

5.2.3 Separation of Roles

Roles requiring Separation of duties include at least the following:

1. Validation of information in Certificate Applications.

2. Acceptance, rejection, or other processing of Certificate Applications, revocation requests, Registration Authority or enrolment information.

3. Issuance or revocation of Certificates.

4. The generation, issuing or destruction of a CA certificate.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

The CBJ is responsible and accountable for the operations of the CBJ-PKI infrastructure.

Personnel acting directly or indirectly for the CBJ-PKI will be required to possess the required qualification and/or proved experience in certification service provision environments. All involved personnel will be required to act according to the CBJ Information Security and Cyber Security Management Policies and to possess:

1. Knowledge and training (according to the role assigned to the person) in Public Key Infrastructures.
2. Knowledge and training (according to the role) in Information Systems Security.
3. Knowledge and training specific for the responsibilities assigned.

5.3.2 Background Check Procedures

As per Recruitment procedures in Human Resource Department within CBJ.

5.3.3 Training Requirements

Personnel directly involved in CBJ-PKI will follow an internal training plan that is adapted to their assigned attributions. They are also trained on the operations of the system.

5.3.4 Re-training Frequency Requirements

Retraining sessions are required for all involved personnel in the case of environmental, technology and/or operative changes, Changes in practices and/or policies.

Personnel are informed and made aware of changes. In addition; records are maintain of the training received by each person assigned.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

If an unauthorized action is detected the CBJ-PKI will undertake necessary disciplinary actions. Any action that (intentionally or unintentionally) contravenes the Certification Practice Statement or the Certificate Policies or other policies adopted in the CBJ-PKI will be considered unauthorized.

Upon detection of an unauthorized action, the CBJ-PKI will initiate an investigation process. During this process, the involved persons will be prevented from obtaining access to CBJ-PKI systems and information. Disciplinary actions will be taken after the investigation determines the severity and intent of the action.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the CBJ-PKI Infrastructure will have the necessary experience,

Contractors and subcontractors are contractually obligated to perform their duties in accordance with this CPS, Information Security policies of the CBJ and contract between them and CBJ.

Contractor shall be required to sign the Contractor agreement prior to being granted access to Information resources.

5.3.8 Documentation Supplied to Personnel

All personnel incorporated within the CBJ-PKI are provided access to at least the following documentation:

1. Certification Practices Statement/Certificate Policies.
2. Organization chart and assigned functions and responsibilities.
3. Operational procedures.
4. Any relevant statutes, policies or contracts.

When these documents are revised, CBJ-PKI personnel are notified of the changes and updated documents are provided.

5.3.9 Contract Termination and Assigned Role Change Procedures

In the event that a contract is terminated or the role assigned to a person is changed, CBJ-PKI ensures that the appropriate procedure is executed. This procedure includes at least the necessary changes in the privileges granted to access facilities, information systems and documentation. The change or termination will be notified to all involved parties.

5.4 Audit Logging Procedures

This section describes the event logging and audit systems that have been implemented to maintain a secure environment in the CBJ-PKI.

5.4.1 Types of Events Recorded

CBJ-PKI records in their servers all events related to:

1. Successful or unsuccessful logon and logoff of accounts.

2. Successful or unsuccessful account management.
3. Successful or unsuccessful server policy changes.
4. Successful or unsuccessful privilege use (including starting and stopping services).

5.4.2 Frequency of Issuing Logs

Logs are processed and audited in a regular basis. CBJ-PKI defines daily, weekly and monthly frequencies for log processing. The automatic logger creates alarms if anomalies are encountered.

5.4.3 Retention Period for Audit Logs

CBJ-PKI and involved parties retain all audit logs during a minimum period after the creation time according to the local regulatory requirements set forth by the Telecommunications Regulatory Commission (TRC) of Jordan.

5.4.4 Protection of Audit Logs

All audit records and archives are signed using an administrative CBJ-PKI certificate (AuditLogSigning).

5.4.5 Audit Log for Backup Procedures

The audit logs are backed up according to CBJ established backup policy.

5.4.6 Audit Collection System (Internal vs. External)

The automatic collection systems for audit logs in CBJ-PKI is executed by the appropriate operating systems, software applications, and personnel operating these systems. Where an external audit is required, the operator of the Issuing CA will be responsible of providing the requested information.

All audit logs are ingested into the Security Event and Incident Management (SEIM) tool.

5.4.7 Notification to Event-Causing Subject

No notice that an event was audited is provided to the individual, organization, device, or application that caused the event

5.4.8 Vulnerability Assessments

CBJ performs self-assessments of the security controls at the time of initial installation and configuration of the CBJ-PKI.

CBJ-PKI executes regular vulnerability assessment and intrusion tests. In depth assessments and checks are performed on a regular basis, including conformance to disaster recovery plans.

CBJ provides a report of the analysis of the results of both internal and external vulnerability assessments and mitigation procedures of those vulnerabilities.

5.5 Records Archival

This section includes the stipulations regarding record retention policies.

5.5.1 Types of Events Archived

The information and events archived are:

1. Audit logs stipulated in section 5.4.1 of this CPS.
2. Information generated during the life cycle of all CBJ-PKI certificates.
3. Contracts and agreements.

5.5.2 Retention Period for Archive

All information related to or affecting the CBJ-PKI certificates is kept during a 5-year period.

5.5.3 Protection of Archive

Access to archived materials is restricted to authorized persons, and controls to ensure the archive integrity are enforced.

5.5.4 Archive Backup Procedures

Daily backup copies are executed. The main copy is stored in a fireproof safe inside a secured zone.

The detailed procedure is confidential.

5.5.5 Requirements for Timestamping of Records

In addition to stipulations in 5.5.3, a time stamp is included in the electronically signed records.

5.5.6 Archive Collection System (Internal or External)

Archive collection is an internal task in the CBJ-PKI that cannot be outsourced to third parties. Procedures to obtain and verify archive information only authorized personnel obtain access to the physical media containing archives, backups and other recorded information.

5.5.7 Procedures to Obtain Archive Information

Archived content is only shared based on formal requests. Records related to a specific entity can be shared with that entity's authorized point of contact (POC) upon official request.

5.6 Key Changeover

Key changeover is considered as a Certificate Re-key, which is understood as the issuance of a new certificate to a Certification Authority, and therefore applies the stipulations set in section 4.7.

5.7 Compromise and Disaster Recovery

When the Continuity Plan is activated. It ensures restoration of critical services (see Section 5.7.4). Specific scenarios and responses are summarized internally; full details are documented in a confidential Continuity Plan.

5.7.1 Incident and compromise handling procedures

The Certification and/or Registration Authorities operating under the CBJ-PKI are required to enforce the necessary controls to ensure and demonstrate that the Incident and Compromise Handling Procedures are effective. Involved people must be conveniently trained in their roles and responsibilities in the execution of their duties.

The CBJ will be notified if any of the following is experienced by the CBJ-PKI infrastructure:

1. Suspected or detected compromise of CBJ-PKI Trust Infrastructure systems.
2. Physical or electronic penetration of CBJ-PKI Trust Infrastructure systems.
3. Successful denial of service attacks on a CBJ-PKI Trust Infrastructure component.
4. Any incident preventing the CBJ-PKI Trust Infrastructure from issuing a CRL.

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

If the hardware or software resources are altered or suspected to have been altered, the CBJ-PKI will stop normal operations until a secure environment is established. In parallel, an investigation will be conducted in order to identify the cause and stipulate the necessary actions to avoid future iterations.

In the event digital certificates are issued during the uncertainty period and a risk exists that these certificates could be compromised, then those certificates will be revoked, and subscribers will be notified of the need to reissue their certificates.

During restoration, CRLs must be updated to reflect revoked Entity CA certificates and reissued if needed

5.7.3 Entity Private Key Compromise Procedures

In case of a private key is compromised in CBJ-PKI architecture and in addition to stipulations in section 5.7.2, the subordinated entities depending on the compromised private key will be notified of this event and the necessary actions will be undertaken. All certificates

issued by entities subordinated to the compromised key from the time of the key's compromise and the certificate's revocation will be revoked, and the involved parties notified. Additional steps to re-issue the necessary certificates will be taken.

5.7.4 Business Continuity Capabilities after a Disaster and Force Majeure

The CBJ-PKI Infrastructure CA servers operate with back-up power, telecommunications, and appropriate infrastructure system redundancies to minimize outages. However, In the event of a disaster (independent of its nature) that affects CBJ-PKI's main facilities, and any services that are provided from these, the CBJ-PKI business Continuity plan will be activated, ensuring that the services identified as "Critical" are available in a secondary facility.

The rest of services would be available in the reasonable terms, as judged adequate for their importance and critically level. The "Force Majeure" clauses are defined in section 9.15.5.

5.8 CA or RA Termination

The causes that could imply the termination of the certificate of the Certification or Registration Authority operating under the CBJ-PKI are:

1. Private Key Compromise
2. A License expiration or cancellation
3. A Political Decision

In the case of certificate Termination for the Certification Authority under CBJ-PKI, the minimum actions to be executed by the terminated subject are:

1. Notify all certificate subscribers and revoke all certificates under the CA.
2. Inform all relying parties that have a registered direct relationship with that Certification Authority
3. Publish a public notice of its termination, and undertake other public communications as deemed necessary to inform the wider relying party community.
4. [OTHER ACTIONS listed in TRC regulations].

In the case of the certificate of CBJ-PKI Root CA is terminated; this will imply the termination of the entire defined by this CP/CPS.

6. Technical Security Controls

This section describes the security measures taken by Certification Authorities operating under the CBJ-PKI. The CBJ-PKI established the necessary means to ensure and demonstrate that these controls are enforced.

These controls are under surveillance and audited both internally and externally by accredited bodies. This CPS describes the controls affecting the Certification Authorities and other principal components in the CBJ-PKI.

6.1 Key Pair Generation and Installation

The CBJ-PKI Infrastructure CAs do not issue Extended Validation Certificate Policy (EVCP), Domain Validation Certificate Policy (DVCP), Individual Validation Certificate Policy (IVCP) and Lightweight Certificate Policy (LCP) and therefore do not generate key pairs for such certificates.

Key pairs generation for end entities and subscribers are there responsibility.

6.1.1 Entity Private Key Compromise Procedures

Key pairs for all internal components in the CBJ-PKI are generated in hardware security modules (HSM) accredited under the standards specified in section 6.2.1.

Private keys of CBJ-PKI Infrastructure CAs are generated using the CBJ-PKI Infrastructure CAs Key Signing Ceremony procedures.

6.1.2 Private Key Delivery to Subscriber

In the CBJ-PKI the generation of the private key by the Registration Authority or by the Subscriber. Therefore; The Entity generates its own key pair, and does not need private key delivery (The procedures undertaken are defined at the appropriate Integration Guide & Onboarding Procedures Document.)

Policy Certification Authorities and Issuing Certification Authorities will generate the private key in HSM devices in such a manner that it will be always under the control of the CA Responsible.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys generated by subscribers are submitted to CBJ-PKI Registration Authorities as part of a certificate request, using accepted formats (PKCS#10, PKCS#7, and CMC). Each request must be signed using the private key corresponding to the public key being certified. Identity checking and proof of possession of the private key is accomplished as described in Section 4.3.1. (The procedures undertaken are defined at the appropriate Integration Guide & Onboarding Procedures Document.)

6.1.4 CA Public Key Delivery to Relying Parties

The public keys of all Certification Authorities operating under the CBJ-PKI are published and can be freely downloaded from its repository which is located as mentioned in section 1.3.1.

6.1.5 Key Sizes

Key sizes for certificate type issued in the CBJ-PKI are detailed in the following table:

CA Name	Key Length
CBJ RSA Root CA	4096 bit
CBJ RSA B2B PCA	4096 bit
CBJ RSA B2C PCA	4096 bit
CBJ RSA B2B ICA	4096 bit
CBJ RSA B2C ICA	4096 bit
Entity Certificate	≥ 2048 bit

Table 10: Key sizes for certificate type issued in the CBJ-PKI

Where the acceptable algorithms for generating signing key pairs are:

Algorithms	Key Length
DSA	(L, N) = (2048, 224), (2048, 256) or (3072, 256) bit
ECDSA	≥ 224 bit
RSA	≥ 2048 bit

Table 11: Acceptable algorithms for generating signing key pairs

The CBJ-PKI will not issue a certificate to any Entity that does not adhere to requirements regarding key size on the certificates they request.

6.1.6 Public Key Parameters Generation and Quality Checking

The algorithm used in the CBJ-PKI for key generation is RSA. However; the acceptable algorithms for generating signing key pairs are describe in Table10 above.

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

All certificates issued in the CBJ-PKI contain the “KEY USAGE” and “ENHANCED KEY USAGE” attributes, as defined by the X.509 v3 standard. Section 7 contains further details on key usage.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CBJ Information Security and Cyber Security Management Policies has established controls to ensure that the risks derived from a private key compromise are managed and kept under reasonable levels.

6.2.1 Cryptographic Module Standards and Controls

Pursuant to the provisions of (Annex 1: Technical Standards and Specifications) issued by Telecommunication Regulatory Commission (TRC), The main components in the CBJ-PKI are required to use Hardware Security Modules at least compliant with FIPS 140-1 level 3 or higher for PKI components.

All cryptographic modules are operated such that the private cryptographic keys are never output in plaintext.

Activation of the cryptographic module requires activation material under multi-party control. Physical access to the cryptographic module requires two-party control (see Section 5.1.2).

Entities, in addition to their roles as RAs and EAs, are responsible for deploying solutions that enable generating key pairs and perform digital signing operations on secure signature creation devices (i.e. cryptographic modules), and must fulfil the requirement of FIPS 140-1 level 3 or higher to be qualified signature creation device. Therefore ensuring far greater protection of private keys.

6.2.2 Private Key Multi-Person Control

Private keys for Certification Authorities are always under multi-person control. Activation data needed to enable a Certification Authority will be shared in such a way that at least two authorized persons are needed to perform any sensitive operation on a Certification Authority.

Private keys for subscribers are under the sole control them or authorized representative. In addition to their responsibility for storing, managing and protecting it.

6.2.3 Private Key Escrow

CBJ-PKI does not support private key escrow for any certificate type. All key pairs must be generated, stored, and protected by the certificate holder. CBJ-PKI does not retain or manage private keys under any circumstance.

6.2.4 Private Key Backup

No stipulation.

6.2.5 Private Key Archival

The Private Keys are never archived for any PKI participant in CBJ-PKI (see Section 6.2.3).

6.2.6 Private Key Transfer Into or From a Cryptographic Module

For Certification Authorities operating under the CBJ-PKI it is mandatory that key pairs are generated into Hardware Security Modules as defined in section 6.2.1. Private Keys can only be transferred to adequate hardware security modules for back-up and recovery operations

6.2.7 Private Key Storage on a Cryptographic Module

CA private keys are only stored in encrypted form in the hardware cryptographic module (HSM) at least compliant with FIPS 140-1 level 3 or higher .

Entities, in addition to their roles as RAs and EAs, are responsible for deploying solutions that enable generating key pairs and perform digital signing operations on secure signature creation devices (i.e. cryptographic modules), and must fulfil the requirement of FIPS 140-1 level 3 or higher to be qualified signature creation device. Therefore ensuring far greater protection of private keys.

6.2.8 Method of Activating a Private Key

The private key in Certification Authorities in the CBJ-PKI is activated by initiating the PKI Software and activating the HSM where the key is stored.

The FIPS-140-1 level 3 or higher validated cryptographic module requires multi-party control through several split digital credentials and a combination of PINs and passphrases in order to activate cryptographic module partitions. PINs and passphrases require a minimum of six characters. Entry of PINs and passphrases is not displayed while being entered.

The specific method for activating subscriber private keys is stipulated in section 6.4.

6.2.9 Method of Deactivating a Private Key

The private key in Certification Authorities is deactivated by shutting-down the associated server or by terminating the PKI software or by extracting or shutting-down the HSM that contains the key. This task can be done by a System Administrator and, when planned, has to be notified and authorized to/from the CA Responsible.

Entities, in addition to their roles as RAs and EAs, are responsible for deactivating private keys.

6.2.10 Method of Destroying a Private Key

The procedure to destroy a private key is initiated in the following cases:

1. Private Key is no longer used.

2. The token or HSM containing the key has deteriorated to an extent that prevents normal usage.

3. A lost or stolen token is found, and the keys it contained are suspected to be compromised.

A private key can be destroyed by the key owner or a legal representative. In such cases the corresponding certificate will be revoked, and the community will be notified. The particular procedures is detailed in the appropriate Key Destruction Document and will be documented as of the formal authorization process (Key Destruction Request Form or equivalent).

Entities, are responsible for destroying subscriber private keys.

6.2.11 Cryptographic Module Rating

No stipulation additional to section 6.2.1.

6.3 Other Aspects of Key Pair Management

This section includes additional stipulations regarding key pair management.

6.3.1 Public Key Archival

Public keys in the CBJ-PKI are archived after the expiry or revocation of the corresponding digital certificate.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The certificates are operational for signature validation from the issuance to the end of the archival period stated in 6.3.1.

CBJ-PKI follows defined validity and usage periods for CA key pairs and certificates:

1. **Online-Issuer CA:** Certificate and key pair are valid for 5 years.
2. **Online-Policy CA:** Certificate and key pair are valid for 20 years.
3. **Offline-Root CA:** Key pair and self-signed certificate are valid for 20 years.
4. **Subscribers**: The usage period for key pairs is 2 years.

6.4 Activation Data

This section stipulates the management of the data necessary to activate the private keys.

6.4.1 Activation Data Generation and Installation

Activation data for Certification Authorities are generated and stored in cryptographic tokens and/or smart cards and are only used by authorized persons.

In addition, these tokens require a password or PIN in order to enable the activation process. Activations requiring a multi-person control will be enforced by splitting the activation data in several tokens.

6.4.2 Activation Data Protection

Only the authorized persons know the password or PIN to activate the private keys.

In the case of end entities, only the certificate subscriber is entitled to know this information. In all cases, the owner of the activation data is required to safeguard the secrecy of this information.

6.4.3 Other Aspects of Activation Data

No additional detail.

6.5 Computer Security Controls

This information is classified and therefore not made public. The documents describing Computer Security Controls are only available for the people involved in the CBJ-PKI and only disclosed to accredited external parties for auditing purposes.

Certification and Registration Authorities operating under the CBJ-PKI are required to meet these Security Controls. The compliance is periodically enforced by an auditing procedure.

6.5.1 Specific Computer Security Technical Requirements

This information is classified and therefore not made public.

6.5.2 Computer Security Rating

No stipulation.

6.6 Lifecycle Security Controls

This information is classified and is therefore not disclosed in detail. The detailed documents are available for review by external auditors after the appropriate authorization process.

6.6.1 System Development Controls

This information is classified and therefore not made public.

6.6.2 Security Management Controls

This information is classified and therefore not made public.

6.6.3 Life Cycle Security Controls

This information is classified and therefore not made public.

6.7 Network Security Controls

The CBJ-PKI enforces the adoption of effective controls to minimize any risk related to Network Security. The detailed information about these controls is classified and only made available for external auditors after the appropriate authorization process.

In particular, the server used for the CBJ-PKI Root CA is offline, physically disconnected from any computer network, and all communication of sensitive information is protected using encryption and digital signature techniques.

6.8 Time Stamping

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic based.

The CBJ-PKI provides a time-stamping service that will be responsible for replying to timestamp issuance requests to provide trusted time entry.

The key pair of the CBJ-PKI TSA authority is secure within an HSM that complies with FIPS 140-2 Level 3 certification. NTP protocol is used to synchronize date and time with a trusted time source.

CBJ TSA service which has developed according to Pursuant to the provisions of (Annex 1: Technical Standards and Specifications) issued by Telecommunication Regulatory Commission (TRC).

7. Certificate, CRL, and OCSP Profiles

All certificates issued under the CBJ-PKI are compliant to:

1. **ITU-T Recommendation X.509:** The base specification for public key certificates. Defines fields, extensions, and general structure

2. **RFC 5280:** Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. This is the IETF profile for X.509 certificates in PKI, specifying allowed extensions, naming rules, validation, etc.

7.1 Certificate Profile

This section summarizes the certificate profiles for the types of certificates covered by this document, which contained in:

1. Root CA.
2. B2B/ B2C Policy CA.
3. B2B/ B2C Issuing CA.
4. B2B Enrollment Agent/ API Client.
5. B2B/ B2C Digital Signature for Natural Person.
6. B2B/ B2C Digital Signature for Legal Entity.

Certificates issued by the CBJ-PKI conform to the Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles.

7.1.1 Version Number(s)

All certificates issued under CBJ-PKI CAs are compliant with X.509 v3.

7.1.2 Certificate Extensions

The following table include the extensions included in the certificate profiles covered by this CPS:

Certificate Policy Identifier	Extensions	
Root CA	☒Version ☒Signature Algorithm ☒Public Key Parameters ☒Signature Hash Algorithm ☒Subject Key Identifier ☒Certificate Policies ☒Basic Constraints	☒Serial Number ☒Ca Version ☒Thumbprint ☒Key Usage ☒Subject ☒Valid From ☒Valid To

	☒Issuer	☒Public Key
B2B/ B2C Policy CA	☒Version ☒Signature Algorithm ☒Public Key Parameters ☒Signature Hash Algorithm ☒Subject Key Identifier ☒Certificate Policies ☒Basic Constraints ☒Authority Key Identifier ☒CRL Distribution Point ☒Authority Information Access	☒Serial Number ☒CA Version ☒Thumbprint ☒Key Usage ☒Subject ☒Valid From ☒Valid To ☒Public Key ☒Issuer ☒Certificate Template Name
B2B/ B2C Issuing CA	☒Version ☒Signature Algorithm ☒Public Key Parameters ☒Signature Hash Algorithm ☒Subject Key Identifier ☒Basic Constraints ☒Authority Key Identifier ☒CRL Distribution Point ☒Authority Information Access	☒Serial Number ☒Thumbprint ☒Key Usage ☒Subject ☒Valid From ☒Valid To ☒Public Key ☒Issuer ☒Certificate Template Name
B2B Enrollment Agent/ API Client	☒Version ☒Signature Algorithm ☒Public Key Parameters ☒Signature Hash Algorithm ☒Subject Key Identifier ☒Authority Key Identifier ☒CRL Distribution Point ☒Enhanced Key Usage ☒Application Policies ☒Authority Information Access	☒Serial Number ☒Thumbprint ☒Key Usage ☒Subject ☒Valid From ☒Valid To ☒Public Key ☒Issuer ☒Certificate Template Information
B2B/ B2C Digital Signature for Natural Person	☒Version ☒Signature Algorithm ☒Public Key Parameters ☒Signature Hash Algorithm ☒Subject Key Identifier ☒Authority Key Identifier ☒CRL Distribution Point ☒Enhanced Key Usage ☒Application Policies	☒Serial Number ☒Thumbprint ☒Key Usage ☒Subject ☒Valid From ☒Valid To ☒Public Key ☒Issuer
B2B/ B2C Digital Signature for Legal Entity		

	☒Authority Information Access ☒SMIME Capabilities	☒Certificate Template Information

Table 12: Certificate Extensions

7.1.3 Algorithm Object Identifier

Certificates issued under the CBJ-PKI must use the SHA-2 algorithm, the Algorithm object identifiers are:

Algorithm	OID
sha256WithRSAEncryption	{iso(1)member-body(2)us(840)rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
sha384WithRSAEncryption	{iso(1)member-body(2)us(840)rsadsi(113549) pkcs(1) pkcs-1(1) 12 }
sha512WithRSAEncryption	{iso(1)member-body(2)us(840)rsadsi(113549) pkcs(1) pkcs-1(1) 13 }

Table 13: Algorithm Object Identifier

7.1.4 Name Forms

Certificates issued under the CBJ-PKI contain the "Distinguished Name", in X.500 format, for the issuer and the subscriber, set in the fields "Issuer" and "Subject" respectively, and are formed as defined in section 3.1.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

All certificates issued by CBJ-PKI will contain the "Certificate Policies" extension.

A certificate issued by the CBJ-PKI will assert in the certificate policies extension one or more of the OIDs listed in the following Table:

Certificate Policy Identifier	OID
Self-signed Root Certification Authority	::={ 1.3.6.1.4.1.56472.1.1 }
B2B Certification Authority	::={ 1.3.6.1.4.1.56472.1.1.1.2 }
B2C Certification Authority	::={ 1.3.6.1.4.1.56472.1.1.1.1 }
Certificate Request Agent	::={ 1.3.6.1.4.1.311.20.2.1 }
Server Authentication	::={ 1.3.6.1.5.5.7.3.1 }
Client Authentication	::={ 1.3.6.1.5.5.7.3.2 }
Code Signing	::={ 1.3.6.1.5.5.7.3.3 }
Document Signing	::={ 1.3.6.1.4.1.311.10.3.12 }
Secure Email	::={ 1.3.6.1.5.5.7.3.4 }

Table 14: Certificate Policy Object Identifier

7.1.7 Usage of Policy Constraints Extension

Policy constraints appear in the following table:

Certificate Policy Identifier	Description	Permitted uses
1. Root CA	Self-Signed Certification Authority that acts as Trust Anchor for the full CBJ-PKI Infrastructure.	☒ Certificate Signing ☒ CRL Signature
2. B2B/ B2C Policy CA	Intermediate Policy CA. Issues Certification Authorities owned by CBJ licensed/ Accredited by the TRC to operate under the CBJ-PKI	
3. B2B/ B2C Issuing CA	Certificate for subordinated Issuing CAs, operating under the B2B/ B2C Policy CA.	☒ Certificate Signing ☒ CRL Signature ☒ Digital Signature
4. B2B Enrollment Agent	Certificate issued to sign certification requests on behalf of another user.	☒ Digital Signature ☒ Key Encipherment
5. B2B API Client	Certificate issued to authenticate Participants services that consume Internal API.	
6. B2B/ B2C Digital Signature for Natural Person	Individuals authenticates and digitally signs contractual e documents, liable data, and/or emails.	☒ Digital Signature ☒ Non-Repudiation ☒ Key Encipherment
7. B2B/ B2C Digital Signature for Legal Entity	Individuals representing legal entities authenticates and digitally signs contractual e-documents, liable data, and/or emails on behalf of the legal entity.	

Table 15: Usage of Policy Constraints Extension

The following table summarize the certificate profile defined by CBJ-PKI:

Certificate Policy Identifier/ Attributes	Enrollment Agent	API Client	Digital Signature for Natural Person	Digital Signature for Legal Entity
Issuer	**B2B ICA**	**B2B ICA**	**B2B ICA B2C ICA**	**B2B ICA B2C ICA**
X509 Version	**As in section 7.2.1**			
Serial Number	**Unique integer (unique for each certificate issued by given CA).**			
Signature Algorithm	**SHA256RSA - See section 7.1.3**			
Validity Period	**See section 6.3.2- The usage period for key pairs is 2 YEARS**			
Subject Public Key Info	**See section 6.1.5 Key length ≥ 2048 bit Algorithm = RSA**			
Subject Key Identifier	**OCTET STRING containing hash of the subject's public key**			
Authority Key Identifier	**OCTET STRING containing hash of the issuer's public key**			
Enhanced Key Usage	**☒ Certificate Request Agent**	**☒ Server Authentication ☒ Client Authentication ☒ Certificate Request Agent**	**☒ Client Authentication ☒ Document Signing ☒ Secure Email**	**☒ Code Signing ☒ Client Authentication ☒ Document Signing ☒ Secure Email**
Certificate Template Information	**Identifier and version numbers of template used to issue the certificate.**			
Archive Subject Private Key	**NO**	**NO**	**NO**	**NO**
Subject Private Key Is Exportable	**YES**	**YES**	**YES**	**YES**

Table 16: Certificate Profile

7.1.8 Policy Qualifiers Syntax and Semantics

The certificates issued by CBJ-PKI Infrastructure CAs do not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The "Certificate Policy" identifies the Policy that the CBJ-PKI assigned explicitly with a certificate policy.

Software Applications requiring a specific certificate profile to process a digital signature must check this extension in order to verify the suitability of the certificate for the intended purpose. See section 7.1.6.

7.2 CRL Profile

In general, CRLs generated under the CBJ-PKI are compliant with RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile).

7.2.1 Version Number(s)

The CRL linked to the certificates use the X.509 standard, in its version 3.

7.2.2 CRL and CRL Entry Extensions

The certificates issued with this CP include a "Certificate Distribution Point" extension, pointing to the repositories specified in section 2.1 of this document and the CRL issuance frequency in section 4.9.7

7.3 OCSP Profile

In general, the status of all certificates in the CBJ-PKI can be validated by sending requests compliant with RFC 2560.

7.3.1 Version Number(s)

CBJ-PKI provides support for Version 1 of RFC 2560.

7.3.2 OCSP Extensions

The certificates include the standard "Authority Information Access" extension, that contains a link to the OCSP responder server. Pointing to the repositories specified in section 2.1 of this document and for On-line revocation/status checking availability, see section 4.9.9.

8. Compliance, Audit, and Assessment

CBJ-PKI and TRC monitors and ensures compliance to legal, security and industry requirements, through internal and external audits as per each party determined role.

As defined by the Jordanian Legislation, TRC shall monitor the Certificates Authorities activities and for this purpose, it may undertake the following:

1. Inspecting the location where the Certification Authority operates, including the examination of the operating environment for electronic authentication system specifications.

2. Ensure the commitment of Certificates Authorities compliance to technical specifications and standards adopted by TRC.

3. Authentication System, Licensing and/or Accreditation terms and conditions, and any instructions or decision issued by the TRC.

For the purpose of Auditing and Monitoring CA's activities, TRC shall have the right to obtain a specialized technical support from third party. The TRC's major functions in this domain are:

1. TRC shall undertake the task of licensing and accreditation for any CA wishes to provide Certificate services within the Kingdom in compliance to the provisions of this law and related regulations.

2. TRC is responsible for issuing instructions that determine the requirements and specifications that should be present in the Certificate Practices Statement to be disclosed by the CA.

3. A mechanism to protect and store the certificate's information for the period specified by the TRC.TRC shall issue the necessary instructions to execute the provisions of this Bylaw, including:

    a. Information that shall be included in the certificate.

    b. Retention of electronic certificates records issued by the Certificates Authorities, thus set them electronically viewable on ongoing basis, and retention period.

    c. Determine the requirements and specifications must be met by the Certificate Practice Statement (CPS).

4. Licensing or Accreditation duration shall be stated in its decisions and considered renewable on the condition of fulfilling the requirements specified in this Bylaw and related instructions.

5. TRC shall issue the necessary instructions to execute the provisions of this Bylaw, including:

a. Information that shall be included in the certificate.

b. Retention of electronic certificates records issued by the Certificates Authorities, thus set them electronically viewable on ongoing basis, and retention period.

c. Determine the requirements and specifications must be met by the Certificate Practice Statement (CPS).

6. TRC shall charge the following Fees as stipulated in the related legislations for the following:

   a. Initial License or Accreditation.

   b. Annual renewal for the License or Accreditation.

8.1 Frequency or Circumstances of Assessment

All Certification Authorities must follow the adequate assessment program on an annual frequency as TRC regulations:

1. Upon starting the operation of the CBJ-PKI and before starting the issuance of certificates.

2. Every year from the date of starting the operation of the CBJ-PKI, or from the date of accreditation.

3. When submitting a request for renewal of the license or accreditation.

8.2 Identity/Qualifications of Assessor

The assessor will be selected when an audit or assessment is required. Any company or professional whose services are contracted as auditor or assessor will be required to fulfil these requirements:

1. Adequate and accredited capability and experience to perform the required services (PKI audit, Security assessment, etc.)

2. In the case of external audits, independence from the CBJ-PKI.

8.3 Assessor Relationship to Assessed Entity

For external audits, the CBJ-PKI audit policy does not allow any kind of legal, organizational or other relationship between the CA owner and the assessor, which would result in a conflict of interests.

8.4 Topics Covered by Assessment

The TRC defines and executes the official assessment process for all Certification Authorities willing to operate in Jordan. The CBJ-PKI are subject to audits and assessment by both:

1. The TRC.
2. Independent third-party auditors, adequate and accredited capability and experience to perform the required services (PKI audit, Security assessment, etc.).

The scope of these assessments includes:

1. Certificate Practice Statements issued by CBJ-PKI.
2. The Root CA, Policy CAs and Issuing CAs owned by the CBJ-PKI. These services are audited against the TRC criteria.
3. Commitment to the technical requirements and standards issued by the TRC.
4. Commitment to the law, regulations, and relevant instructions issued by the TRC.

In particular, it will be ensured compliance with all the relevant controls and Reference Audit List stipulated by TRC.

8.5 Actions Taken as a Result of Deficiency

In the case a deficiency is identified during the assessment, the CBJ-PKI will adopt and will be responsible for all necessary corrective measures. In the case of a severe deficiency affecting the reliable operation of a Certification or a Registration Authority, the CBJ-PKI could decide “with restriction to TRC regulations” to temporarily suspend the activities of the affected systems or services until the deficiency is solved.

8.6 Communication of Results

The assessment results or external audits will be conformed as detailed Report includes all the topics covered by the executed assessment program in detail. The audit report must include both the results and a description of the available technical solutions; it must also include the field and impact of the defect or violation on operations, the proposed deadlines for implementing corrective solutions.

The detailed report is deemed private and only available to the following parties:

1. Jordanian Telecommunication Regulation Commission (TRC).
2. Certification Authority owner-Central Bank of Jordan (CBJ).

9. Other Business and Legal Matters

This section includes the stipulations for business and legal matters and should be understood as having a contractual value by all the PKI participants.

9.1 Fees

Services bounded to the issuance, usage or revocation of the certificates can apply certain fees that must be efficiently communicated by the CA to subscribers, before issuing their certificates as The CBJ reserves the right to charge a fee to each Entity in order to support operations of the CBJ-PKI.

9.1.1 Certificate Issuance or Renewal Fees

At this time, the CBJ does not charge a fee for certificate issuance or renewal.

9.1.2 Certificate Access Fees

At this time, The CBJ does not charge a fee for certificate access.

9.1.3 Revocation or Status Information Access Fees

At this time, The CBJ does not charge a fee for access to certificate revocation or status information.

9.1.4 Fees for Other Services

Currently, the CBJ does not charge a fee for any other services.

9.1.5 Refund Policy

At this time, since there are no fees associated with CBJ services, there is no refund policy in place.

9.2 Financial Responsibility

The financial responsibilities of these certificates is a sole decision of the CBJ.

9.2.1 Insurance Coverage

The CBJ does not provide any insurance or warranty coverage for the use of any certificates issued either by the CBJ-PKI CAs.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following information is classified as confidential and is therefore not allowed to be exposed to third parties:

1. The private keys for all entities in the CBJ-PKI, including subscribers
2. All information about CBJ-PKI operations.
3. All information about security parameters and detailed assessment and audit reports.
4. All personal information exchanged between the parties during operations and affected by legal or regulations.
5. Continuity and emergency plans.
6. Audit and operation logs.
7. All information classified explicitly as “SECRET”, “TOP SECRET” when generated or exchanged among involved parties.

9.3.2 Information Not Within the Scope of Confidential Information

The CBJ-PKI classifies as publicly accessible information:

1. The information contained in the Certification Practices Statement.
2. The certificates issued under the CBJ-PKI.
3. The list of revoked certificates (CRL).
4. All information classified expressly as “PUBLIC”, “INTERNAL USE”.

9.3.3 Responsibility to Protect Confidential Information

The CBJ-PKI is responsible of the protection of the confidential information generated or communicated during all operations. Delegated parties, as the entities acting as Registration Authorities, are responsible for protecting confidential information that has been generated or stored by their own means.

For end entities, the certificate subscribers are responsible to protect their own private key and all activation information (i.e. passwords or PIN) needed to access or use the private key.

9.4 Privacy of Personal Information

The Privacy Policy of the CBJ-PKI is compliant with the legal requirements in Jordan.

9.4.1 Privacy Plan

Personal Information directly communicated to the CBJ-PKI by the certificate subscribers is stored in a database owned by the CBJ-PKI operator. This database is conveniently protected to avoid any unauthorized access or modification.

9.4.2 Information Treated as Private

In any case, the following information is considered and treated as private:

1. Certificate requests (approved or rejected) and other personal information collected during the certificate life cycle and not included in these certificates.
2. Private keys generated or stored in the CBJ-PKI.

9.4.3 Information Not Deemed as Private

In any case, the following information is considered as "non private", and therefore the CBJ-PKI has rights to make it public:

1. The issued (or pending of issuance) certificates, and their details.
2. The condition of "subscriber" of a CBJ-PKI for a person or entity.
3. Characteristics included in the certificate, including validity periods, liability limits, serial number, etc.
4. The status of the certificates (valid, pending, revoked, expired, etc.).
5. The Certificate Revocation Lists.
6. Any information required demonstrating the accreditation of a participant in the CBJ-PKI

9.4.4 Responsibility to Protect Private Information

The CBJ-PKI ensures the compliance of the legal obligations for Certification Authorities, Registration Authorities and other entities operating under the CBJ-PKI. Each of these participants is responsible to protect the private information that has been provided by subscribers or other participants in the issuance and maintenance of digital certificates.

9.4.5 Notice and Consent to Use Private Information

In order to perform the certification provisioning service, the CBJ-PKI is required to obtain the consent to use the subscriber's personal information. This consent is understood by the acceptance of the "Terms and Conditions" by the subscriber. This acceptance is recognised by the subscriber's written signature on the "Subscriber Agreement".

It's the Registration Authority responsibility to provide notice or obtain consent of their customers in order to perform the certification provisioning service.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The CBJ-PKI will disclose personal information of the participants if required by a judicial or administrative process, according to Jordanian legislations. Any request for release information will be authenticated.

9.4.7 Other Information Disclosure Circumstances

There are no other disclosure circumstances.

9.5 Intellectual Property Rights

All Intellectual Property rights, including the digital certificates and CRLs issued under the CBJ-PKI, Object Identifiers, and the CP/CPS are owned by the CBJ-PKI.

The private and public keys are the property of their respective owners.

Any commercial or protected trademark included in the Distinguished Name of a certificate is the responsibility of the certificate subscriber.

9.6 Representations and Warranties

This section includes general stipulations.

9.6.1 CA Representations and Warranties

Certification Authorities operating under the CBJ-PKI undertakes that:

1. Their certificates meet all material requirements of this CP/CPS.
2. No errors have been introduced in the certificate information by the entities approving the Certificate Application as a result of a failure when managing the Certificate Application.
3. There are no material misrepresentations of fact in the certificate by the entities approving the Certificate Application or Issuing the Certificate.
4. Availability of revocation services (when applicable) and use of a repository conforming to the applicable CP/CPS in all material aspects.

9.6.2 RA Representations and Warranties

Only Sectors subject to the control and supervision of the Central Bank of Jordan may integrate with CBJ-PKI and utilize provided services, in order to act as RAs and EAs for their customers.

The Registration Authorities operating under the CBJ-PKI undertakes that:

1. The Certificates managed by the RA meet all material requirements of this CP/CPS.
2. The identification requirements are dutifully executed according to this CP/CPS.
3. Managing subscriber certificate lifecycle (approval, rejection, cancellation) including certificate status change request workflow (revoke/activate/request/approve).

9.6.3 Subscriber Representations and Warranties

The Subscribers of certificates issued under the CBJ-PKI warrant that:

1. All information supplied by the Subscriber and contained in the Certificate is true and valid.
2. All representations made by the Subscriber in the submitted Certificate Application are true and valid.
3. His or her private key is protected, and that no unauthorized person has ever had access to the Subscriber's private key.
4. The Certificate is being used exclusively for authorized and legal purposes, consistent with this CPS.
5. Each electronic signature created using the private key corresponding to the public key listed in the Certificate is the electronic signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the electronic signature is created.

9.6.4 Relying Party Representations and Warranties

Relying parties of certificates issued under the CBJ-PKI warrant that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences of their failure to perform the Relying Party obligations in terms of this CPS.

9.6.5 Representations and Warranties of Other Participants

The CBJ-PKI makes no representation or warranty for other participants.

9.7 Disclaimers of Warranties

Disclaimer of warranties (if existing) is mentioned in this CPS and included as part of the agreement presented to subscriber's agreement.

9.8 Limitations of Liability

Neither CBJ, CBJ-PKI nor the employee shall be liable for any (a) direct (b) indirect or special damages and/or (c) loss of income or profit and/or (d) any other form of consequential damages howsoever arising, and regardless of form or cause of action.

CBJ-PKI does not assume financial liability for any losses resulting from the use of its certificates or services.

9.9 Indemnities

This CBJ-PKI does not include any claims of indemnity.

9.10 Term and Termination

This section refers to the times and validity periods related to this document.

9.10.1 Term

This document becomes effective when approved and once published. This CPS has no specified term.

9.10.2 Termination

This Document (at the current version) is valid until replaced by a new/modified version. Termination of this CPS is at the discretion of the CBJ.

9.10.3 Effect of Termination and Survival

The certificates issued during the validity period of the version of this document are bound to the clauses hereby included until the end of these certificates archival period.

9.11 Individual Notices and Communications with Participants

Any notice, request or any other communication required by this document can be addressed to contact information in section 1.5.2.

9.12 Amendments

The CBJ-PKI can unilaterally amend this document, by attaining adhering to the following procedure:

1. The modification needs to be justified under legal and technical considerations.
2. There is a modification procedure and change management for these amendments.
3. Any implications to the participants due to such amendments will be conveniently publicised

9.12.1 Procedure for Amendment

The entity with the authority to make and approve any change in the CPS/CP is the Central Bank of Jordan/ FinCERT (described in section 1.5 of this document).

On the assumption that the CBJ decides to modify the CPS/CP, a new version of the document will be generated. The version of the document (exposed in all the pages of the document) is controlled with two numbers separated by a period.

The first number (major version) is incremented if the new version could affect the acceptance of the certificates by the users. The second number (minor version) is incremented if the amendment is not considered to affect the certificate acceptance criteria. These two version numbers are included as the last two numbers in the OID identifying the document.

Once a new version of the document is approved, the procedures stipulated in section 9.12.2 will be executed.

9.12.2 Notification Mechanism and Period

Any modification in this document will be published and affected participants will be directly notified if necessary.

In particular, it is not considered necessary to directly notify participants of “minor version” changes of the documents. In the case of a change in the “major version” of a document, the CBJ-PKI will notify the affected participants

9.12.3 Circumstances Under Which OID Must be Changed

The OID of this CP/CPS Document will be modified to reflect a change of major version of the document.

9.13 Dispute Resolution Procedures

In the event of any disputes, customers have the right to submit a formal complaint. Complaints may be filed with the Central Bank concerning all licensed banks and regulated financial institutions.

As a first step, the complaint must be submitted directly to the concerned bank or financial institution. If the institution fails to respond, or if the response is deemed unsatisfactory, the customer has the right to escalate the complaint to the Central Bank or seek legal remedies through the judiciary.

9.14 Governing Law

The operations of the CBJ-PKI are regulated by the "electronic transactions law No. (15) of the year 2015" and “the licensing and accreditation bylaw” Number 11 of the year 2014.

9.15 Compliance with Applicable Law

The CBJ-PKI will comply with applicable law.

9.16 Miscellaneous Provisions

This section includes miscellaneous contractual and legal clauses

9.16.1 Entire Agreement

No stipulation

9.16.2 Assignment

This CP/CPS does not assign rights or responsibilities other than what is specified in this CP/CPS.

9.16.3 Severability

In the event that a clause or section of this document is declared not valid by a court of law or other entity having authority, the remainder of the document shall remain valid.

9.16.4 Enforcement (Attorney's Fees or Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

Force Majeure clauses, if existing, are included in the Subscriber Agreements.

9.17 Other Provisions

No stipulations.