BTC Licensed CA- Certificate Policy and Certification Practice Statement (CP/CPS)

Issue Date:	12 December 2019
Effective Date:	28 September 2022
Document Identifier:	POL-BTC-CPS-01
Version:	1.2
Document Classification:	**PUBLIC**
Document Status:	**FINAL**

Document OID: **2.16.682.1.101.5000.1.4.1.1.1**

Policy Authority Committee

Digitally signed by Policy Authority Committee
Date: 2022.10.03
14:25:45 +03'00'

Document Revision History

Version	Date	Author(s)	Revision Notes and Comments
1.0	12 December 2019	Parag Parikh	First official issue
1.1	22 December 2019	Parag Parikh	- Rectification in URL for CA Certificates in AIA extension of child CA certificate profile. - Rectification in URL for CRL in CDP extension of child CA certificate profile.
1.2	29 September 2021	Sivaraman Natrajan	- Added new certificate profiles for Digital Signature Certificate (DSC) and Time Stamping Authority (TSA) CAs - Changed CRL frequency

	Reviewer	Approver
Name	Navaneetha Gopala Krishnan	Ibrahim AlKharboush
Title	General Manager	Chairman - Policy Authority Committee
Date	22-JUL-2022	23-JUL-2022

Table of Contents

1. Introduction

BTC Licensed Certification Authority (henceforth referred as BTC LICENSED CA) is owned by the Baud Telecom Company (referred as BTC). BTC LICENSED CA is a Certification Authority under the Saudi National Root-CA. This is achieved by the Saudi National Root-CA issuing a digitally signed CA Certificate that authenticates the Public Key of the BTC LICENSED CA.

BTC LICENSED CA is licensed by Communications and Information Technology Commission (CITC) and regulated by National Centre for Digital Certification (NCDC). For more information on NCDC, please refer to https://www.ncdc.gov.sa

CA acts as a “Certification Service Provider”, as defined under the definition of Article 1(21) of Kingdom’s e-Transactions Law. The Digital Certificates issued by BTC LICENSED CA provides legal validity for its electronic signature, under the definitions of Article 1(17) of Kingdom’s e-Transactions Law.

The e-Transactions Law of Kingdom of Saudi Arabia grants legal recognition to digital / electronic signatures. This provides that “If a signature is required for any document or contract or the like, such requirement shall be deemed satisfied by an electronic signature generated in accordance with this Law. The electronic signature shall be equal to a handwritten signature, having the same legal effects.”

BTC LICENSED CA provides trust services to secure the exchange of information between key stakeholders. Participants include, Government, Citizens and Businesses.

1.1. Overview

This document combines the CP and CPS documents and is thus presented as a single document.

This document defines a high level of trust and assurance for use by all BTC LICENSED CA PKI participants. It provides definitions for the policies by which the BTC LICENSED CA operates.

This document also establishes the processes and procedures followed by the BTC LICENSED CA to:

- Issue cross certificates to Level-2 issuing CAs which are under full control of BTC,
- Certificate issuance, management and revocation for supportive administrative roles for the BTC LICENSED CA operations,
- Manage core infrastructure that supports BTC PKI setup,
- Maintain or revoke certificates issued by the BTC LICENSED CA, and
- Operate the OCSP responder(s)

This CP and CPS comply with:

- Saudi National Root CA CP and CPS.
- Internet Request for Comment “RFC 3647” of Internet Engineering Task Force (IETF) for Certificate Policy and Certification Practice Statement.
- The latest versions (as on date of this CP/CPS) of the CA/Browser Forum (CABF) Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (Ref: https://cabforum.org)
- Adobe Approved Trust List (AATL)/Microsoft Certificate policies.

- Internet Request for Comment “RFC 5280” of Internet Engineering Task Force (IETF) for Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

If any inconsistency exists between this CP/CPS and aforesaid requirements, then the aforesaid Requirements take precedence over this CP/CPS.

The terms used in this document shall have the meanings as defined in BTC LICENSED CA Glossary section which can be found at https://www.emdha.sa.

BTC LICENSED CA constitutes the Policy Authority as specified in section 1.3.1 of this CP/CPS. This document is subject to regular review by the Policy Authority and subject to amendment as well as exceptions to mitigate material, imminent impacts to subscribers, partners, relying parties, and/or others within the certificate ecosystem where practical workarounds do not exist. Such exceptions are tracked, documented and reported as part of the audit process.

Under the descriptions provided in this CP/CPS, BTC LICENSED CA establishes a hierarchical trust with the self-signed offline Saudi National Root-CA.

It is the responsibility of all parties applying for or using a digital certificate issued under this CP/CPS, to read this CP/CPS and the PKI Disclosure Statement (PDS) to understand the practices established for the lifecycle management of the certificates issued by the BTC LICENSED CA. Any application for digital certificates or reliance on BTC LICENSED CA issued certificates signifies understanding and acceptance of this CP/CPS and its supporting policy documents.

BTC LICENSED CA is a Level-1 subordinate/intermediate CA in the Saudi National PKI hierarchy, maintained and operated by BTC in an online environment. The BTC LICENSED CA shall issue certificates to approved Level-2 Issuing CAs and supportive functions for the BTC LICENSED CA operations, and Certificate Revocation Lists (CRLs).

1.1.1 Certificate Policy

This Certificate Policy document is assigned the OID: 2.16.682.1.101.5000.1.4.1.1.1. OIDs will not be included as a certificate policy extension in CA certificates.

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 BTC LICENSED CA. It also states how BTC LICENSED CA meets the requirements for policies defined in this document.

This CP/CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by BTC LICENSED CA as governed by this document and related documents which describe Saudi National PKI requirements and use of Certificates.

1.1.3 Interaction with other PKIs

BTC LICENSED CA will decide on issues related to cross-certification with other Certification Authorities under the directions of BTC Policy Authority Committee, after obtaining approval from NCDC.

1.1.4 Scope

This CP/CPS applies to all certificates issued by the BTC LICENSED CA. BTC LICENSED CA is a Level-1 subordinate CA in the Saudi National PKI hierarchy, maintained and operated by BTC in an online environment. The BTC LICENSED CA shall issue certificates and Certificate Revocation Lists (CRLs) only to approved Issuing CAs and supportive functions for the BTC LICENSED CA operations.

1.2. Document Name and Identification

The OID assigned to BTC by NCDC is: {joint-iso-itu-t(**2**) country(**16**) sa(**682**) sa-organizations(**1**) government-organizations(**101**) ncdc(**5000**) pki-public-key-infrastructure(**1**) licensed-cas(**4**) certificate-policies(**1**) baud-telecom-company-btc(**1**)}

The object identifier (OID) values corresponding to the organization, CP and CPS are as follows:

Entity / Certificate Policy	OID
Baud Telecom Company (BTC)	2.16.682.1.101.5000.1.4.1.1
BTC LICENSED CA Certificate Policy Document	2.16.682.1.101.5000.1.4.1.1.1
OCSP Certificate	2.16.682.1.101.5000.1.4.1.1.1.1

BTC LICENSED CA organizes its OID arcs for the various Certificates described in this CP/CPS as per the table “Certificate Types”

Certificate Types

Sl No	Certificate Type	Certificate Policy OID
1.	emdha eSign CA Certificate Policy Document	2.16.682.1.101.5000.1.4.1.1.2
2.	emdha DSC CA Certificate Policy Document	2.16.682.1.101.5000.1.4.1.1.3
3.	emdha TSA CA Certificate Policy Document	2.16.682.1.101.5000.1.4.1.1.4

1.3. PKI Participants

The following are the PKI Participants under the BTC LICENSED CA CP/CPS.

1.3.1 BTC Policy Authority Committee (BTC PAC)

BTC Policy Authority Committee (BTC PAC) is responsible for the governance of the BTC LICENSED CA. Its members are appointed by BTC. Its tasks include:

- Establishing and implementing its CP, CPS and PDS for CAs under its domain, in conjunction with the Saudi National PKI Policy document;
- Ensuring the operation of the BTC CAs comply with the requirements of its CP, CPS, PDS and Operations Policies and Procedures;
- Review and approve the Subscriber Agreement, Relying Party Agreement and other related Agreements based on the CA’s specific business requirements;
- Review the compliance of internal audits, external audits and any security assessments;
- Seeking resolution of disputes between participants operating in its domain;

- Act as liaison with NCDC; and
- Perform an annual review on key algorithms and lengths to determine appropriate level of security and assurance.
- Obtain NCDC approval for Issuing CAs under BTC Licensed CA
- Approval of Issuing CAs under BTC Licensed CA

1.3.2 BTC Licensed Certification Authority (BTC LICENSED CA)

The term BTC LICENSED CA refers to the entity owned and operated by BTC which is approved by NCDC to join the Saudi National PKI, directly under the Saudi National Root-CA.

BTC LICENSED CA is responsible for:

- Generation and issuance of Issuing CA certificates under the BTC LICENSED CA;
- Publication of Issuing CA certificates;
- Revocation of Issuing CA certificates;
- Publication of revocation information;
- Re-key of Issuing CAs;
- Conduct regular internal security audits;
- Assist in audits conducted by or on behalf of NCDC; and
- Performance of all aspects of the services, operations and infrastructure related to BTC LICENSED CA.

1.3.3 Registration Authority (RA)

BTC LICENSED CA shall designate RAs to perform the Subscriber Identification and Authentication and Certificate request and revocation functions defined in this CP and related documents.

The RA is obligated to perform certain functions pursuant to an RA Agreement including the following:

- Process Certificate application requests in accordance with this CP/CPS and applicable RA Agreement, and other policies and procedures with regard to the Certificates issued;
- Maintain and process all supporting documentation related to the Certificate application process;
- Process Certificate Revocation requests in accordance with BTC LICENSED CA CP/CPS, applicable RA Agreement, and other relevant operational policies and procedures with respect to the Certificates issued. Without limitation to the generality of the foregoing, the RA shall request the revocation of any Certificate that it has approved for issuance according to the conditions described in this document;
- Comply with the provisions of its RA Agreement and the provisions of the BTC LICENSED CA CP/CPS including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements; and

- Follow BTC LICENSED CA Privacy policy in accordance with BTC LICENSED CA CP/CPS and applicable RA Agreement.

1.3.4 Subscribers

Subscribers are individuals (end users), entities (organizations) or devices to whom certificates are issued and are legally bound by a Subscriber Agreement or Terms of use.

BTC LICENSED CA shall only issue certificates to the issuing CAs approved by BTC Policy Authority Committee and NCDC. Any subscriber under this CA's hierarchy asserts that he or she relies on the BTC LICESNSED CA certificate in accordance with this CP/CPS.

1.3.5 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the CA's or subscriber's identity to a public key. The Relying Party is responsible for checking the validity of the certificate by examining the appropriate certificate status information, using validation services provided by the BTC LICENSED CA. A Relying Party's right to rely on a certificate issued under this CP, requirements for reliance, and limitations thereon, are governed by the terms of the BTC LICENSED CA CP and the Relying Party Agreement.

1.3.6 Online Certificate Status Protocol Responder

Online Certificate Status Protocol (OCSP) Responders provide revocation status information. The BTC LICENSED CA shall make their certificate status information available through an OCSP responder in addition to any other mechanisms they wish to employ. The BTC LICENSED CA shall publish status information for the certificates it issues in a Certificate Revocation List (CRL).

1.4. Certificate Usage

1.4.1 Appropriate Certificate Uses

The use of Certificates supported by the BTC LICENSED CA is restricted to parties authorized by contract to do so. Entities and persons other than those authorized by contract may not use certificates for any purpose.

BTC Licensed CA shall issue certificates and Certificate Revocation Lists (CRLs) only to approved Issuing CAs and certificates required by the PKI components and supportive functions for the BTC LICENSED CA operations.

1.4.2 Prohibited Certificate Uses

Certificates issued under this CP shall not be authorized for use in any circumstances listed below, and the BTC LICENSED CA shall not be liable for any claims arising from such use.

BTC LICENSED CA certificates are not for use in circumstances where:

1. Usage of certificate is in connection to any activity, which is illegal under the laws of Kingdom of Saudi Arabia.

2. Usage of certificate is inconsistent with the certificate extensions in key usage and extended key usage.
3. Usage of certificate is above the designated reliance limits indicated in the EMDHA Warranty Policy
4. Usage of certificate is for any equipment operated in hazardous conditions or under fail proof conditions (eg. Nuclear facilities, aircraft navigation, medical devices, direct life support devices, other systems where any failure could lead to injury, death or environmental damage etc.)
5. Usage of certificates is in connection with fraud, pornography, obscenity, hate, defamation, harassment and other activity that is contrary to public policy.
6. Usage for man-in-the-middle (MITM) or traffic management of domain names or IPs that the certificate holder does not legitimately own or control.

BTC LICENSED CA certificates do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment into which the Certificate has been installed is free from defect, malware or virus.

BTC LICENSED CA certificates should be used only for the designated purposes, in addition to specific types and categories. An end subscriber certificate should not be used for CA function, like, to issue/sign a certificate under it. Similarly, the CA certificates are to be used only for CA function, and not to perform any end subscriber usage like document signing, etc.

More generally, certificates shall be used only to the extent where use is consistent with all applicable laws, statutes, orders, decrees, rules, regulations, and court judgements of this jurisdiction or governmental order; of Kingdom of Saudi Arabia.

1.5. Policy Administration

1.5.1 Administration Organization

This CP is administered by BTC Policy Authority Committee (see section 1.3.1).

1.5.2 Contact Person

Queries regarding BTC LICENSED CA CP/CPS shall be directed to:

Email: policy@emdha.sa

Telephone: +966-11-4663000

Fax: +966-11-4613311

Any formal notices required by this CP/CPS shall be sent in accordance with the notification procedures specified in section 9.12.2 of this CP/CPS.

1.5.3 Person Determining CP Suitability for the Policy

The BTC LICENSED CA Policy Authority Committee is responsible for approving the BTC LICENSED CA CP/CPS and establishing that the it conforms to the intended requirements in accordance with policies and procedures specified by Saudi National PKI.

1.5.4 CP/CPS Approval

Changes or updates to the BTC LICENSED CA CP/CPS document shall be made in accordance with the stipulations of Saudi e-Transactions act and bylaws and are subject to BTC LICENSED CA Policy Authority Committee approval, as well as NCDC Approval.

1.6. Definitions and Acronyms

The terms used in this document shall have the meanings as defined in BTC LICENSED CA Glossary section which can be found at https://www.emdha.sa/.

2. Publication and Repository Responsibilities

2.1. Repositories

BTC LICENSED CA-issued Level-2-CA certificates and certificate revocation lists (CRLs) will be published in repositories. BTC LICENSED CA shall operate highly-available repositories to support the BTC LICENSED CA's operations. The repositories shall be available for public internet access through HTTP and HTTPS on a 24x7 basis.

2.1.1 Repository Obligations

Repositories shall support:

- Appropriate standard-based access protocols;
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CP/CPS; and
- Access control mechanisms, when necessary to protect the repository availability and information.

2.2. Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

The BTC LICENSED CA shall publish in the appropriate repository: CA Certificates and CRLs.

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

2.2.2 Publication of CA Information

This CP/CPS shall be made available to all BTC LICENSED CA PKI participants at BTC LICENSED CA website https://www.emdha.sa. This website is the only source for up-to-date documentation and BTC LICENSED CA reserves the right to publish newer versions of the documentation without prior notice.

Additionally, BTC LICENSED CA will publish an approved, current and digitally signed version of the BTC LICENSED CA CP/CPS and PDS.

The information published through this website resource is the only authoritative source for:

- The certificate revocation list (CRL) for BTC LICENSED CA;
- All Level-2-CA Certificates issued under BTC LICENSED CA;
- Test websites for the CA Certificates (wherever applicable)
- CP/CPS and PDS Documents.
- Subscriber and Relying Party Agreements.

2.2.3 Interoperability

Pointers to repository information in CA and end entity Certificates shall only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties. The extensions containing such URIs shall comply to the RFC 5280 specifications.

2.3. Time or Frequency of Publication

CA Certificates are published promptly following their generation and issuance. CRL information shall be published as set in section 4.9.7.

This CP/CPS shall be reviewed and/or updated at least annually. This CP and any subsequent changes shall be made available to the participants as set forth in section 2.2.2 within 15 days of approval by the BTC PAC and NCDC.

This CP/CPS and PDS are provided as public information on BTC LICENSED CA official website https://www.emdha.sa. Public documents are only valid if they are published as a PDF, digitally signed by BTC.

The OCSP responder(s) will immediately report a certificate that has been revoked as set in section 4.9.9.

2.4. Access Controls on Repositories

The information published in BTC LICENSED CA online repository is publicly accessible information and, has been provided with unrestricted read only access to the contents of the repository. BTC LICENSED CA shall put in place sufficient safeguards, logical and physical, to prevent any unauthorized write access or alteration/modification of repository entries.

3. Identification and Authentication

3.1. Naming

3.1.1. Types of Names

Each Certificate must have a unique identifiable Distinguished Name (DN) according to the X.500 standard. Naming conventions for BTC LICENSED CA is approved by the Saudi National Root-CA, while BTC LICENSED CA approves BTC Level-2 Issuing CA names.

3.1.2. Need for names to be meaningful

The CA certificates issued pursuant to this CP/CPS are meaningful only if the names that appear in the certificates are understood and used by Relying Parties. Names used in the certificates must identify the CA in a meaningful way to which they are assigned.

The subject name contained in a CA certificate must be meaningful in the sense that BTC LICENSED CA and NCDC are provided with proper evidence of the association existing between the name and the entity to which it belongs.

3.1.3. Anonymity or Pseudonymity of Subscribers

Not Applicable.

3.1.4. Rules for Interpreting Various Name Forms

The naming convention used by BTC LICENSED CA is ISO/IEC 9595 (X.500) Distinguished Name (DN).

3.1.5. Uniqueness of Names

All distinguished names shall be unique across the BTC LICENSED CA.

3.1.6. Recognition, Authentication, and Role of Trademarks

Where permitted or required, the use of a trademark is reserved to the holder of that trademark.

3.2. Initial Identity Validation

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.

3.2.2. Authentication of Issuer Identity

Not Applicable

3.2.3. Identity-Proofing of Individual Identity

3.2.3.1. Identity-Proofing of End User Subscribers

BTC LICENSED CA shall not issue end-entity or subscriber certificates directly under it.

BTC LICENSED CA may issue certificates internally within the organization for its supporting roles, such as internal RAs. BTC PAC will verify information in the application, authenticity of the requesting representative and the representative's authorization to act in the assigned role.

3.2.3.2. Identity-Proofing of Device Subscribers

BTC LICENSED CA shall not issue certificates to device subscribers.

BTC LICENSED CA may issue certificates to devices internally within the organization for its supporting components, such as OCSP. BTC PAC will verify information in the application, authenticity of the requesting device sponsor and the representative's authorization to act in the assigned role.

3.2.3.3. Identity-Proofing of Organizational Entities

If the Certificate subject is an organizational entity, then an authorized representative of the entity applies for a certificate. The BTC LICENSED CA will authenticate the identity of this representative and the validation of authority with an acceptable identity proof and a reliable method of communication.

BTC LICENSED CA shall not issue certificates to third-party level-2 CAs, only to BTC owned level-2 CAs.

3.2.4. Non-verified Subscriber Information

Non-verified information shall not be included in certificates issued under BTC LICENSED CA, unless specifically mentioned in the Certificate Types section in Appendix-A.

3.2.5. Validation of Authority

As stated in 3.2.3.3

3.2.6. Criteria of Interoperation

No stipulation.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-Key

An authorized representative should request re-key of CA, in compliance with the BTC LICENSED CA Operations Policy.

3.3.2. Identification and Authentication for Re-key After Revocation

If a CA certificate is revoked, an authorized representative of the CA shall provide sufficient information before BTC LICENSED CA initiates generation of the new CA certificate.

3.4. Identification and Authentication for Revocation Requests

Revocation requests shall be authenticated to verify that the revocation has been requested by an authorized entity.

Acceptable procedures for authenticating the revocation requests include communication with the requesting entity to provide reasonable assurances that the person or organization requesting revocation is who they claim to be. Such communication, depending on the circumstances, may include one or more of the following: face-to-face verification, telephone, facsimile, e-mail, postal mail, or courier service.

Prior to the revocation of a certificate, BTC PAC shall verify that the revocation has been requested by an entity authorized to request revocation.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

This section specifies the requirements for initial application for certificate issuance by BTC Licensed CA.

4.1.1. Submission of Certificate Application

Applications for Level-2- CAs shall be submitted and approved by BTC PAC and NCDC.

4.1.2. Enrollment Process and Responsibilities

Please refer to BTC LICENSED CA Operations Policy

4.2. Certificate Application Processing

4.2.1. Performing Identity-proofing Functions

RAs shall perform identification and authentication of all required certificate information as described in the BTC LICENSED CA Operations Policy.

4.2.2. Approval or Rejection of Certificate Applications

The RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required information as described in Appendix-A of respective certificate type.
- NCDC approval
- BTC PAC approval

The RA will reject a certificate application if:

- Identification and authentication of all required applicant information as described in the Appendix-A of this CP and the BTC LICENSED CA Operations Policy cannot be completed;
- The requestor fails to furnish supporting documentation upon request;
- The requestor fails to respond to notices within a specified time; or
- The RA believes that issuing a certificate to the requestor may bring the BTC LICENSED CA or Saudi National PKI into disrepute.

Policies specific to each certificate type have been detailed in the Certificate Types section in Appendix-A. It is mandatory to comply with all policies specific to the respective certificate type.

Detailed procedures for CA and RA issuance are described in BTC LICENSED CA Operations Policy.

4.2.3. Time to Process Certificate Applications

No Stipulation.

4.3. Certificate Issuance

4.3.1. CA Actions During Certificate Issuance

When RAs receive a request for Certificate, it is not issued before the applicant accepts the terms of Agreement (for CAs).

Following successfully completion of the registration process, the BTC LICENSED CA will create and sign the certificate if all certificate requirements have been met, and make the certificate available to the requesting CA and/or the requesting RA.

Detailed procedures for CA and RA issuance are described in BTC LICENSED CA Operations Policy.

4.3.2. Notification to Subscriber of Certificate Issuance

Not Applicable.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Certificate acceptance is governed by the agreements set out between the BTC LICENSED CA and CA Applicants, any requirements imposed by BTC LICENSED CA CP and CPS and the relevant agreements under which the certificate is being issued.

The use of a Certificate or the reliance upon a Certificate signifies acceptance by that person of the terms and conditions of the CP and applicable agreements by which they irrevocably agree to be bound.

4.4.2. Publication of the Certificate by the CA

Level-2-CA Certificates will be published, once accepted, in the appropriate repository as described in section 2.1.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

NCDC shall be informed by email when a Level-2-CA has been issued under the BTC Licensed CA.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Level-2-CAs shall use their certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of the Agreement (for CAs), this CP/CPS, and applicable laws. Level-2-CAs shall protect their Private Keys from access by any other party and shall notify the BTC LICENSED CA upon the compromise of the private key or any reasonable suspicion of compromise.

4.5.2. Relying Party Public Key and Certificate Usage

The Relying Party (RP) Agreement becomes effective when the RP relies on information provided by the BTC LICENSED CA or a CA/subscriber under it, regarding a specific transaction that the RP uses to accept or reject their participation in the transaction. The RP's use of the Repository, or any CRL or OCSP services is governed by the RP Agreement and BTC LICENSED CA CP/CPS. The RP is solely responsible for deciding whether or not to rely on the information in a certificate provided by BTC LICENSED CA. The RP bears the legal consequences of any failure to comply with the obligations set in the RP agreement.

4.6. Certificate Renewal

Certificate renewal is the issuance of a new certificate without changing the public key or any other information in the certificate. Certificate renewal shall not be allowed for BTC LICENSED CA issued certificates.

4.7. Certificate Re-Key

Re-keying a certificate (key update) refers to the issuance of new certificate with a different key pair and serial number while retaining other subject information from old certificate.

The new Certificate may be assigned a different validity period and/or signed using a different issuing CA private key and/or use a different approved signing algorithm.

4.7.1. Circumstances for Certificate Re-key

Manual Certificate re-key may take place after a certificate is revoked and the Level-2-CA information is still accountable.

BTC PAC may also decide to perform manual certificate re-key without revocation based on a risk-assessment, or based on business requirements for certificate validity period of Level-2-CAs or their subscribers.

4.7.2. Who can Request a Certificate Re-key

In accordance with the conditions specified in previous section, Certificate re-key may be requested by:

- BTC PAC for BTC LICENSED CA certificate;
- BTC PAC for Level-2 CAs under BTC LICENSED CA;

4.7.3. Processing Certificate Re-keying Requests

Re-key requests for Level-2-CAs and RAs shall follow a process similar to new issuance, as defined in BTC LICENSED CA Operations Policy.

4.7.4. Notification of Re-Keyed Certificate Issuance to Subscriber

Not Applicable.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

Conduct constituting acceptance of a re-keyed certificate is same as listed in section 4.4.1.

4.7.6. Publication of the Re-keyed Certificate by the CA

Same as listed in section 4.4.2.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

NCDC shall be notified by email upon re-key of Level-2-CA certificates.

4.8. Certificate Modification

Certificate modification for all applicants will be accomplished through Certificate re-key as specified in section 4.7.

The BTC LICENSED CA shall not support other forms of Certificate modification.

4.9. Certificate Revocation and Suspension

The CA will notify all participants of certificate revocation or suspension through access to the CRL in the CA repository.

4.9.1. Circumstance for Revocation of a Certificate

The following reasons identify the need for a certificate to be revoked:

- Contravened any provisions of the Saudi e-Transactions Act and Bylaws made there under;
- The Subject has failed to meet its obligations under this CP/CPS or any other applicable Agreements, regulations, or laws;
- BTC PAC determines that revocation of a Certificate is in the best interest of Saudi National PKI;
- BTC PAC determines that a Certificate was not issued correctly in accordance with this CP/CPS;
- The private key corresponding to the public key in the certificate has been lost, disclosed without authorization, stolen or compromised in any way;
- There has been an improper or faulty issuance of a certificate due to:
  - A material prerequisite to the issuance of the Certificate not being satisfied;
  - A material fact in the Certificate is known, or reasonably believed, to be false.
- BTC PAC requests a Level-2-CA or RA certificate to be revoked;

4.9.2. Who Can Request Revocation of a Certificate

The following entities can request revocation of a certificate:

- NCDC can request the revocation of any certificate issued by BTC LICENSED CA;
- BTC PAC can request the revocation of any certificates issued under its authority;
- BTC LICENSED CA can request the revocation of any RA or LRA certificates;
- The RA for their own certificate or other RA certificates(s), if any certificates/individuals are suspected or known for key compromise, affiliation change or cessation of operation/employment;
- A legal, judicial or regulatory agency in Saudi Arabia, within applicable laws and in coordination with BTC PAC.

If any request for revocation cannot be resolved, the request is subject to the Dispute Resolution process described in BTC LICENSED CA Dispute Resolution Policy.

4.9.3. Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The CA or RA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements.

Subject to circumstances for revocation in 4.9.1, An investigation into the need for revocation of a Level-2-CA certificate will be done by BTC PAC under which the following is carried out:

- Analyze and validate the need for revocation and obtaining authorization for the revocation;
- Investigation results shall determine the decision to revoke a certificate
- Upon decision to not revoke, the investigation results shall be recorded.

- Upon decision of revocation:
    - Investigation summary is recorded;
    - The reason for the revocation is recorded;
    - A CRL (Certificate Revocation List) is immediately generated and published in the CA repository and specified as revoked by respective OCSP Responder(s);
    - A notification containing the certificate details, date and time of revocation, and reason for revocation is issued to the Level-2-CA, NCDC and Saudi National Root CA.

Revocation of RA certificates maybe performed without investigation, the procedure for which is provided in BTC LICENSED CA Operations Policy.

4.9.4. Revocation Request Grace Period

Revocation request grace period is not permitted once a revocation request has been verified and approved.

4.9.5. Time within which CA must Process the Revocation Request

BTC LICENSED CA shall process authorized revocation requests within seven days.

4.9.6. Revocation Checking Requirements for Relying Parties

Relying Parties should comply with the signature validation requirements defined in the Relying Party Agreement.

4.9.7. CRL Issuance Frequency

The BTC LICENSED CA will publish its CRLs at least once every eight days, and at the time of any Certificate revocation of CAs under it.

4.9.8. Maximum Latency of CRLs

CRLs shall be published in the Repositories within 30 minutes of Certificate revocation. Certificate status information is updated within 60 minutes of certificate revocation.

4.9.9. Online Revocation Checking Availability

BTC LICENSED CA shall make CRLs available in repositories as described in section 2.1.

BTC LICENSED CA shall also provide access to an OCSP Responder covering the certificates they issue.

4.9.10. Online Revocation Checking Requirements

The BTC LICENSED CA shall make its Certificate status information available through an OCSP responder.

4.9.11. Other Forms of Revocation Advertisements Available

The BTC LICENSED CA shall not provide other forms of revocation advertisements.

4.9.12. Special Requirements Related to Key Compromise

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

BTC LICENSED CA will,

(1) determine the scope of certificates that must be revoked,
(2) publish a new CRL at the earliest feasible time,
(3) use reasonable efforts to notify NCDC, Level-2-CAs, subscribers and potential relying parties that there has been a key compromise, and
(4) generate new CA key pair as per BTC LICENSED CA operations policies and procedures.

4.9.13. Circumstances for Certificate Suspension

If BTC PAC suspects that a certificate may be revoked for one of the circumstances described in Section 4.9.1, the BTC LICENSED CA may suspend the suspected certificate pending completion of investigation.

4.9.14. Who Can Request Suspension

Same as 4.9.2.

If any request for suspension cannot be resolved, the request is subject to the Dispute Resolution process described in the BTC LICENSED CA Dispute Resolution Policy.

4.9.15. Procedure for Suspension Request

A request to suspend a certificate shall identify the certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated (e.g., digitally or manually signed). The CA or RA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements. For suspension of RA Certificates refer to BTC LICENSED CA Operations Policy.

4.9.16. Limits on Suspension Period

The period for which a Certificate shall be suspended will be defined by the BTC PAC, but shall not exceed ninety (90) days.

4.9.17. Circumstances for Terminating Suspended Certificates

A suspended Certificate is reactivated when BTC PAC or the entity which requested the suspension of a Certificate is satisfied that the circumstances leading to the suspension are no longer valid. Once reactivated, the certificate will be valid for the remainder of its initial life time.

A suspended Certificate is revoked when BTC PAC or the entity which requested the suspension of a Certificate is satisfied that the circumstances leading to the suspension are indeed valid.

When the period for suspension has reached its maximum duration without resolution, the certificate shall be revoked.

4.9.18. Procedure for Terminating the Suspension of a Certificate

A request to unsuspend a certificate shall identify the certificate to be unsuspended, explain the reason for unsuspension, and allow the request to be authenticated (e.g., digitally or manually signed). The BTC LICENSED CA or RA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements. Detailed procedure is provided in BTC LICENSED CA Operations Policy.

4.10. Certificate Status Services

The status of public certificates is available from CRLs in the repositories and via OCSP responder(s).

Revocation entries on a CRL or OCSP response shall not be removed until after the expiry of the revoked certificate.

4.11. End of Subscription

No stipulation.

4.12. Key Escrow and Recovery

4.12.1. Key Escrow Policy and Practices

No keys will be escrowed for the BTC LICENSED CA, Level-2-CAs or RAs.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5. Facility Management and Operational Controls

5.1. Physical Security Controls

BTC operates the BTC LICENSED CA and Repositories at Tier III qualified data center, with appropriate physical and procedural access controls for all hardware and software sub-systems used in the issuance and revocation of certificates. BTC limits access to sensitive CA zones to personnel in Trusted Roles (see section 5.2.1 of this CP).

BTC LICENSED CA is co-located in third-party data center and follows the physical security requirements specified as below:

- Permit only authorized access to the hardware;
- Store all removable media and paper containing sensitive plain-text information in secure containers;
- Monitor, either manually or electronically, for unauthorized intrusion at all times; and
- Maintain and periodically inspect access logs.

RA equipment shall be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the CA environment.

A security check of the facility housing the CAs equipment shall occur on a regular basis.

5.1.1. Site Location and Construction

The location and construction of the facility housing the BTC LICENSED CA equipment is consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and multi-factor access controls, provides robust protection against unauthorized access to the CA equipment and records.

Main Site (Primary) Location: Riyadh

Alternate Site (DR Site) Location: Al Khobar (400+ KMs away from Main Site)

5.1.2. Physical Access

BTC PKI systems are protected by atleast four zones of physical security, with access to the lower zone required before gaining access to the higher and more secure zone. Progressively restrictive physical access privileges control access to each zone. Sensitive CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical zones. Physical access is automatically logged and video recorded. Additionally, zones enforce individual access control through the use of two factor biometric authentication. Unescorted personnel, including un-trusted employees or visitors, are not allowed into such secured areas unless accompanied by trusted personnel.

Main Site is protected by seven zones of physical security. More details are provided in the Physical Security Documentation.

BTC LICENSED CA has implemented policies and procedures to ensure that the physical environments in which the BTC LICENSED CA systems are installed maintain a high level of security:

- CA systems are installed in a secure facility that is isolated from outside networks, with all access controlled;
- CA is separated into a series of progressively secure areas; and
- The entrances and exits from the secure areas are under constant video surveillance and all systems that provide authentication, as well as those that record entry, exit and network activity, are in secured areas.

The security techniques employed are designed to resist a large number and combination of different forms of attack. The mechanisms used include:

- Perimeter alarms
- Closed circuit television
- Electronic access controls using two-factor authentication
- Multi-person access for most secure zones
- Human guards

To prevent tampering, cryptographic hardware is stored in a most secure area of the BTC PKI datacenter, with access limited to authorized personnel.

Human guards continually monitor the facility housing the CA equipment on a 24x7x365 basis. The BTC PKI datacenter facility is never left unattended.

The security mechanisms employed are commensurate with the level of threat in the equipment environment.

5.1.3. Power and Air Conditioning

Power to the BTC PKI datacenter is delivered through 2 different active-active feeds. Sufficient power capacity is available to the datacenter. Sufficient resilience is available in the Tier III datacenter using battery backup and N+1 generator to provide sufficient time to respond and act on any power related events.

The cooling system is designed as N+1 according to uptime institute’s tier 3 requirements. Sufficient monitoring for cooling systems is in place to ensure optimum cooling is available to the aisle/rack level.

5.1.4. Water Exposure

The BTC LICENSED CA shall ensure that CA equipment is installed such that it is not in danger of exposure to water (e.g., on elevated floors).

5.1.5. Fire Prevention and Protection

The CA equipment is housed in a facility with appropriate fire suppression and protection systems.

Some of the measures deployed include:

- Fire-resistant walls and pillars;
- Modern FM-200 fire suppression systems to detect and suppress fire with appropriate 24x7 monitoring

- The controls implemented comply meet all applicable safety regulations of the Kingdom of Saudi Arabia.

5.1.6. Media Storage

BTC LICENSED CA shall ensure that CA media is stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains archive or backup information is duplicated in an alternate location with reasonable distance between the two sites.

5.1.7. Waste Disposal

Sensitive media and documentation that are no longer needed for operations are destroyed using appropriate disposal processes. For example, sensitive paper documentation is shredded, burned, or otherwise rendered unrecoverable. HSM and related devices are physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal. Other electronic media is physically destroyed prior to disposal.

5.1.8. Off-Site Backup

Full system backups of CAs, sufficient to recover from system failure, shall be made on a periodic schedule as per procedures approved by BTC PAC.

5.2. Procedural Controls

5.2.1. Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the BTC LICENSED CA.

Trusted roles and personnel assigned to each trusted role are defined in the BTC Trusted Roles document.

5.2.2. Number of Persons Required per Task

BTC LICENSED CA shall ensure separation of duties for critical CA functions to prevent one person from maliciously using the PKI systems without detection. Each user's system access is limited to those actions which are required to fulfill their responsibilities.

A single person may be sufficient to perform tasks associated with a role, except for the activation of the CA's signing Private Key. Activation of the CA's signing Private Key shall require actions by at least two individuals. Two-role-authorization, Split-knowledge and ownership techniques such as split-password's and MofN tokens shall be deployed to perform any critical CA signing key operations, key backup or key recovery operation.

5.2.3. Identity-proofing for Each Role

An individual shall identify and authenticate himself before being permitted to perform any actions set forth above for that role or identity.

5.2.4. Separation of Roles

Role separation, when required, may be enforced either by the CA equipment, or procedurally, or by both means.

Separation of roles is identified in the BTC Trusted Roles document.

5.3. Personnel Controls

5.3.1. Background, Qualifications and Experience Requirements

All persons filling trusted roles shall be selected on the basis of skills, experience, loyalty, trustworthiness, and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA are set forth in the BTC Trusted Roles document.

While performing any critical operation, one of the trusted roles should be held by a Saudi Citizen.

5.3.2. Background Check and Clearance Procedures

BTC LICENSED CA conducts background investigations for all CA personnel (trusted roles) positions. Background check shall take into account the following:

- A check (for completeness and accuracy) of the applicant's CV;
- Independent identity check (National ID card, Passport or similar document);
- Availability of satisfactory character reference, i.e. one business and one personal;
- Confirmation of claimed academic and professional qualifications;
- Interviews with references shall be done as required; and
- Security clearance.

Security clearance shall be repeated every 3 years for personnel holding trusted roles.

5.3.3. Training Requirements

The BTC LICENSED CA shall ensure that all personnel receive appropriate training. Such training shall address relevant topics such as PKI and Information security concepts, security requirements, operational responsibilities and associated procedures.

The RA Administrator(s) engaged in Certificate issuance shall be given detailed training to perform their tasks. BTC LICENSED CA shall design examination based on the training which is to be qualified by each RA Administrator.

Documentation of all personnel who received training and the level of training completed shall be maintained by the BTC LICENSED CA.

5.3.4. Retraining Frequency and Requirements

Individuals responsible for PKI roles are made aware of changes in the CA operation. Any significant change to the operations shall have a training/awareness plan, and the execution of such plan shall be documented.

The BTC LICENSED CA shall review and update its training program at least once every two years to accommodate changes in the CA system.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

BTC LICENSED CA shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions (i.e., not permitted by the CP, CPS and/or other procedures) involving the CA or its associated components.

5.3.7. Contracting Personnel Requirements

BTC LICENSED CA may employ independent contractors as may be necessary. When independent contractors are employed, they will be subjected to the same process, procedures and controls as prescribed in this document under 'Personnel Controls'.

5.3.8. Documentation Supplied to Personnel

BTC LICENSED CA will make available to its personnel its CP, CPS, and any relevant documents required to perform their jobs competently and satisfactorily.

5.4. Audit Logging Procedures

BTC LICENSED CA will implement and maintain Trustworthy Systems to preserve an audit trail for material events and for key life cycle management, including key generation, backup, storage, recovery, destruction and management of cryptographic devices, the CA and OCSP Responder.

5.4.1. Types of Events Recorded

BTC LICENSED CA shall ensure recording in audit log files all events relating to the security of the CA system hosted in its data center. All security audit capabilities of the CA operating system and CA applications shall be enabled. Such events include, but are not limited to:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement;
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of certificate requests;
    e. Issuance of Certificates; and
    f. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies;

e. Firewall and router activities; and
f. Entries to and exits from the CA facility.

Log entries MUST include the following elements:

- Date and time of entry;
- Identity of the person making the journal entry; and
- Description of the entry.

All logs, whether electronic or manual, must contain the date and time of the event and the identity of the Entity which caused the event. The CA shall also collect, either electronically or manually, security information not generated by the CA system such as:

- Physical access logs;
- System configuration changes and maintenance;
- CA personnel changes;
- documentation relating to certificate requests and the verification;
- documentation relating to certificate revocation;
- Discrepancy and No compromise reports;
- Information concerning the destruction of sensitive information;
- Current and past versions of all Certificate Policies;
- Current and past versions of Certification Practice Statements;
- Vulnerability Assessment Reports;
- Threat and Risk Assessment Reports;
- Compliance Inspection Reports; and
- Current and past versions of Agreements.

5.4.2. Frequency of Processing Data

Audit logs are required to be processed in accordance with BTC LICENSED CA Audit and Compliance Policy.

5.4.3. Retention Period for Security Audit Data

The BTC LICENSED CA shall retain all system generated (electronic) and manual audit records onsite for a period not less than six months from the date of creation.

Video recording of CA facility access will be retained for a minimum of 90 days.

5.4.4. Protection of Security Audit Data

The BTC LICENSED CA shall protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction. This can be achieved by:

- Read access to the journal information is granted to personnel requiring this access as part of their duties;
- Only authorized roles can obtain access; and

- The journal is stored in appropriate database and access to the database is protected against unauthorized access by the application and through special security measures on the operating system level.

5.4.5. Security Audit Data Backup Procedures

BTC LICENSED CA shall back up all audit logs and audit summaries. Detailed policy and standard operating procedures are provided in IT Security Policies Manual.

5.4.6. Security Audit Collection System (Internal or External)

The audit collection system is detailed in IT Security Policies Manual.

5.4.7. Notification to Event-Causing Subject

Event-causing subject are not notified.

5.4.8. Vulnerability Assessments

Vulnerability assessments of security controls shall be performed by the BTC LICENSED CA for its CA and other supporting systems hosted in its data center at least every three months, and after any significant system or network changes as determined by the CA. Such assessments shall be performed on public and private addresses for the BTC LICENSED CA and associated components.

BTC LICENSED CA security program shall include an annual Risk Assessment which includes identification of foreseeable internal and external threats, assess the likelihood and potential damage of these threats and assess the sufficiency of the policies, procedures, information systems and technology. Based on the Risk Assessment exercise, the BTC LICENSED CA shall develop, implement, and maintain a security plan to control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

Apart from this BTC PKI datacenter(s) are constantly (24x7) monitored, and all attempts to gain unauthorized access to any of the services are logged and analyzed.

BTC performs third party penetration testing on public IPs for hosted CA infrastructure at least once a year and after infrastructure or application upgrades or modifications that the CA determines are significant.

5.5. Records Archival

5.5.1. Types of Events Archived

CA archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA.

These include:

- Audit logs generated by the CA software;
- Agreements;
- Records pertaining to identification and authentication information;
- Physical access logs;
- System configuration changes and maintenance;
- CA personnel changes;

- Discrepancy and compromise reports;
- Information concerning the destruction of sensitive information;
- Current and past versions of Certificate Policies and Certification Practice Statements;
- Vulnerability Assessment Reports, and associated remediation reports;
- Threat and Risk Assessment Reports;
- Compliance Inspection Reports;
- Documents identifying all personnel who received CA related training and the level of training completed;
- BTC LICENSED CA shall archive any necessary keys and passwords for a period of time sufficient to support the functionalities; and

The CA shall make these audit logs available to its Qualified Auditor upon request.

5.5.2. Retention Period for Archive

BTC LICENSED CA's minimum retention period for archive data is established at 10 years.

Applications needed to process the archive data shall also be maintained for the archival retention period.

5.5.3. Protection of Archive

Only authorized individuals shall be permitted to review the archive. The contents of the archive shall not be released except as determined by BTC PAC, or as required by law. Records and material information relevant to use of, and reliance on, a certificate shall be archived. Archive media shall be stored in a secure storage facility separate from the component itself. Any secondary site must provide adequate protection from environmental threats such as temperature, humidity and magnetism.

5.5.4. Archive Backup Procedures

Backup of archive is detailed in IT Security Policies Manual.

5.5.5. Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information obtained from the BTC PKI time-server(s). System logs shall be time stamped and all connected systems shall use a dedicated time server to maintain synchronized time.

The system time of all servers is synchronized with official time-source. BTC PKI time-source is also synchronized with the GPS clock as a backup. Further, there is a procedure in place that checks and corrects drift in the real time clock.

5.5.6. Archive Collection System (Internal or External)

The type of Archive Collection System, whether internal or external, is specified in IT Security Policies Manual.

5.5.7. Procedures to Obtain and Verify Archive Information

As specified in IT Security Policies Manual.

5.6. Key Changeover

The CA system utilized by the BTC LICENSED CA supports key rollover, allowing CA keys to be changed periodically, as required. This may be done to minimize risk to the integrity of the BTC LICENSED CA or based on business requirements for certificate validity period of Level-2-CAs or their subscribers. Once changed the new key is used for certificate signing purposes. The unexpired older keys are used to sign CRL's until all certificates signed by the unexpired older private key have expired. Old and unexpired CA signing keys, if retained for signing CRLs shall be protected just as the new key.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

If the BTC LICENSED CA detects a potential hacking attempt or other form of compromise to the CA, it shall perform an investigation in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in BTC LICENSED CA Operations Policy shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

BTC PAC shall be notified in case of:

- Suspected or detected compromise of the CA system;
- Physical or electronic attempts to penetrate the CA system;
- Denial of Service attacks on a CA system component;
- Any incident preventing the CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

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

BTC LICENSED CA maintains backup copies of hardware, system, databases, and private keys in order to rebuild the CA capability in case of software and/or data corruption. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, Business Continuity procedures will be enacted.

5.7.3. CA Private Key Compromise Recovery Procedures

Recovery procedure is as specified in BTC LICENSED CA Operations Policy.

5.7.4. Business Continuity Capabilities after a Disaster

BTC LICENSED CA has developed robust Business Continuity Management System for critical PKI services to provide the minimum acceptable level of assurance to its subscriber for service availability.

All BTC LICENSED CA critical infrastructure equipment at the primary site have built-in hardware fault-tolerance, and configured to be highly available with auto-failover switching. BTC LICENSED CA currently maintains copies of backup media and infrastructure system software, which include but are not limited to: PKI services related critical data; database records for all certificates issued and audit related data, at its offsite business continuity and disaster recovery storage facilities.

BTC LICENSED CA Business Continuity Management System (BCMS) demonstrates the capability to restore or recover critical PKI services at the primary site within twenty-four (24) hours in the event of service(s) non-availability.

Business Continuity Management components at BTC LICENSED CA are being regularly tested, verified, and updated to be operational to address crisis situation in the event of a disruption. For security reasons details of these plans are not publicly available.

BTC LICENSED CA business continuity plan includes:

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

BTC LICENSED CA has developed recovery plans to mitigate the effects of any kind of natural, man-made or equipment failure related disaster.

BTC LICENSED CA has implemented an alternate recovery site as per industry standards to provide full recovery of critical PKI services within five days following a disaster at the primary site. BTC LICENSED CA Business Continuity Policy contains further details.

5.8. CA or RA Termination

5.8.1. CA Termination

No stipulation.

5.8.2. RA Termination

Upon termination of the RA Agreement, the RA certificate shall be revoked and the tasks performed by the RA must be handled by another RA.

BTC LICENSED CA will be the custodian of CA/RA archival records in case of termination.

6. Technical Security Controls

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Key pair generation for CAs will be witnessed and attested to by a party separate from the Trusted Roles as mentioned in the BTC LICENSED CA Key Generation Ceremony Policy.

Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. CA's shall use Hardware Security Modules (HSMs) for CA key generation and storage. HSM's shall be minimum FIPS 140-2 Level 3 validated.

BTC LICENSED CA key pair generation is performed by multiple trusted personnel using trustworthy systems and processes that provide security and required cryptographic strength for the generated keys.

BTC LICENSED CA key pair is generated in pre-planned Key Generation Ceremony. The activities performed in Key Generation Ceremony are video recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by BTC PAC.

6.1.2. Private Key Delivery to Subscriber

Subscriber certificates are not issued by the BTC LICENSED CA.

6.1.3. Public Key Delivery to Certificate Issuer

Public keys generated by the applicant must be delivered for certificate issuance using industry standard secure protocol such as PKCS#10 or similar.

6.1.4. CA Public Key Delivery to Subscribers and Relying Parties

The BTC LICENSED CA shall ensure that Subscribers and Relying Parties receive and maintain the trust anchor (Saudi National Root CA) in a trustworthy fashion. Methods for trust anchor delivery may include:

- A trusted role loading the trust anchor onto Tokens delivered to Subscribers via secure mechanisms;
- Distribution of trust anchor through secure out-of-band mechanisms;
- Calculation and comparison of trust anchor hash or fingerprint against the hash made available via authenticated out-of-band sources; or
- Downloading trust anchor from websites secured with a currently valid certificate of equal or greater assurance level than the Certificate being downloaded and the site trust anchor already on the Subscriber system via secure means.
- Availability of CA certificate(s) in public repositories as described in section 2.1.

BTC LICENSED CA and Level-2-CA certificates shall be published on the website https://www.emdha.sa which may be downloaded by subscribers or relying parties.

6.1.5. Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. Key sizes are described as below for BTC LICENSED CA. All FIPS-approved signature algorithms shall be considered acceptable. Acceptable algorithms shall be maintained in accordance with the Saudi National PKI Policy.

All certificates issued shall use at least 4096-bit RSA keys OR at least NIST P-256 ECC keys, with Secure Hash Algorithm version (SHA-256) in accordance with FIPS 186-2 or equivalent.

TLS or other protocol providing similar security to accomplish any of the requirements of this CP/CPS shall use AES (minimum 128-bit key strength) for symmetric keys, and at least 4096-bit RSA or at least NIST P-256 ECC or equivalent for asymmetric keys.

The current BTC LICENSED CA key lengths for minimum key sizes are;

▪ BTC LICENSED CA Key Pair:	RSA 4096 bits
▪ OCSP Key Pair:	RSA 4096 bits

6.1.6. Public Key Parameters Generation and Quality Checking

The HSM pseudo-random number generator is validated by NIST. Public key parameters prescribed are generated in accordance with industry best practices.

6.1.7. Key Usage Purposes

BTC LICENSED CA key and private keys of Level-2-CAs shall be used for certificate and CRL signing.

6.2. Private Key Protection and Crypto-Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

Cryptographic modules employed in BTC LICENSED CA shall comply with FIPS-PUB 140-2 "Security Requirements for Cryptographic Modules". The Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the CA keys. Cryptographic hardware issued to RAs shall be at least FIPS 140-2 Level 2 compliant.

6.2.2. CA Private Key Multi-Person Control

Multi-person control of CA private key is achieved using an "m-of-n" split key knowledge scheme. BTC LICENSED CA keys can only be accessed on the physical and logical level by at least two trusted roles, and is achieved by M=2 in M-of-N scheme.

6.2.3. Private Key Escrow

Not Applicable.

6.2.4. Private Key Backup

6.2.4.1. Backup of CA Signing Private Key

BTC LICENSED CA signing Private Key shall be backed up under the same multi-person control as the original Signing Key. A second and third copy may be kept at CA backup locations for business continuity and Disaster Recovery. Procedures for BTC LICENSED CA signing Private Key backup shall be detailed in BTC LICENSED CA Backup and Restore Policy.

BTC LICENSED CA private keys that are physically transported from one facility to another shall remain confidential and maintain their integrity.

BTC LICENSED CA hardware containing CA private keys, and associated activation materials, shall be transported in a physically secure environment by authorized personnel in trusted roles, using multiple person controls, and using sealed tamper-evident packaging.

BTC LICENSED CA keys and associated activation materials shall be transported in a manner that prevents the key from being activated or accessed during the transportation event; and CA key transportation events shall be logged.

6.2.4.2. Backup of Subscriber Private Keys

Not applicable.

6.2.5. Private Key Archival

BTC LICENSED CA shall maintain controls to provide reasonable assurance that archived CA keys remain confidential, secured, and shall never be put back into production.

6.2.6. Private Key Transfer into or From a Cryptographic Module

The cryptographic modules implemented by BTC LICENSED CA are validated to FIPS 140-2 Level 3 ensuring that the CA keys cannot be exported to less secure media.

The BTC LICENSED CA keys can be cloned for secure backup from the master hardware cryptographic module to other hardware cryptographic module(s) using secure mechanisms so that they can be recovered if a major catastrophe destroys the production set of keys. Such backup or clones shall have the same level of authentication and access control as the production set.

6.2.7. Private Key Storage on Cryptographic Module

CA’s Private Key shall be stored on FIPS 140-2 Level 3 validated cryptographic module in encrypted form.

6.2.8. Method of Activating Private Keys

CA’s private key shall be activated by the main stakeholders and authorized personnel, as defined in BTC LICENSED CA Operations Policy, supplying their activation data. Such activation data shall be held on secure media and shall require the successful completion of a multi-person authentication process.

6.2.9. Methods of Deactivating Private Keys

CA’s private key shall be deactivated by the main stakeholders and authorized personnel, as defined in BTC LICENSED CA Operations Policy.

6.2.10. Methods of Destroying Private Keys

Copies of CA private keys shall be destroyed as per BTC LICENSED CA Cryptographic Devices Lifecycle Management Policy and Procedure.

6.2.11. Cryptographic Module Rating

As described in section 6.2.1.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archive

The Public Key is archived as part of the certificate archive process.

6.3.2. Certificate Operational Periods and Key Usage Periods

The table below details key usage and certificate lifetime for the corresponding keys:

Key/Certificate	**Maximum Validity Period**
BTC LICENSED CA signing key and certificate	120 months or valid not beyond 2029, whichever is earlier
Level-2 Issuing eSign CA key and certificate	120 months or valid not beyond 2029, whichever is earlier
Level-2 Issuing DSC CA key and certificate	120 months or valid not beyond 2029, whichever is earlier
Level-2 Issuing TSA CA key and certificate	120 months or valid not beyond 2029, whichever is earlier

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The CA cryptographic module activation data will be generated locally at the time of key generation by personnel in the trusted role and responsible for controlling the activation data.

6.4.2. Activation Data Protection

Written CA cryptographic module activation data is placed into tamper evident packages which are then stored within secure containers in a highly secured environment inside the BTC PKI Datacenter(s).

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

The computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards.

At a minimum, the datacenter(s) shall have following controls to ensure security of the systems:

- Hardened operating system;
- Software packages are only installed from a trusted software repository;
- Minimal network connectivity;
- Authentication and authorization for all functions;
- Strong authentication and role-based access control for all vital functions;
- Disk and/or file encryption for all relevant data; and
- Proactive patch management.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life-Cycle Security Controls

6.6.1. System Development Controls

The BTC LICENSED CA design, installation, and operation will be documented by qualified personnel. BTC operations personnel, with oversight by the BTC PAC, will develop and produce appropriate qualification documentation establishing that BTC LICENSED CA components are properly installed and configured, and operate in accordance with the technical specifications.

BTC LICENSED CA shall undertake reasonable precautions to prevent malicious software being loaded on the CA equipment. Only applications necessary to perform the CA operations shall be implemented. The CA systems and software shall be scanned for malicious code on first use and periodically thereafter.

Hardware and software implementation, including updates and patches are performed by trained and trusted personnel.

6.6.2. Security Management Controls

The configuration of the BTC LICENSED CA systems as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to software or configuration. A formal change-management methodology shall be used on-going maintenance of systems. Appropriate backups shall be taken before and after any major change to systems.

6.6.3. Life Cycle Security Ratings

No stipulation.

6.7. Network Security Controls

The BTC LICENSED CA shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Also, it shall employ network security and firewall management, including port restrictions and IP address filtering.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

BTC PKI datacenter(s) use a network design of multiple security layers making use of several security technologies including network firewalls, application firewalls, and Endpoint protection technologies to protect network access to on-line CA’s, Repository and OCSP Responder equipment.

Access shall not be provided to the BTC LICENSED CA through the public internet.

6.8. Time Stamping

Time stamping shall be supported for the Certificates, CRLs, and other revocation database entries containing time and date information from dedicated time-server(s) to maintain synchronized time.

Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber's Certificate;
- Revocation of a Subscriber's Certificate;
- Posting of CRL updates;
- OCSP response.

7. Certificate, CRL and OCSP Profiles

7.1. Certificate Profile

This section contains the rules and guidelines followed by this CA in populating X.509 certificates and CRL extensions. The Certificate profile for the Level-2-CAs is described in Appendix A.

7.1.1. Version Numbers

The BTC LICENSED CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2. Certificate Extensions

Level-2-CA certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CP.

7.1.3. Algorithm Object Identifiers

BTC LICENSED CA shall sign Certificates using `sha256WithRSAEncryption` algorithm (`1.2.840.113549.1.1.11`).

Algorithm identifier of the subject Public Key shall be `rsaEncryption` (`1.2.840.113549.1.1.1`)

7.1.4. Name Forms

Certificates issued by BTC LICENSED CA contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names are in the form of an X.501 printable string.

7.1.5. Name Constraints

No Stipulation.

7.1.6. Certificate Policy Object Identifier

No Stipulation.

7.1.7. Usage of Policy Constraints Extension

It is expected that all members of the BTC LICENSED CA apply to this policy.

7.1.8. Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9. Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical certificate policy extension shall conform to X.509 certification path processing rules.

7.2. CRL Profile

Certificate Revocation Lists are issued in the X.509 version 2 format in accordance with RFC 5280.

The BTC LICENSED CA CRL Profile is as below:

Field	Content	Comment
Version	`1`	
Algorithm	`SHA256withRSA`	

Issuer	`CN=BTC LICENSED CA`
	`O=BAUD Telecom Company`
	`C=SA`	

This update	*<issue date>*	
Next update	*<issue date + 8 days>*	Or immediately upon revocation
AuthorityKeyIdentifier	*<BTC LICENSED CA's Subject Key Identifier>*	
CRL number	*<number>*	

7.2.1. Version Numbers

The BTC LICENSED CA shall issue X.509 version two (v2) CRLs (populate version field with integer "1").

7.2.2. CRL and CRL Entry Extensions

Critical private extensions shall be interoperable in their intended community of use.

7.3. OCSP Profile

OCSP requests and responses shall be in accordance with RFC 6960.

7.3.1. Version Number

The version number for request and responses shall be v1.

7.3.2. OCSP Extensions

No stipulation.

8. Compliance Audit and Other Assessments

The BTC PAC shall be responsible for overseeing compliance of the BTC LICENSED CA, RAs, BTC LICENSED CA CP/CPS. BTC PAC shall ensure that the requirements of the BTC LICENSED CA CP/CPS and the provisions of applicable Agreements are implemented and enforced.

8.1. Frequency of Audit or Assessments

The BTC LICENSED CA shall be subjected to periodic compliance audits which are no less frequent than once a year. BTC LICENSED CA shall also be performing internal audit at least on a quarterly basis against a randomly selected sample for monitoring adherence and service quality.

8.2. Identity and Qualifications of Assessor

The audit under Saudi National PKI shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme; and
- Bound by law, government regulation, or professional code of ethics.

A licensed WebTrust auditor will be appointed to perform such compliance audits as a primary responsibility.

8.3. Assessor’s Relationship to Assessed Entity

To provide an unbiased and independent evaluation, the auditor and audited party shall not have any current or planned financial, legal or other relationship that could result in a conflict of interest.

8.4. Topics Covered by Assessment

The compliance audits will verify whether the CA PKI operations environment is in compliance with the applicable CP/CPS and supporting operational policies and procedures. The term CA PKI Operations environment defines the total environment and includes:

- All documentation, records;
- Contracts/agreements;
- Compliance with applicable Law;
- Physical and logical controls;
- Personnel and approved roles/tasks;
- Hardware (e.g. servers, desktops, hardware security modules, network devices and security devices); and
- Software and information.

The auditor shall provide the BTC PAC and NCDC with a compliance report highlighting any discrepancies.

8.5. Actions Taken as A Result of Deficiency

If irregularities are found by the auditor, the audited party shall be informed in writing of the findings. The audited party must submit a report to the auditor or directly to NCDC or BTC PAC, as determined, as to any remedial action the audited party will take in response to the identified deficiencies. This report shall include a time for completion to be approved by the auditor or by NCDC in conjunction with BTC LICENSED CA, as appropriate.

Where an audited party fails to take remedial action in response to the identified deficiencies, NCDC shall be informed by the auditor and shall take the appropriate action, according to the severity of the deficiencies.

8.6. Communication of Results

An Audit Compliance Report, including identification of corrective measures taken or being taken by the audited party, shall be provided to the BTC PAC and/or NCDC as applicable.

The BTC LICENSED CA shall make the Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, an explanatory letter is to be signed by the Qualified Auditor.

9. Other Business and Legal Matters

9.1. Fees

9.1.1. Certificate Issuance/Renewal Fee

Currently, no fees are charged by BTC LICENSED CA for Digital Certificates, although BTC LICENSED CA reserves the right to change this in the future.

9.1.2. Certificate Access Fees

No fees are charged by BTC LICENSED CA, but BTC LICENSED CA may charge access fee for providing access to its repository, for certain use-cases, at the sole discretion of BTC LICENSED CA.

9.1.3. Revocation or Status Information Access Fee

No fee will be charged by BTC LICENSED CA for revocation of a certificate. Further no fee will be charged for a relying party to check the validity of the existing certificate using a CRL.

BTC LICENSED CA reserves the right to charge a fee for providing certificate status information through OCSP.

9.1.4. Fees for Other Services

BTC LICENSED CA may charge for the services including online signature service, timestamping and/or any other additional services depending on business needs.

9.1.5. Refund Policy

Refunds are not possible for the Digital Certificates for which no fees are charged.

9.2. Financial Responsibility

BTC LICENSED CA disclaims all liability implicit or explicit due to the use of any certificates issued by the BTC LICENSED CA which certify public keys of CAs.

9.2.1. Insurance Coverage

Insurance coverage for any CA shall be in accordance with the applicable Agreement between the contracting party and the CA.

9.2.2. Other Assets

BTC LICENSED CA shall have sufficient financial resources to maintain their operations and perform their duties.

9.2.3. Insurance/warranty Coverage for End-Entities

BTC LICENSED CA disclaims all liability implicit or explicit due to the use of any certificates issued by the BTC LICENSED CA, which only certifies public keys of CAs. It is the sole responsibility of subscribers and relying parties to ensure an adequate insurance, to cover risks using the certificate or rendering respective services.

9.3. Confidentiality of Business Information

Information pertaining to the BTC LICENSED CA and not requiring protection may be made publicly available at the discretion of BTC PAC. Specific confidentiality requirements for business information are defined in BTC LICENSED CA Privacy Policy and the applicable Agreements.

9.3.1. Scope of Confidential Information

Any corporate or personal information held by BTC LICENSED CA, CSPs related to the application and issuance of Certificates is considered confidential and will not be released without the prior consent of the relevant holder, unless otherwise required by law or to fulfil the requirements of this CP/CPS, and in accordance with BTC LICENSED CA Privacy policy. BTC LICENSED CA Document Control Policy specifies which documents are considered to be confidential. Information contained in certificates and related certificate status is not confidential.

A. Registration Information

All registration records are considered to be confidential information, including;

- Certificate applications, whether approved or not;
- Certificate information collected as part of the registration process;
- Completed Subscriber Agreements;
- Any information or supporting documentation requested and/or received by the BTC LICENSED CA pertaining to a certificate application.

B. Certificate Information

The reasons for a certificate being suspended or revoked is considered confidential information, with the sole exception of the revocation of the BTC LICENSED CA, Level-2 CAs due to;

- The compromise of their private key, in which case a disclosure may be made that the private key has been compromised;
- The termination of the BTC LICENSED CA or Level-2 CAs, in which case prior disclosure of the termination may be given.

C. PKI Documentation

BTC PKI Document Control Policy specifies which documents are considered to be confidential.

9.3.2. Information not within the Scope of Confidential Information

Such information as specified by the BTC PAC, BTC LICENSED CA Privacy Policy, BTC LICENSED CA Document Control Policy, BTC LICENSED CA Operations Policies and procedures and applicable Agreements.

9.3.3. Responsibility to Protect Confidential Information

All PKI participants shall be responsible for protecting the confidential information they possess in accordance with BTC LICENSED CA Privacy Policy and applicable laws and Agreements.

9.4. Privacy of Personal Information

Any personal identifying information collected by BTC LICENSED CA shall be protected in accordance with BTC LICENSED CA Privacy Policy. It shall use reasonable measures to protect personal identifying information from disclosure to any third party.

9.4.1. Privacy Plan

Any confidential information collected by BTC LICENSED CA shall be protected in accordance with BTC LICENSED CA Privacy Policy.

9.4.2. Information Treated as Private

Any information that is not publicly available through the content of the issued certificate, repository and online CRL's is treated as private.

9.4.3. Information not Deemed Private

Information appearing in issued Certificates such as the name, organization affiliation and pubic key will not be deemed private.

9.4.4. Responsibility to Protect Private Information

Access to BTC LICENSED CA held private information shall be restricted to those with an official need-to-know basis in order to perform their official duties.

9.4.5. Notice and Consent to Use Private Information

Requirements for notice and consent to use private information are defined in the respective Agreements and BTC LICENSED CA Privacy Policy.

9.4.6. Disclosure Pursuant to Judicial/Administrative Process

Any disclosure shall be handled in accordance with BTC LICENSED CA Privacy Policy.

9.4.7. Other Information Disclosure Circumstances

Any disclosure shall be handled in accordance with BTC LICENSED CA Privacy Policy.

9.5. Intellectual Property Rights

BTC PAC retains exclusive rights to any products or information developed under or pursuant to this CP/CPS.

9.6. Representations and Warranties

9.6.1. BTC LICENSED CA's Representations and Warranties

BTC LICENSED CA provides representations and warranties in accordance with this CP/CPS, respective agreements and applicable laws and regulations as below:

- Providing the operational infrastructure and certification services;
- Making reasonable efforts to ensure it conducts an efficient and trustworthy operation. "Reasonable efforts" include but are not limited to operating in compliance with:
  - Documented CP/CPS and PDS;
  - Documented BTC LICENSED CA Operations Policies and Procedures; and
  - Within applicable agreements, Saudi Law and regulations.
- At the time of Certificate issuance; BTC LICENSED CA implemented procedure for verifying accuracy of the information contained within it before installation and first use;
- Implemented a procedure for reducing the likelihood that the information contained in the Certificate is not misleading;
- Maintaining 24 x 7 publicly-accessible repositories with current information and replicates BTC LICENSED CA issued CA certificates and CRLs;
- For the CA's, the Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the CA keys and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key CA private key is generated using multi-person control "m-of-n" split key knowledge scheme;
- Backing up of the CA signing Private Key is under the same multi-person control as the original Signing Key;
- Keep confidential, any passwords, PINs or other personal secrets used in obtaining authenticated access to PKI facilities and maintain proper control procedures for all such personal secrets;
- Use its private signing key only to sign certificates and CRLs and for no other purpose;
- Perform authentication and identification procedures in accordance with applicable Agreement and BTC LICENSED CA Operations Policies and Procedures;
- Provide certificate and key management services in accordance with the CP and CPS; and
- Ensure that CA personnel use private keys issued for the purpose of conducting CA duties only for such purposes.

9.6.2. RA Representations and Warranties

RA's discharge their obligations in accordance with the practices outlined in overview of this CP/CPS and the RA Agreement.

9.6.3. Relying Parties Representations and Warranties

Relying Parties who rely upon the certificates issued under BTC LICENSED CA shall:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Verify the Validity by ensuring that the Certificate was valid at the time of signing;
- Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 amendment;
- Ensure that the Certificate has not been suspended or revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon; and
- Determining that such Certificate provides adequate assurances for its intended use.

9.6.4. Subscriber Representations and Warranties

Subscribers are Individuals, entities, non-human subscribers (like Servers and Network Devices) to which certificates are issued, and are legally bound by a subscriber agreement or terms of use.

It is the responsibility of the Subscriber to:

1. Subscriber is obligated to:

- Provide accurate and complete information at all times to the RA, both in the certificate request and verification process defined by the RA;
- Review and verify provided information for accuracy and completeness;
- Secure authentication and consent mechanisms for certificate requests and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, Mobile Phone for OTP, or other activation data that is used to control access to the Subscriber's private key;
- Use Subscriber Certificate only for its intended use;
- Notify the CA/RA in the event of any information in the Certificate is, or becomes, incorrect or inaccurate;
- Notify the CA/RA in the event of a key compromise immediately whenever the Subscriber has reason to believe that the Subscriber's private key has been lost, accessed by another individual, or compromised in any other manner;
- Use the Subscriber Certificate that does not violate applicable laws in the Kingdom of Saudi Arabia; and
- Upon termination of Subscriber Agreement, revocation or expiration of the Subscriber Certificate, immediately cease use of the Subscriber Certificate.

2. Subscriber agrees that any use of the Subscriber Certificate to sign or otherwise approve the contents of any electronic record or message is attributable to Subscriber. Subscriber agrees to be legally bound by the contents of any such electronic record or message.

3. Subscriber shall indemnify and hold BTC LICENSED CA harmless from and against any and all damages (including legal fees), losses, lawsuits, claims or actions arising out of:

- Use of Subscriber's Certificate in a manner not authorized by the CA/RA/SIP or otherwise inconsistent with the terms of this Subscriber Agreement or the BTC LICENSED CA CP/CPS;
- A Subscriber Certificate being tampered with by the Subscriber; or
- Inaccuracies or misrepresentations contained within the Application. A Subscriber shall indemnify and hold the BTC LICENSED CA harmless against any damages and legal fees that arise out of lawsuits, claims or actions by third parties who rely on or otherwise use Subscriber's Certificate, where such lawsuit, claim, or action relates to a Subscriber's breach of its obligations outlined in this Subscriber Agreement or the BTC LICENSED CA CP/CPS, a Subscriber's use of or reliance upon a Subscriber Certificate in connection with its business operations, a Subscriber's failure to protect its private key, a Subscriber's failure to protect its authentication material or devices, or claims pertaining to content or other information or data supplied, or required to be supplied, by Subscriber.

9.7. Disclaimers of Warranties

BTC LICENSED CA hereby disclaims all warranties including warranty on merchantability and /or fitness to a particular purpose other than to the extent prohibited by law or otherwise expressly provided in BTC LICENSED CA CP/CPS.

BTC LICENSED CA, through its associated components, seeks to provide digital certification services according to international standards and best practices, using secure physical and electronic installations.

The BTC LICENSED CA provides no warranty, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of the BTC LICENSED CA or for the legal validity, acceptance or any other type of recognition of its own certificates, those issued by it through other Subordinate entity, any digital signature backed by such certificates, and any products/solutions/services provided by BTC LICENSED CA. BTC LICENSED CA further disclaims any warranty of merchantability or fitness for a particular purpose of the above-mentioned certificates, digital signatures and products/solutions/services.

9.8. Limitations of Liability

BTC Licensed CA disclaims liability to the certificate beneficiaries or any other third-parties for any loss suffered as a result of use or reliance on a certificate beyond those specified in BTC Licensed CA CP/CPS, when such certificate has been issued and managed by BTC Licenses CA in compliance with this CP/CPS. In any other case:

- BTC LICENSED CA will not incur any liability to Subscribers or any person to the extent that such liability results from their negligence, fraud or willful misconduct;
- BTC LICENSED CA assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under this policy for any use other than in accordance with this policy. Subscribers will immediately indemnify BTC LICENSED CA from and against any such liability and costs and claims arising therefrom;
- BTC LICENSED CA will not be liable to any party whosoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services;

- End-Users are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by BTC LICENSED CA;
- Subscribers to compensate a Relying Party which incurs a loss as a result of the Subscriber's breach of Subscriber agreement;
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations;
- Registration Authorities shall bear the consequences of their failure to perform the Registration Authorities obligations described in the Registration Authorities agreement and
- BTC LICENSED CA denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

9.9. Indemnities

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, BTC LICENSED CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the BTC LICENSED CA under these requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, BTC LICENSED CA shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by BTC LICENSED CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the BTC LICENSED CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.1. Indemnification by Subscribers

Any subscriber of BTC LICENSED CA or its subordinates, shall indemnify and hold harmless BTC LICENSED CA, its directors, its partners, its employees, any trusted root entities and their respective directors, officers, employees, agents, and contractors from any and all damages and losses arising out of

- use of the Certificate in a manner not authorized by BTC LICENSED CA;
- tampering with the Certificate; or
- misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional.

In addition, Subscribers shall indemnify and hold harmless BTC LICENSED CA from any and all damages (including legal fees) for lawsuits, claims or actions by third-parties relying on or otherwise using the Certificate relating to:

- Subscriber's breach of their obligations under the Subscriber Agreement or BTC LICENSED CA CP/CPS;
- Subscriber's failure to protect its private key; or

- Claims (including without limitation infringement claims) pertaining to content or other information or data supplied by Certificate Holder.

9.9.2. Indemnification by Relying Parties

Any relying party of a certificate issued by BTC LICENSED CA or its subordinate, shall indemnify and hold harmless BTC LICENSED CA, its directors, its partners, any trusted root entities and their respective directors, officers, employees, agents, and contractors from any and all damages and losses arising out of:

- breach of the Relying Party Agreement, BTC LICENSED CA CP/CPS, or applicable law;
- unreasonable reliance on a Certificate;
- failure to check the Certificate's status prior to use.
- use of the Certificate in a manner not authorized by BTC LICENSED CA;
- tampering with the Certificate; or
- misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional.

9.10. Term and Termination

9.10.1. Term

This CP/CPS shall be effective upon approval by BTC PAC in liaison with approval by NCDC. Once the CP/CPS becomes effective it is published in the repository. Amendments to this CP/CPS upon approval become effective and replace the older version in the repository.

9.10.2. Termination

This CP/CPS as amended from time to time shall remain in force until it is replaced by a new version. The latest version of the BTC LICENSED CA CP/CPS can be found at: https://www.emdha.sa

9.10.3. Effect of Termination and Survival

Upon termination of this CP/CPS, all BTC LICENSED CA participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11. Individual Notices and Communications with Participants

All communication between NCDC, BTC PAC, Saudi National Root-CA, BTC LICENSED CA and RAs shall be in writing or via digitally signed communication. If in writing, the communication shall be signed on the appropriate organization letterhead. If electronically, a Digital Signature shall be made using a Private Key whose companion Public Key is certified using a Certificate meeting a high assurance level.

9.12. Amendments

9.12.1. Procedure for Amendment

The BTC PAC shall review this CP/CPS at least once per year. Errors, updates, or suggested changes to this CP/CPS shall be communicated to the BTC PAC. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change. Any technical changes in the BTC LICENSED CA shall be managed as per the BTC LICENSED CA Change Management Policy.

Subject to the approval of NCDC, the BTC PAC reserves the right to change this CP/CPS from time to time. The BTC PAC will incorporate any such change into a new version of this CP/CPS and, upon approval, publish the new version. The new CP/CPS will carry a new version number.

9.12.2. Notification Mechanism and Period

This CP/CPS and any subsequent changes shall be made available to the BTC LICENSED CA participants at: https://www.emdha.sa within two weeks of approval. The BTC PAC reserves the right to amend this CP/CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URL's, and changes to contact information. All the PKI participants and other parties designated by the BTC PAC shall provide their comments to the BTC PAC in accordance with NCDC rules. The BTC PAC's decision to designate amendments as material or non-material shall be at the PAC's sole discretion.

9.12.3. Circumstances under which OID must be changed

The policy OID shall only change if the change in the CP/CPS results in a material change to the trust by the relying parties, as determined by the BTC PAC and shall only change pursuant to a decision from NCDC.

9.13. Dispute Resolution Procedures

The use of certificates issued by the BTC LICENSED CA is governed by contracts, agreements, and standards set forth by BTC LICENSED CA. Those contracts, agreements and standards include dispute resolution policy and procedures that shall be employed in any dispute arising from the issuance or use of a certificate governed by this CP/CPS. Dispute Resolution mechanism is described in BTC LICENSED CA Dispute Resolution Policy.

9.14. Governing Law

This CP/CPS is governed by the laws of the Kingdom of Saudi Arabia.

9.15. Compliance with Applicable Law

This CP/CPS is subject to applicable national, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

In the event that any one or more of the provisions contained in this CP/CPS shall for any reason be held to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability shall not affect any other provision of this CP/CPS, which shall be construed as of such invalid, illegal or unenforceable provision had never been set forth herein, and the CP/CPS shall be enforced as nearly as possible according to its original terms and intent.

9.16.2. Assignment

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

9.16.3. Severability

Should it be determined that one section of this CP/CPS is incorrect or invalid, the other sections of this CP/CPS shall remain in effect until the CP/CPS is updated. The process for updating this CP/CPS is described in section 9.12.

9.16.4. Enforcement (Attorney Fees/Waiver of Rights)

This document shall be treated according to laws of Kingdom of Saudi Arabia. Legal disputes arising from the operation of the BTC LICENSED CA will be treated according to laws of Kingdom of Saudi Arabia.

9.16.5. Force Majeure

The BTC LICENSED CA shall not be liable for any failure or delay in its performance under this CP/CPS due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and reasons beyond provisions of the governing law.

9.17. Other Provisions

9.17.1. Fiduciary Relationships

Nothing contained in this CP/PCS shall be deemed to constitute either the BTC LICENSED CA, or any of its subcontractors, agents, officers, suppliers, employees, partners, principals, or directors to be a partner, Affiliate, trustee, of any Relying Party or any third party, or to create any fiduciary relationship between the BTC LICENSED CA and any Relying party, or any third party, for any purpose whatsoever.

Nothing in this CP/CPS or any Agreement between a third party and a Relying Party shall confer on any Subscriber, Customer, Relying Party, Registration Authority, Applicant or any third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of the BTC LICENSED CA.

9.17.2. Administrative Processes

No Stipulation

Appendix- A: Type of Certificates

This section details different certificate types issued under the BTC LICENSED CA and their respective policies and certificate profiles.

For issuance of a particular certificate type, Issuing CA shall submit request to BTC LICENSED CA. Based on BTC LICENSED CA approval and NCDC Approval, RA(s) are authorized to issue particular certificate type. It is mandatory to comply with all requirements applicable to the respective certificate type, as well as, any additional restrictions or conditions communicated to the RA by BTC LICENSED CA.

Refer to table "Certificate Types" in Section 1.2 for the type of certificates issued by BTC LICENSED CA, with detailed information in subsequent sections.

1. Level-2 Issuing eSign CA

Level-2 Issuing eSign CA will be issued as per the process defined in Level-2 Issuing CA Manual. Level-2 Issuing CAs shall have the following certificate extensions:

1.1. Extension Definitions for Level-2 Issuing eSign CA

Field / x.509 extension	Value or Value Constant	Critical

Subject	CN = EMDHA eSign CA
	O = Baud Telecom Company
	C = SA
		V1 Field

Serial Number	Unique serial number with minimum 64-bit entropy	V1 Field

CRL Distribution Points	`[1] CRL Distribution Point`
	`Distribution Point Name:`
	`Full Name:`
	`URL=http://repository.emdha.sa/crls/L1CA19.crl`
		NO

Authority Key Identifier	<Same as the SubjectKeyIdentifier of the BTC Licensed CA>	NO
Subject Key Identifier	key Identifier encoded in compliance to RFC 5280 The key Identifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Level-2 CA (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=CA Path Length Constraint=None	YES

Authority Information Access	`[1]Authority Info Access`
	`Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)`
	`Alternative Name:`
		NO

	URL=http://ocsp.emdha.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repository.emdha.sa/cacerts/L1CA19.crt	
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.emdha.sa [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= BTC LICENSED CA Certification Policy and associated documentation available at https://www.emdha.sa/ is hereby incorporated into your use or reliance on this Certificate.	NO
Key Usage	Certificate Signing; CRL Signing	YES

2. Level-2 Issuing DSC (Digital Signature Certificate) CA

Level-2 Issuing DSC CA will be issued as per the process defined in Level-2 Issuing CA Manual. Level-2 Issuing CAs shall have the following certificate extensions:

2.1. Extension Definitions for Level-2 Issuing DSC CA

Field / x.509 extension	Value or Value Constant	Critical

Subject	CN = EMDHA DSC CA
	O = Baud Telecom Company
	C = SA
		V1 Field

Serial Number	Unique serial number with minimum 64-bit entropy	V1 Field
CRL Distribution Points	[1] CRL Distribution Point Distribution Point Name: Full Name: URL=http://repository.emdha.sa/crls/L1CA19.crl	NO
Authority Key Identifier	<Same as the SubjectKeyIdentifier of the BTC Licensed CA>	NO
Subject Key Identifier	key Identifier encoded in compliance to RFC 5280 The key Identifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Level-2 CA (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=CA Path Length Constraint=None	YES
Authority Information Access	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.emdha.sa [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://repository.emdha.sa/cacerts/L1CA19.crt	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.emdha.sa [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= BTC LICENSED CA Certification Policy and associated documentation	NO

	available at https://www.emdha.sa/ is hereby incorporated into your use or reliance on this Certificate.	
Key Usage	Certificate Signing; CRL Signing	YES

3. Level-2 Issuing TSA (TimeStamping Authority) CA

Level-2 Issuing TSA CA will be issued as per the process defined in Level-2 Issuing CA Manual. Level-2 Issuing CAs shall have the following certificate extensions:

3.1. Extension Definitions for Level-2 Issuing TSA CA

Field / x.509 extension	Value or Value Constant	Critical

Subject	CN = EMDHA TSA CA
	O = Baud Telecom Company
	C = SA
		V1 Field

Serial Number	Unique serial number with minimum 64-bit entropy	V1 Field

CRL Distribution Points	`[1] CRL Distribution Point`
	`Distribution Point Name:`
	`Full Name:`
	`URL=http://repository.emdha.sa/crls/L1CA19.crl`
		NO

Authority Key Identifier	<Same as the SubjectKeyIdentifier of the BTC Licensed CA>	NO
Subject Key Identifier	key Identifier encoded in compliance to RFC 5280 The key Identifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the Level-2 CA (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=CA Path Length Constraint=None	YES

Authority Information Access	`[1]Authority Info Access`
	`Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1)`
	`Alternative Name:`
	`URL=http://ocsp.emdha.sa`
	`[2]Authority Info Access`
	`Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)`
	`Alternative Name:`
	`URL=http://repository.emdha.sa/cacerts/L1CA19.crt`
		NO

Certificate Policies	`[1]Certificate Policy:`
	`Policy Identifier=All issuance policies`
	`[1,1]Policy Qualifier Info:`
	`Policy Qualifier Id=CPS`
	`Qualifier:`
	`http://www.emdha.sa`
	`[1,2]Policy Qualifier Info:`
	`Policy Qualifier Id=User Notice`
	`Qualifier:`
	`Notice Text= BTC LICENSED CA Certification Policy and associated documentation`
		NO

	available at https://www.emdha.sa/ is hereby incorporated into your use or reliance on this Certificate.	
Key Usage	Certificate Signing; CRL Signing	YES
Extended Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)	NO