banqup

Certificate Policy and Practice Statement (CP/CPS)

v.1.1

We ensure compliance

and business growth

www.banqup.com

1. Document History

1.1. Version History

Version	Date	Status	Description
1.01	11/08/2025	Draft	Initial version of the CP/ CPS
1.02	25/09/2025	Draft	Minor updates made in preparation for trust services certification by the conformity assessment body.
1.1	30/01/2026	Final	Section 8.7 was updated to ensure compliance with Commission Implementing Regulation (EU) 2025/2530.

1.2. Document Approval

Version	Date	Status	Approved by
1.1	02/02/2026	Approved	TSP Authority

1.3. Related Documents

Document	Relation
Solution Specific Terms for QES and QSeal Services	Establish the contractual terms applicable to customers for the provision of trust services, and are aligned with and subordinate to the Certification Policy and CPS.

Table of Contents

1 Introduction

This document is the Banqup CA (BQCA) *Certificate Policy and Certification Practice Statement* ("CP/CPS") for certificates delivered and qualified according to the eIDAS regulation. It describes the practices that BQCA, as a Trusted Service Provider (TSP), employs in providing certification services for qualified certificates for qualified electronic signatures and qualified certificates for qualified electronic seals.

It also establishes the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing certificates and providing associated trust services. It describes the practices that BQCA employs for:

- Securely managing the related infrastructure that supports BQCA's PKI, and
- Issuing, maintenance and life-cycle management of qualified certificates

This CP/CPS conforms to the *Internet Engineering Task Force (IETF) RFC 3647 for certificate Policy and Certification Practice Statement* construction.

The CA implements the services described in this CP/CPS in a non-discriminatory manner within the limits of what current technologies allow.

This CP/CPS is also a certificate policy (CP) as a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements."

This CP/CPS covers the issuance and controls surrounding the following types of certificates:

- **qualified Signing certificates for natural persons** – to produce qualified electronic signatures with a legal effect equivalent to a handwritten signature on electronic transactions and documents.
- **qualified Signing certificates for Legal Persons (eSeal certificates)** – certificates used to apply eSeals on documents issued by an entity (legal person) to confirm the identity of the document issuer, the origin and integrity of the data source in these documents.
- **OCSP Responder certificates** – certificates for the Online certificate Status Protocol (OCSP) responder to sign OCSP responses related to certificates issued by the CAs.
- **CA certificates** – certificates for the root, intermediates and issuing CA of the PKI.

This CP/CPS practices and procedures are compliant with:

- **ETSI EN 319 411-2** Policies:
    - QCP-n / QCP-n-qscd for qualified certificates for qualified electronic signatures; and
    - QCP-l / QCP-l-qscd for qualified certificates for qualified electronic seals,
- **ETSI EN 319 411-1** Policies:
    - Normalized certificate Policy (NCP)
    - extended Normalized certificate Policy (NCP+)
- **ETSI EN 319 401** (General Policy Requirements for Trust Service Providers)
- **ETSI EN 319 412-1** (certificate Profiles; Part 1: Overview and common data structures)
- **ETSI EN 319 412-2** (certificate Profiles; Part 2: certificate profile for certificates issued to natural persons)

- **ETSI EN 319 412-3** (certificate Profiles; Part 3: certificate profile for certificates issued to legal persons)
- **ETSI EN 319 412-5** (certificate Profiles; Part 5: QcStatements)

The CP/CPS is a public document and is published in the BQCA public repository.

1.1 Overview

Banqup is the organization that owns and operates BQCA PKI hierarchy.

As such Banqup operates as a qualified trust services provider (QTSP) offering qualified and non-qualified trust services through a hierarchy of CAs.

1.1.1 Banqup CA Policy Management Authority

The entity that governs the PKI is referred to as the Banqup CA Policy Management Authority (TSP authority). The TSP authority comprises the necessary functions including policy, compliance, legal and architecture that are required to provide strategic direction and continuously supervise the PKI operations.

The TSP authority is consists at least of:

- The TSP manager
- A representative from Banqup's board
- A representative from the IT security team

The TSP authority is the highest-level management body with final authority and responsibility to:

- Maintain compliance with the legal and normative requirements,
- Define the PKI services and approve its delivery model,
- Define, maintain and approve the PKI policies and practices,
- Conduct regular supervision activities on the PKI operations team,
- Approve PKI budget, and take major commercial decisions,
- Approve major changes on the PKI infrastructure,
- Approve key ceremonies, and allocate internal/external auditors as required,
- Get involved in major incidents, when applicable.

1.2 Document's name and identification

This document can be identified through its title and version number.

The certificate policies used for qualified end-user certificates are identified by their CertificatePolicies attributes, which use the following ETSI object identifier values:

- **QCP-n-qscd**: certificate policy for EU qualified certificates issued to natural persons with private key related to the certified public key in a QSCD; `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)`

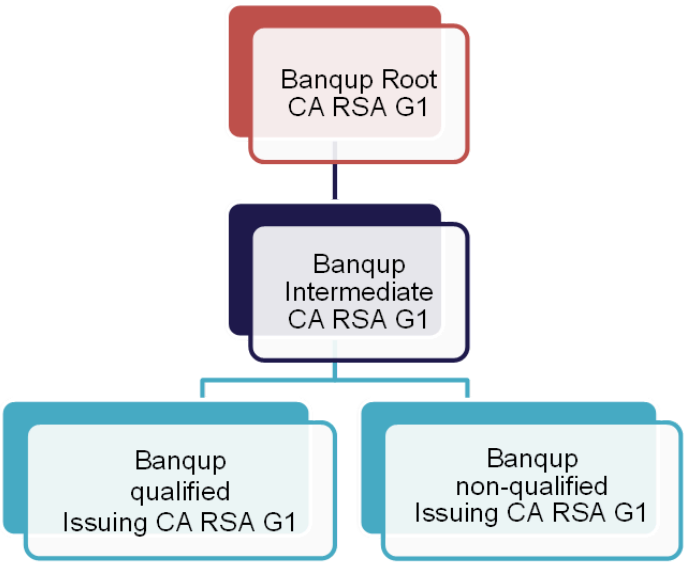
- **QCP-l-qscd:** certificate policy for EU qualified certificates issued to legal persons with private key related to the certified public key in a QSCD; `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3)`

The applicable and current CP/CPS (OID) shall be inserted by reference within each end-user certificate ruled by the present BQCA CP/CPS.

1.3 PKI Participants

1.3.1 Certification Authorities

BQCA as a QTSP offering qualified trust services uses a three-level PKI hierarchy that consists of a Root CA, an intermediate CA and issuing CAs as follow:



1.3.2 Registration Authorities

1.3.2.1 BQCA RA

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

Duly authorized members of BQCA PKI team and systems act as Registration Authority (hereinafter BQCA RA) for the PKI.

Identity validation of the natural persons can be performed by external organisations under contract (which can have their own subcontractors):

- by Signicat as Identification Service/Method Provider (ISP) using its eIDAS-certified (acc. to Art. 24, paragraph 1a) identification methods.
- IDnow as Identification Service/Method Provider (ISP) using its eIDAS-certified (acc. to Art. 24, paragraph 1a) identification methods.
- Electronic identification means providers (notified at eIDAS level high).

Identification of legal persons is performed through (automated) retrieval of company information in the applicable national trade register.

1.3.3 Subscribers

The Subscribers of the PKI services are either:

- Natural persons identified as private persons;
- Natural persons identified as natural persons entitled to represent a legal person (i.e., self-employed, employee), or
- Legal Persons.

Before issuing any certificate, the subscriber shall agree to the BQCA subscribers' agreement.

1.3.4 Relying Parties

Relying Parties are entities including physical or legal persons who rely on a certificate and/or a security operation verifiable with reference to a public key listed in a certificate. Prior to relying on electronic certificates for security operations, Relying Parties must always ensure:

- The validity of the certificate with regards to algorithms and procedures defined in **RFC 5280**.
- The validity of the certificate through CA certificate revocation status services
- The context in which the certificate is used against the OID's of the certificates.

Relying parties shall also comply with the relying parties obligations and liabilities as stated in the relevant sections of the present CP/CPS.

1.3.5 Other Participants

Other Participants include:

- **Accreditation or Supervisory body:** The Supervisory Body will be the corresponding management body that admits, accredits and supervises the TSPs within a specific geographical area.
- **The TSP authority**, which is responsible for amendments to this CP/CPS.

1.4 Certificate usage

1.4.1 Appropriate certificate usage

1.4.1.1 CA certificates

The CA certificates shall be solely used for verifying the certificates issued by the CA, the lists of the certificates revoked by the CA (CARL's or CRL's), and the OCSP responses released by the CA's OCSP responder (if applicable).

1.4.1.2 Certificates issued for electronic signatures

These certificates are used to produce qualified electronic signatures on documents and e-transactions. These certificates are issued only to the individuals whose identity are vetted through in-person meetings or equivalent by the relevant Registration Authority.

These certificates are compliant with QCP-n-qscd specification. Certificates issued under these requirements are aimed to support qualified electronic signatures with the use of a "Qualified Signature Creation Device" (QSignCD).

1.4.1.3 Certificates issued for electronic seals

Qualified certificates for electronic seal are normally used to ensure the integrity and the origin of that data to which it is linked, or for other purposes, provided that the usage is not otherwise prohibited by law, by this CP/CPS and any agreements with Subscribers.

Certificates are compliant with QCP-l-qscd. Certificates issued under these requirements are aimed to support qualified electronic seals with the use of a “Qualified Seal Creation Device” (QSealCD).

1.4.1.4 Certificates issued to ocsp responders

These are used to sign the Online certificate Status Protocol (OCSP) responses.

1.4.2 Prohibited certificate usage

Certificates referred to in this CP/CPS document shall not be used for purposes other than the ones listed above.

1.5 Policy administration

1.5.1 Organization administering the document

BQCA, through the Banqup CA Policy Management Authority, is bearing responsibility for drafting, publishing, OID registration, maintenance and interpretation of this CP/CPS, and other policies and practices within the domain of the PKI.

The TSP authority is comprised of members with relevant PKI policy experience and appointed to conduct the following PKI policy administration tasks:

- Drafting, amending, maintaining and interpreting this CP/CPS.
- Approve and publish this CP/CPS and its updates after the completion of a review process. The updated CP/CPS is published on the CA’s website as promptly as possible and, in any case, no later than its effective date (as indicated on the first page).

1.5.2 Contact person

TSP authority may be contacted at the following addresses:

Email: qtsp@banqup.com

- Postal address: Banqup, Av. Reine Astrid 92A, 1310 La Hulpe, Belgium

The TSP authority accepts comments regarding this CP/CPS only when they are addressed to the contact above.

1.5.3 Person determining cps suitability for the policy

The TSP authority is responsible for determining the suitability and applicability of this CP/CPS.

1.5.4 CPs approval procedures

The TSP authority formally approves any new version of this CP/CPS.

1.6 Definitions and acronyms

BCA	Banqup CA
BCA PMA	Banqup CA Policy Management Authority
CA	Certification Authority
CP	certificate Policy
CPS	Certification Practice Statement
CRL	certificate Revocation List
CSR	certificate Signing Request
DN	Distinguished Name
DNS	Domain Name System
FIPS	Federal Information Processing Standards
EID	Electronic Identity Card
EIDAS	Electronic IDentification, Authentication and trust Services
ETSI	European Telecommunications Standards Institute
GCP	Google Cloud Platform
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IPSEC	Internet Protocol Security
ISO	International Standards Organization
IT	Information Technology
NCP	Normalized certificate Policy
NCP+	Extended Normalized certificate Policy
OCSP	Online certificate Status Protocol
OID	Object Identifier
PIN	Personal Information Number
PKCS#1	Public Key Cryptography Standards (PKCS) #1
PKCS#7	Cryptographic Message Syntax

PKCS#10	Certification Request Syntax Specification
PKI	Public Key Infrastructure
QSCD	qualified Electronic Signature/Seal Creation Device
RA	Registration Authority
RSA	Rivest-Shamir-Adleman (The names of the inventors of the RSA algorithm)
RTO	Recovery Time Objective
SIC	Signer’s interaction component (EN 419241-1)
SSL	Secure Sockets Layer
TLD	top-level domain
TSA	Timestamping Authority
TLS	Transport Layer Security
TSP	Trust Service Provider
URI	Universal Resource Identifier, a URL, FTP address, email address, etc.
URL	Universal Resource Locator

2 Publication and repository responsibilities

2.1 Repositories

BQCA set up and operates an online publicly accessible repository, available at https://www.pki.banqup.com/repository/.

This repository is accessible 24×7 and ensures uptime for at least 99,6% over the course of one year.

2.2 Publication of certification information

BQCA makes the following information available on its public repository:

- Overview of the certification hierarchy
- Certificate Policies
- Certification Practice Statement
- Conformity Assessment Body attestation letter
- CA certificates, including Root CA and Subordinate CAs
- Solution Specific Terms and Conditions for use of qualified Trust Services
- Certificate Revocation Lists and OCSP certificates
- Privacy Policies

The PKI publishes electronic certificate status information in intervals indicated in this CP/CPS. The provision of PKI issued electronic certificate validity status information is a 24×7×365 service:

- The PKI publishes CRLs including any changes since the publication of the previous CRL, at regular intervals. The PKI adds a pointer (URL) to the relevant CRL to Subscribers' certificates as part of the CDP extension whenever this extension is present,
- The PKI maintains an OCSP responder compliant with **RFC 6960**. OCSP information is available immediately to relying party applications. The actual OCSP URL to be queried by relying party organizations is referenced in the certificates issued by the PKI.

2.2.1 Publication and notification policies

This CP/CPS is published in BQCA's public information repository. BQCA CP/CPS along with the enforcement dates is published no less than 30 days prior taking effect.

2.3 Time or frequency of publication

The TSP authority ensures that the CP/CPS of the PKI is reviewed at least annually.

2.4 Access controls on repositories

Read-only access is given to the PKI public repository. Security controls are implemented on the repository by the PKI operations team to prevent any unauthorized addition, or modification of the data published on the public repository.

3 Identification and authentication

3.1 Naming

Naming in certificates is as specified in *Recommendation ITU-T X.509* or *IETF RFC 5280* and the applicable part of *ETSI EN 319 412*.

3.1.1 Name encoding

The PKI issues certificates with name forms compliant to *ETSI EN 319 412-2* for certificates issued to natural persons and *ETSI EN 319 412-3* for certificates issued to legal persons.

3.1.2 Types of names

3.1.2.1 Subject information - subscriber certificates

The applicable subject information for natural person and legal person certificates is specified in the table below.

The PKI issues qualified certificates to natural persons where the contents of the Subject DN fields are compliant with their corresponding requirements stated in section 4.2.4 of *ETSI EN 319 412-2*.

The PKI issues qualified certificates to legal persons where the contents of the Subject DN fields are compliant with their corresponding requirements stated in section 4.2.1 of *ETSI EN 319 412-3*.

certificate Type	Subject DN
qualified Signing certificate (natural person)	• `commonName` • `givenName` • `surname` • `serialNumber` • `countryName`
qualified Seal certificate (legal person)	• `commonName` • `organizationName` • `organizationIdentifier` • `countryName`

3.1.2.2 subject information – BQCA CA's certificates

In the CA certificates, `commonName`, `organizationName` ,`organizationIdentifier` (in case of BQCA Issuing CAs) and `countryName` attributes are present and the combination of these contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.

3.1.3 Name constraints

Name constraints extension is not supported.

3.1.4 Need for names to be meaningful

Subscriber certificates contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the certificate.

BQCA CA certificates contain names with commonly understood semantics permitting the determination of the identity of the CA.

3.1.5 Anonymity or pseudonymity of subscribers

The PKI does not support the issuance of anonymous or pseudonymous certificates.

3.1.6 Rules for interpreting various name forms

3.1.7 Uniqueness of names

BQCA ensures that Subject Distinguished Names (DN) of Subscriber are unique within the domain of a specific CA through automated components of the Subscriber enrolment process.

The uniqueness of the *Distinguished Name* for electronic signatures is ensured by the *Serial Number* attribute value in the *Subject* field of the certificate, which contains the subject's ID document's serial number used during his/her registration.

For electronic seals, it is ensured by the *Organizational Identifier* attribute value in the Subject field of the certificate. Format: `NTR`, followed by the 2-character *ISO 3166*-1 country code and hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)), and the identifier from a national trade register (as defined by *ETSI EN 319 412-1*).

3.1.8 Recognition, authentication, and role of trademarks

Certificate applicants are prohibited from using names in their certificate Applications that infringe upon the Intellectual Property Rights of others. BQCA, however, does not verify whether a certificate Applicant has Intellectual Property Rights in the name appearing in a certificate Application or arbitrate, mediate or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark. BQCA is entitled, without liability to any certificate Applicant, to reject or suspend any certificate Application because of such dispute.

The PKI shall have the right to revoke a certificate upon receipt of a properly authenticated order from TSP authority or court of competent jurisdiction requiring the revocation of a certificate or certificates containing a Subject name in dispute.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The key generation process is ensured by this CP/CSP in compliance with the *ETSI EN 319 401*, *ETSI EN 319 411-1* and *ETSI EN 319 411-2* technical standards.

For qualified certificates associated with private keys in a qualified Signature/Seal Creation Device (QSCD), private keys are generated and stored under the control of the certificate holder within a hardware security module that is located in the BQCA's data centre.

BQCA manages the signers/sealers' private key, providing SCAL-2 access control compliant means.

3.2.2 Authentication of organization identity

The organization identity is verified using the applicable national trade registers, which are expected to provide detailed information about the entity, including the entity's legal name, address, and authorized representative's information.

BQCA may require the applicant to submit official entity documentation to confirm the identity of the subject such as corporate charter, government issued tax document, Professional letter (Accountant letter or Legal opinion), or other relevant documents and may conduct a site visit to the entity to verify the entity's address.

PKI RA verifies the association with the legal person certificate subject by ensuring that the information provided in the application form exactly matches the information that appear in the applicable national trade registers.

PKI RA verifies the authority of the authorized representative and the requester in accordance with section 4.2.1

3.2.3 Authentication of individual identity

Evidence of the identity of an Individual is checked against an official ID document in combination with the personal appearance of the Individual. The ID document must contain:

- full name (including surname and given names),
- date and place of birth,
- a serial number or other attributes which may be used to distinguish the person from others with the same name.

It is also permitted to check the identity of the Individual using an eID mean.

There are two scenarios for authentication of Individual identities:

a) Authenticating an Individual who is acting as a "Requester" to apply for a certificate issued to legal person entity (3.2.3.1)

b) Authenticating an Individual who is applying for one the of certificates issued to natural persons (3.2.3.2)

3.2.3.1 Authentication of requester's identity (legal person)

The requester is an organization official representative, or an employee appointed by the entity's authorized representative (i.e., Official representative), who submits certificate management requests to PKI RA.

The legal representative of the company must provide an electronically signed authorisation form to BQCA (Banqup). His signature (more precisely the signature certificate) is used to verify his identity.

The signed form requests a seal certificate for the legal entity and identifies the subject end entity and sources of documents.

3.2.3.2 Authentication of individuals applying for natural person certificates

The subscriber's identity is verified based on:

- A remote identity proofing service, compliant with ETSI 119 461 and implementing additional requirements for identity proofing for EU qualified trust services;
- An authentication using a notified high level eID means

- Physical presence of the subscriber

3.2.4 Unverified subscriber information

All fields constituting the subscriber information written in the certificate are verified by a PKI RA.

3.2.5 Validation of authority

For certificates issued to Legal Persons:

The PKI RA verifies that:

- The legal person certificate applicant (see 3.2.3.1) is listed in authorized representative's information given by the applicable national trade register, or;
- The legal person certificate applicant is appointed by a person listed in authorized representative's information given by the applicable national trade register.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

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

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

3.3.2 Identification and authentication for re-key after revocation

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

3.4 Identification and authentication for revocation request

All requests regarding the revocation of a certificate are, prior to any action being taken, authenticated by checking if they came from an authorized source.

The PKI RA authenticates the revocation request through one of the following methods:

- The revocation request will be signed with the user's device key (SIC's private key). In case of device loss, the user re-authenticates using their username and password, and the Registration Authority (RA) verifies the identity as described in section 1.3.2.
- When performing a revocation request is not possible, the user must send an email to BCA (see section 1.5.2) and will have to prove his identity using identity documents and other personal data (request for investigation).

4 Certificate Life cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

For qualified certificates issued for Legal Persons:

Seal certificate requests are initiated by a legal person representative who signs the request and authorisation form for the entity.

For certificates issued for natural persons issued through RA:

Signing certificate applications must be initiated directly by the applicants themselves through their Banqup mobile application.

4.1.2 Enrolment process and responsibilities

All applicants must agree with the terms of the *Subscriber Agreement*, which contains representations and warranties. and undergo an enrolment process that consists of:

- Completing an application form and providing true and correct information along with all supporting documents required for validation of the information contained in the certificate.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

PKI performs identification and authentication of all required Subscriber information either:

a) by physical presence,

b) by using a method equivalent to physical presence in accordance with section 3.2.

All the activities comprising the certificate application processing (email communication, phone calls, vetting evidence) are stored along with the certificate application.

4.2.2 Approval or rejection of certificate applications

The certificate application is approved only following a successful identification and authentication of all required subscriber information.

4.2.3 Time to process certificate applications

After certificate application approval, the RA generates a certificate request and send it to the CA:

- Immediately for a natural person certificate
- On a document seal request from a sealer designated by the request and authorisation form for a legal person certificate

Certificates are issued within a few minutes after the RA's approval. Certificates may be issued only within a maximum period of 30 days after successful initial identity validation. If this period is exceeded, a new identity validation of the subscriber and subject shall be performed.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA generates the subject key pair in a QSCD.

- For a signing key pair, the subject mobile application, used for creating the request, is associated with the private key as its activation mean, i.e. the user SIC.
- For a sealing key pair, the signed consent, used for creating the request, is associated with the private key as its activation mean.

A certificate is created and issued following the approval of a certificate application by the PKI RA.

The CA validates the format and structure of the CSR, and generates the certificate in accordance to the configured certificate template.

4.3.2 Notification of certificate issuance

The subscriber is informed on his/her mobile app that his/her certificate has been generated.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

When receiving a certificate, the Subscriber is committed to check its content, especially the data correctness and the complementariness of the public key with the private key owned. If the certificate has any faults or mistakes that cannot be accepted, the Subscriber must immediately inform the BQCA and request the certificate's revocation.

The certificate is deemed accepted by the subscriber if no complaints are raised by the subscriber within 5 business days from receiving the certificate or at the first use, whichever event occurs first.

4.4.2 Publication of the certificate by the CA

The PKI do not publish end-user certificates.

CA certificates are published in the PKI repository.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The subscriber uses their private key, only and exclusively, for the intended purpose (in accordance with the provisions in the field of the certificate "keyUsage") and always for legal and authorized purposes in accordance with the common general requirements applicable to this CP/CPS.

The subscriber always is responsible for the use of his/her certificate.

Additionally, the subscriber is obliged to:

- Not tamper with a certificate,
- Protect the private key's activation data from compromise, loss, disclosure within his/her SIC.
- Notify the CA to revoke the certificate immediately if any details in the certificate become invalid, or because of any compromise, loss, disclosure, or otherwise unauthorized use.

4.5.2 Relying party public key and certificate usage

Relying Parties providing services or directly relying on certificates issued in accordance with the applicable CP/CPS must perform the following and assume the responsibility for having performed the following:

- Use software that complies with X.509 standards.
- Successfully perform public key operations as a condition of relying on a certificate, compliant with RFC 5280.
- Validate a certificate by using the CA's certificate Revocation Lists (CRLs) and OCSP in accordance with the certificate path validation procedure.
- Rely on a certificate only for appropriate applications (and context), considering all the limitations on the use of the certificate specified in the certificate, the applicable contractual documents, and the present CP.
- It is reminded that, as part of the conditions for a certificate to be relied upon as an EU Qualified Certificate, the trust anchor for the validation of the certificate shall be as identified in a service digital identifier of an appropriate EU trusted list entry for a QTSP.
- Assent to the terms of the applicable Relying Party Agreement as a condition of relying on a certificate.

4.6 Certificate renewal

Certificate renewal is not allowed under this CP/CPS.

4.7 Certificate re-key

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

Certificate re-key is supported by the CA.

For natural person certificates, the re-key process (including identity validation, certificate issuance and communication to relevant parties) implies the same steps as the initial certificate application.

For legal person certificates, the RA verifies and processes the original registration file whenever a request to seal a document emanates from a sealer designated by the request and authorisation form of the legal person, when no valid certificate is currently active for this company. A full registration process is required 6 years after initial registration. Authorisation could be revoked based on risk and events (changes…) at any time by the company's legal representative.

4.8 Certificate modification

Modification of a certificate is not allowed under this CP/CPS.

4.9 Certificate revocation and suspension

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period. Prior to revoking a certificate, all revocation requests are authenticated as per 3.4

Suspension of a certificate is not allowed under this CP/CPS.

4.9.1 Circumstances for revocation

The CA revokes a certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests the revocation
2. The Subscriber notifies BQCA that the original certificate request was not authorized and does not retroactively grant authorization
3. BQCA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the certificate suffered a key compromise
4. BQCA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the certificate
5. BQCA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement
6. BQCA is made aware that the certificate was not issued in accordance with the present CP/CPS
7. BQCA determines or is made aware that any of the information appearing in the certificate is inaccurate
8. The certificate no longer complies with the requirements of sections 6.1.5 and 6.1.6 of this CP/CPS
9. BQCA obtains evidence that the certificate was misused
10. If a subscriber loses legal eligibility, is declared absent or deceased, or is dissolved or bankrupt
11. Subscriber loses ability to use the local QSCD or mobile device required to access a remote QSCD
12. A final court judgment requires the revocation
13. The private key of the CA has been compromised
14. The supervisory body requests the revocation according to the law.

Once the PKI approves the revocation request, the certificate is permanently revoked and cannot be reinstated.

4.9.2 Who can request revocation

The revocation of certificate can be requested by:

- The CA at its own discretion
- The subscriber to whom certificates were issued
- The supervisory body
- Any relying party possessing evidence of compromise of the subscriber's certificate
- Revocations can be directly initiated by BQCA RA officers

4.9.3 Procedure for revocation request

The subscriber may submit a revocation request through his/her SIC.

- The RA assigns a unique ID to the revocation request. The BQCA RA records the submitted documents under the assigned ID,
- The RA authenticates the Requester's identity and verifies its authorization,
- The RA validates the certificate revocation information,
- The RA execute the certificate revocation,
- The CA revokes the certificate and issues an updated CRL,
- The RA notifies, via email, the subscriber/the entity who requested the revocation, of the completion of the certificate revocation operation.

4.9.4 Revocation request grace period

As soon as the subscriber is aware that one of the circumstances for revocation has occurred, he must request the revocation without delay..

4.9.5 Time within which CA must process the revocation request

A proper certificate revocation request is processed within 24 hours. The maximum delay between a revocation request and either the rejection of the demand or the public availability of the certificate's revocation information is at most 24 hours.

For certificate problem reports, BQCA RA begins investigations within 24 hours, starting from the reception of the report. The RA initiates communication with the Subscriber and, where appropriate, with other concerned authorities (e.g. law enforcement). A preliminary communication on the certificate problem is sent to the Subscriber and to the originator of the problem report.

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

If the investigations results led to one of the certificate revocation circumstances listed above, then the certificate will be revoked.

4.9.6 Revocation checking requirement for relying parties

Before relying on the information contained in a certificate, the Relying Party shall validate the appropriateness of the certificate for the intended purpose and ensure that the certificate is valid. The PKI

makes available to relying parties a status information service for certificates based on the OCSP protocol, and access and download of certificate Revocation Lists (CRLs).

4.9.7 CRL issuance frequency

Issuing CA CRLs are issued every hour and whenever a revocation is approved.

Intermediate CA CARLs are issued whenever a CA certificate is revoked and at least every six months.

Root CA CARLs are issued whenever a CA certificate is revoked and at least annually, and are made available via the Intermediate CA CRL Distribution Point.

4.9.8 Maximum latency for CRL

CRLs are published in a timely manner.

4.9.9 On-line revocation status checking availability

Relying parties will be able to validate the certificates published in PKI Repository by means of a certificate status information service based on the OCSP protocol, or by consulting the CRL and CARL Revocation Lists. Both services are available 24 hours a day, 7 days a week.

The PKI offers an OCSP responder that conforms to *RFC 6960*. The OCSP responder avails information immediately to relying party applications based on the CAs' actions on issued certificates.

The OCSP certificates contain an extension of type `id-pkix-ocsp-nocheck`, as defined by *RFC 6960*.

The actual OCSP URL to be queried by relying party organizations is referenced in the certificates issued by the PKI.

4.9.10 On-line revocation checking requirements

Relying parties need to confirm the status of certificates they want to trust. They can check the status of certificates by referring to the latest certificate Revocation List (CRL and CARL) or via Online certificate Status Protocol (OCSP) query.

The CA maintains revoked and expired certificates in the issued CRL.

The PKI supports an OCSP responder capability using both HTTP GET and HTTP POST methods.

The BQCA issuing CAs update information provided via its OCSP responder immediately when status of an issued certificate is changed.

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

OCSP and CRL should not provide different answers regarding a given certificate. In the event of conflicting information obtained from the OCSP and CRL services regarding the status of a certificate, the information provided by the OCSP must be deemed to be the correct response.

4.9.11 Other forms of revocation advertisements available

PKI does not employ any method other than OCSP and CRL for advertising revocation status.

4.9.12 Special requirements related to key compromise

If a private key is compromised, the corresponding certificate shall immediately be revoked. If the CA's private key is compromised, all certificates issued by that CA shall be revoked.

4.9.13 Circumstances for suspension

Not applicable.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

The PKI publish its CRLs at the public repository accessible to relying parties.

The PKI OCSP responder exposes an HTTP interface that is also publicly available to relying parties.

For the revocation status information of certificates, PKI applies the following:

- PKI maintains the status of the issued certificates during their validity period and after they expire.
- PKI removes the terminated certificates from the CRL after they have expired.
- In case PKI decides to terminate the CRL, it issues and publishes the last CRL with a value of the NextUpdate field, as defined in clause 6.3.9 of *ETSI EN 319 411-1*.
    - PKI maintains the integrity and availability of the last CRL for at least seven years;
    - PKI does not issue a final CRL until all certificates in the scope of the CRL have either expired or been terminated.
- When providing the OCSP service, the OCSP response will develop the `ArchiveCutOff` extension, as specified in IETF *RFC 6960*, with the `archiveCutOff` date set in the CA certificate "`notBefore`" date value. The extension will be returned in the OCSP responses only for expired certificates.
- When the CA certificate is about to expire, it may calculate the last OCSP response for each issued certificate (whether terminated or not) by setting the value "`99991231235959Z`" via `nextUpdate`.

4.10.2 Service availability

The public repository where certificate information and CRLs are published is accessible 24 hours a day and 7 days a week and guarantees an uptime for at least 99.6% over a one-year period.

The PKI operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

4.11 End of subscription

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

4.12 Key escrow and recovery

Not applicable.

5 Facility, Management, and operational controls

5.1 Physical security controls

The TSP authority ensures that appropriate physical controls are implemented at the BQCA PKI hosting facilities. Such controls are documented as part of BQCA's internal policies that are enforced and verified regularly through internal audits performed by the TSP authority on the BQCA PKI operations team.

5.1.1 Site location and construction

All critical components of the PKI solution are housed within a highly secure facility operated by BQCA. Physical security controls are enforced so that access of unauthorized persons is prevented through **3-tiers** physical security.

When this layered access control is combined with the physical security protection mechanisms such as guards, intrusion sensors and CCTV, it provides robust protection against unauthorized access to the PKI systems.

The data centres hosting the PKI services are located in Belgium.

5.1.2 Physical access

Physical security controls include security guard-controlled building access, biometric access, and CCTV monitoring protect the PKI systems from unauthorized access, these controls are monitored on a 24×7×365 basis.

Unauthorized personnel, including un-trusted or third-party employees or visitors, are not allowed into the enclave without a prior approval and without an escort from one of employee filling a trusted role.

All the Networking and systems components including the certification components are located in secure data cabinets with locks from both sides.

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

5.1.3 Power and air conditioning

The design of the facility hosting the BQCA PKI provides power and backup generators with enough capability to support the PKI systems operations in power failure circumstances.

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

5.1.4 Water exposures

The data centres hosting the PKI systems are implementing reasonable precautions to minimize impact of water exposure. These include installing the PKI equipment on elevated floors with moisture detectors.

5.1.5 Fire prevention and protection

The secure enclave must be protected from fire, heat with a smoke detection equipment monitored on a 24×7×365. Fire suppression equipment is installed within the enclave.

5.1.6 Media storage

Electronic optical and other media must be stored to protect it from accidental damage (water, fire, electromagnetic). Media that contains security audit archive and backup information must be stored in a secure fire-protected safe while within the enclave.

5.1.7 Waste disposal

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

5.1.8 Off-Site backup

Backup media is securely stored in a separated location from the original media location and are protected against fire and water exposure.

Full and incremental backups of the BQCA CA's online systems are taken regularly to provide enough recovery information when the recovery of the PKI systems is necessary.

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

Disaster recovery sites are located in separate premises sufficiently distant from the primary location and benefit from equivalent security measures.

5.2 Procedural controls

5.2.1 Trusted roles

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

All personnel appointed in a trusted position have their background check before they are allowed to work in such a position. The background check shall be maintained and reviewed annually.

The following are the trusted roles for the PKI:

- **TSP manager:** Having operational and compliance responsibility for the qualified trust service;
- **Qualified Security Officers**: Having overall responsibility for administering the implementation of the security policies and practices;
- **Qualified Crypto Custodian:** Responsible for ensuring the safety, secure storage and managing of “m-of-n” secret parts of cryptographic keys;
- **Qualified Registration Officers**: Responsible for verifying information that is necessary for certificate issuance and approval of certification requests;
- **Qualified Revocation Officers**: Responsible for operating certificate status changes;
- **Qualified System Administrators**: Are authorized to install, configure and maintain TWSs for service management;
- **Qualified System Operators**: Are responsible for operating TWSs on a day-to-day basis. Authorized to perform system backup and recovery;
- **Qualified System Auditors**: Authorized to view archives and audit logs of TWSs for the purposes of auditing the operations of the system in line with the security policy.
- **Qualified Developer (dev-ops engineer)**: is responsible for the development of systems that are used within the context of the QTSP core services

5.2.2 Number of persons required per task

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

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

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

All operational activities performed by the personnel having trusted roles are logged and maintained in a verifiable and secure audit trail.

5.2.3 Identification and authentication for each role

Before exercising the responsibilities of a trusted role:

- The CA confirms the identity and history of the employee by carrying out background and security checks.
- When instructed through the internal BQCA processes, the facility operations team issues an access card to each staff who needs to physically access equipment located in the secure enclave.
- PKI dedicated staff (system administrators) issue the necessary IT system credentials for the trusted role to perform their respective functions.

5.2.4 Roles requiring separation of duties

The trusted roles are established with the appropriate segregation of duties.

5.3 Personnel controls

The PKI ensures the implementation of security controls regarding the duties and performance of the members of the PKI staff. These security controls are documented in an internal confidential policy and includes the areas below.

5.3.1 Qualifications, experience, and clearance requirements

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

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

5.3.2 Background check procedures

All employees filling trusted roles are selected based on integrity, background investigation and security clearance. The TSP authority ensures that these checks are performed at least every 3 years for all personnel holding trusted roles.

5.3.3 Training requirements

The TSP authority provides essential technical training for its personnel to effectively carry out their duties.

5.3.4 Retraining frequency and requirements

The training curriculum is delivered to all PKI staff. The training content is reviewed and amended on a yearly basis to reflect the latest leading practices and the CA systems' configuration changes.

5.3.5 Job rotation frequency and sequence

The TSP authority ensures that any change in the PKI staff will not affect the operational effectiveness, continuity, and integrity of the PKI services.

5.3.6 Sanctions for unauthorized actions

To maintain accountability on PKI staff, the TSP authority sanctions personnel for unauthorized actions, unauthorized use of authority and unauthorized use of systems, according to the relevant human resources policy and procedures, and the applicable law.

5.3.7 Independent contractor requirements

Independent contractors and their personnel are subject to the same background checks as the PKI staff. The background checks include:

A. Criminal convictions for serious crimes,

B. Misrepresentations by the candidate,

C. Appropriateness of references,

D. Any clearances as deemed appropriate,

E. Privacy protection, and

F. Confidentiality conditions.

5.3.8 Documentation supplied to personnel

The TSP authority documents all training material and makes it available to PKI staff.

The TSP authority also ensures that the key operational documentation is made available to the relevant staff members. This includes, at a minimum, this CP/CPS document, security policies, operational guides and technical documentation relevant to every trusted role.

5.4 Audit logging procedures

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

Security audit log files for all events relating to the security of the CAs (including Root CAs and Subordinate CAs), RA and OCSP responders shall be generated and preserved.

These logs shall be reviewed by the PKI' Security officer team and are also subject to review as part of the regular internal audits performed by the BQCA compliance function on the BQCA PKI operations.

5.4.1 Types of events recorded

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

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

- Description of the event.

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

Following events occurring in relation to the PKI's operations are recorded:

1. CA key life cycle management events, including:
    - Key generation, backup, storage, recovery, archival and destruction
    - Cryptographic device life-cycle management events
    - certificate requests, renewal, and re-key requests, and revocation
    - Approval and rejection of certificate requests
    - CRL generation
    - Signing of OCSP responses; and
    - Introduction of new certificate Profiles and retirement of existing certificate Profiles.
2. CA and Subscriber certificate lifecycle management events, including:
    - certificate requests, re-key requests, and revocation
    - All issued certificates including revoked and expired certificates.
    - Verification activities evidence (e.g., date, time, calls, persons communicated with)
    - Acceptance and rejection of certificate requests
    - Issuance of certificates
    - CRL updates (including OCSP entries updates where applicable)
    - Signing of OCSP responses.
3. Security events, including:
    - Successful and unsuccessful PKI system access attempts
    - PKI and security system actions performed.
    - Security profiles and configuration changes
    - User management operations
    - System platform issues (e.g., crashes), hardware failures, and other anomalies
    - Firewall and router activities.
    - Entries an exists from the CA facility.

In addition, all registration information, including the following, is recorded by BQCA or by its subcontractors:

- Type of document(s) presented by the applicant to support registration.

- Record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable.
- Storage location of copies of applications and identification documents, including the signed Subject/ Subscriber agreement.
- Any specific choices in the Subject/ Subscriber agreement (e.g. consent to publication of certificate)
- Identity of entity accepting the application.
- Method used to validate identification documents,

The BQCA also ensures that the following information, is maintained (either electronically or manually):

- CA personnel, security profiles rotations/changes
- All versions of this CP/CPS
- Minutes of meetings
- Compliance internal audit reports
- Current and previous versions of PKI configuration an operation manuals
- Report of disaster recovery tests

5.4.2 Frequency of processing logs

The BQCA ensures that designated personnel review log files at regular intervals to validate log integrity and ensure timely identification of anomalous events, using automated methods for processing audit logs.

Audit and Security logs are continuously monitored to provide real time alerts of significant security and operational events for review by designated system security personnel leveraging log aggregation, automation and alerts tools.

Physical access logs and the user management on the PKI systems are reviewed quarterly, to ensure the correct implementation of the physical and logical access policies.

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

5.4.3 Retention period for audit logs

Registered events record logs are stored in files on the system drive for at least 1 month. During this time, they are available online or upon search by any authorized PKI authorized staff. Logs are centralized and kept for at least 12 months.

After this period, the records are archived in accordance with section 5.5.2.

5.4.4 Protection of audit logs

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

- The PKI' systems generate cryptographically protected audit logs
- The security of audits logs is maintained while these logs transit by the backup system and when these logs are archived

- The access control policies enforced on the PKI systems ensures that read access only is granted to personnel having access to audit logs as part of their operational duties
- Only authorized roles can obtain access to systems where audit logs are stored and any attempts to tamper with audit logs can be tracked to the respective PKI staff.

5.4.5 Audit logs backup procedures

Backup media are stored locally in the BQCA main site, in a secure location.

A second copy of the audit logs data and files is stored in the disaster recovery location that provides similar physical and environmental security as the main site.

5.4.6 Notification to event-causing subject

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

5.4.7 Vulnerability assessments

The PKI operations conduct an annual Risk Assessment that:

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

On a quarterly basis, automated vulnerability scan of all public and internal IP addresses of PKI core and supporting PKI systems is performed.

On an annual basis, the TSP authority coordinates a third-party independent vulnerability assessment and penetration testing is conducted on the PKI systems.

The TSP authority is informed of the outcome of the regular assessments and organize and oversee the execution of the remediations by the respective teams.

Evidence of the vulnerability assessment and penetration testing activities execution are collected and archived by the relevant PKI staff.

5.5 Records archival

5.5.1 Types of records archived

The PKI shall archive all audit logs in addition to the following:

1. Documentation related to the security of CA systems (including Root CA system), certificate management systems, and
2. Documentation related to the verification, issuance, and revocation of certificate requests and certificates.

5.5.2 Retention period for archive

Archived audit logs are retained for a period of at least seven (7) years after any certificate based on these records ceases to be valid.

5.5.3 Protection of archive

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

5.5.4 Archive backup procedures

Archives are stored in Google Cloud Storage, a managed object storage service provided by Google Cloud Platform (GCP). Archive data is protected against unauthorized modification or deletion through access control mechanisms and role-based permissions. Retention and immutability controls are applied to prevent alteration of archived records during the defined retention period. Access to archive storage is restricted to authorized and trusted roles only, and all access and modification events are logged and monitored.

5.5.5 Requirements for timestamping of records

All recorded and archived events include the date and time of the event taking place. The time of PKI online systems is synchronized daily with an UTC(k) time source.

5.5.6 Procedures to obtain and verify archive information

Only authorized and authenticated staff is allowed to access archived material.

Requests to access the archives must be addressed to the TSP authority.

5.6 Key changeover

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

If a potential hacking attempt or other form of compromise to the PKI is detected, an investigation to determine the nature and the degree of damage must be performed.

If a PKI (including Root CAs & Document Signing CAs) Private keys are suspected of compromise, the procedures outlined in the BQCA's Business continuity and disaster recovery plan shall be followed. Otherwise, the scope of potential damage is assessed to determine if the PKI needs to be rebuilt, only some certificates need to be revoked, and/or the PKI key needs to be declared compromised,

The TSP authority also specifies applicable compromise reporting and relevant communications as part of the Business continuity and disaster recovery plan.

Apart from the circumstance of key compromise, the BQCA specifies the recovery procedures used when computing resources, software, and/or data are corrupted or suspected of being corrupted.

5.7.2 Computing resources, software, and/or data are corrupted

BQCA implements the necessary measures to ensure full recovery of the PKI services in case of a disaster, corrupted servers, software, or data.

The BQCA disaster recovery and business continuity document specify the circumstances that imply the triggering of incident recovery procedures.

The BQCA disaster recovery and business continuity plan is tested at least once a year.

5.7.3 Recovery procedures after key compromise

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

5.7.4 Business continuity capabilities after a disaster

In case of a disaster, corrupted servers, software or data, the BQCA business continuity plan is triggered to restore the minimum required operational capabilities of the PKI, in a timely fashion. In particular, the plan targets the recovery of the following services, either on the main site, or the backup site:

- Trusted services
- Public repository where CRLs and CAs certificates are published
- OCSP services

The measures allows a recovery of the PKI critical services at the backup site within a maximum of 12 hours RTO.

The BQCA business continuity plan works as follow: the PKI runs on two separate sites with live replication of data between the two sites. On site is active, the other one is passive. In case of an incident that cannot be resolved quickly on the main site, the operational teams manually switch operation to the backup site.

5.8 CA or RA termination

The provision of the PKI trust services shall be terminated:

- Following an BQCA's Executive Management decision
- with a justifiable decision of the authority exercising supervision
- with a final and irrevocable judicial decision
- upon the liquidation or termination of the operations of PKI.

If PKI determines that termination of their services is deemed necessary, the CA termination plan shall be executed, and it shall cover the following actions:

- PKI notifies the following about the termination:
    - all subscribers and relying parties, as well as all entities with which PKI has agreements or other forms of established relations.
    - Other stakeholders (e.g., Auditors and Root programs)
- Ensure certificate status information services are maintained for the applicable period.
- If applicable, PKI makes the best effort for doing arrangements with other TSP to transfer the provision of services for its existing customers.
- If no alternative TSP continues PKI services, all certificates that have not expired or have not been revoked by the respective subscribers will be revoked by PKI. All relevant documentation will be transferred to the Supervisory Body.
- PKI destroys all private keys, including the backup copies in such manner that the private keys cannot be retrieved.
- PKI reinitializes and/or destroys any hardware appliances related to the services being terminated, depending on the security regulations in force.

6 Technical Security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

The PKI key generation ceremony is planned and is subject to the formal authorization of the TSP authority director.

During the ceremony, the PKI ensures that the CA private keys are generated using a certified HSMs (a trustworthy system) that meet the requirements of *FIPS 140-3 Level 3* and dedicated machine to be setup by authorized PKI personnel only. The detailed key ceremony activities are documented in a key ceremony procedure and related ceremony log which are not publicly accessible documents.

The PKI key generation is witnessed and signed off by a third person not involved in the key generation. All activities performed in each PKI key generation ceremony are recorded, dated, and signed by all individuals involved. These records are kept for future audit purpose. A report is issued following the successful ceremony execution.

PKI cryptographic keys have a limited lifetime period; if the period has expired, the PKI are rekeyed.

6.1.1.2 Subscribers

The subscriber keys are generated according to the below requirements:

Certificate type	Key generation requirements
certificates issued to legal persons (eSeal certificates)	**For qualified remote sealing certificates:** The key pair generation occurs within a Qualified Seal Creation Device (QSealCD) that meets Common Criteria EAL4+ standards operated by PKI for its qualified remote eSeal service meeting the requirements of EU Regulation Nº 910/2014 (eIDAS Regulation).
certificates issued to natural persons	**For qualified remote signing certificates:** Subscribers' keys are generated in a Qualified Signature Cryptographic Device (QSignCD) that meets Common Criteria EAL4+ standards operated by PKI for its qualified remote electronic signature service meeting the requirements of EU Regulation Nº 910/2014 (eIDAS Regulation).
OCSP certificates	Key pairs are generated inside a secure cryptographic device that meets FIPS 140-3 level 3 standards.

6.1.2 Private key delivery to subscriber

Subscriber's private's keys are generated within BQCA remote signing platform where subscribers' keys' confidentiality is ensured.

6.1.3 CA public key delivery to relying parties

The PKI public key certificates are published on the BQCA public repository.

6.1.4 Algorithm type and key sizes

6.1.4.1 Certification authorities

CA key pairs are 4096 bits RSA.

6.1.4.2 Subscribers

Subscriber keys are at least 4096 bits RSA, or at least 256 bits ECDSA.

6.1.5 Public key parameters generation and quality checking

The quality of public keys is guaranteed by using secure random number generation. The medium used to generate and store keys is a crypto module (HSM) with a certified security level *FIPS 140-3 Level 3* and *CC EAL 4+*, which meets the applicable regulatory requirements.

Should any of the algorithms, or associated parameters, used by the BQCA or its subscribers become insufficient for its remaining intended usage then the BQCA shall inform all subscribers and relying parties with whom it has agreement or other form of established relations. In addition, the BQCA shall:

1. make this information available to other relying parties;
2. schedule a revocation of any affected certificate.

6.1.6 Key usage purposes (as per X.509 v3 key usage field)

Certificates issued by the PKI contain a *key usage* bit string in accordance with *RFC 5280*.

6.1.6.1 BQCA root CA

Private Keys corresponding to the BQCA Root CA certificates are used to sign only in the following cases:

- Self-signed certificates to represent the BQCA Root CA itself,
- Certificates for Intermediate CAs,
- CARL.

6.1.6.2 BQCA intermediate CAs

Private Keys corresponding to the BQCA intermediate CAs certificates are used to sign only in the following cases:

- Certificates for Issuing CAs.
- CARL.

6.1.6.3 BQCA issuing CAs

Private Keys corresponding to the BQCA Issuing CAs certificates are used to sign only in the following cases:

- Signing subscriber certificates and CRLs.

- Signing OCSP responder certificates.

6.1.6.4 Subscriber certificates

The key usage extension is set in accordance with the certificate profile requirements specified herein.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

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

6.2.2 Private key (n out of m) multi-person control

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

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

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

6.2.3 Private key escrow

Key escrow is not allowed for CAs key pairs or Subscribers key pairs. Dedicated backup and restore procedures of the PKI' private key are implemented.

6.2.4 Private key backup

The PKI private keys are backed up and held stored safely in exclusive safes maintained in the most inner security zones of the BQCA hosting facility.

Signing and sealing keys are replicated between the signing servers on the separate sites using a vendor-specific protocol. This holds for both end-users, OCSP, and CA keys.

6.2.5 Private key archival

Private keys are not archived.

6.2.6 Private key transfer into or from a cryptographic module

Not applicable.

6.2.7 Private key storage on cryptographic module

See previous sections.

6.2.8 Method of activating private key

6.2.8.1 PKI

The CA's private keys are activated inside the HSM as part of audited key ceremonies attended by several trusted personnel and relevant TSP authority personnel. The principles of dual control and split knowledge are enforced so that each trusted personnel involved in the ceremony holds his own set of secrets/activation data/key share. The activation procedure shall use a PIN entry device attached to the HSMs.

The BQCA Root CA key only remains active for the duration of the activity requiring the BQCA Root CA activation (e.g. certification, CRL generation), after which it is kept offline.

The activation procedure is defined in the key ceremony documentation.

6.2.8.2 Subscribers

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

To activate the subscriber's remote signing private key, the remote signing service implements a secure protocol that complies with *EN 419 241-2 Level of Assurance 2 (SCAL-2)*. This protocol requires the involvement of the subscriber to activate his remote signing private key:

- A qualified signing private key is activated by the certificate holder through his SIC included in its Banqup mobile application, after a strong authentication (e.g. fingerprint, face recognition…);
- A qualified sealing private key is activated after validation of a consent signed by a qualified electronic signature of an authorized representative of the binded legal person.

6.2.9 Method of deactivating private key

6.2.9.1 PKI

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

6.2.9.2 Subscribers

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

6.2.10 Method of destroying private key

6.2.10.1 PKI

At the end of their lifetime, the BQCA CA's private keys, including any backup copy, are irrevocably destroyed in the presence of an authorized personal acting as trusted roles.

A report is produced to attest of the destruction.

6.2.10.2 Subscribers

A subscriber's signing key shall be destroyed after the expiration of the public key certificate or if the signing key is useless for the signer.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Refer to 5.5 for archival conditions.

6.3.2 Certificate operational periods and key pair usage periods

The usage periods for certificates issued by this PKI are as follows:

- The BQCA Root CA certificates are valid for 30 years.
- The Document Signing CAs certificates are valid for 10 years.
- The subscriber certificates have a validity period of at most 3 years.

6.4 Activation data

6.4.1 Activation data generation and installation

6.4.1.1 PKI

The CA's private keys and HSM activation data is generated during their private key generation ceremonies.

6.4.1.2 Subscribers

Subscribers shall set and protect the activation data for their private keys to the extent necessary to prevent the loss, theft, unauthorized disclosure, and use of these private keys. Such obligations are presented to the subscribers as part of the Subscriber Agreement.

6.4.2 Activation data protection

6.4.2.1 PKI

The PKI key management policy and ceremony procedures ensure that the principles of multi-person control and split knowledge are permanently enforced to protect the BQCA CA's keys and HSMs activation data. During the key ceremony, activation data are permanently under the custody of the designated PKI staff.

6.4.2.2 Subscribers

Subscribers shall protect the activation data for their private keys.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

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

In particular, the PKI systems and its operations are subject to the following security controls:

1. Separation of duties and dual controls for CA operations

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

6.5.2 Computer security rating

The technical aspects of computer security are subject to periodic audits.

6.6 Life cycle technical controls

6.6.1 System development controls

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

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

All the PKI hardware and software platforms are hardened using industry best practices and vendor recommendations.

6.6.2 Security management controls

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

A configuration management process is enforced to ensure that PKI systems configuration, modification, and upgrades are documented and controlled by the BQCA PKI operations management. In particular, the configuration of the PKI systems are annually checked for changes which violate the BQCA security policies.

A vulnerability management process is enforced to ensure that the PKI equipment is scanned for malicious code on first use and periodically thereafter. The vulnerability management process supports the processing within 48 hours of discovery of critical vulnerabilities not previously met by the PKI operations team.

6.7 Network security controls

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

PKI Root CAs Keys are kept offline and brought on-line only when necessary to sign certificate-issuing subordinate CAs or periodic CRLs or OCSP certificates.

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

6.8 Timestamping

The PKI components are regularly synchronized with an UTC(k) source.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate profile

7.1.1 Root CA Certificate - RSA

Basic Fields of Root CA certificate

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v3² (0x2)	**MANDATORY**
2	**serialNumber**		Unique serial number of the certificate assigned by the CA.	Positive integer	**MANDATORY**
3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	**sha512WithRSAEncryption** (1.2.840.113549.1.1.13)	**MANDATORYprivate key**
4	**issuer**		Distinguished Name of the Issuer's certificate. See **Issuer Field** below for details.	CN: Banqup Root CA RSA G1 O: Banqup Organization Identifier (2.5.4.97): NTRBE-0649860804 C: BE	**MANDATORY**
5	**validity**			ASN.1 SEQUENCE	

6		**notBefore**	The date on which the certificate validity period begins	UTCTime	**MANDATORY**
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **15 years**	**MANDATORY**
8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See **Issuer Field** below for details.	CN: Banqup Root CA RSA G1 O: Banqup Organization Identifier (2.5.4.97): NTRBE-0649860804 C: BE	**MANDATORY**
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	1.2.840.113549.1.1.1 (RSA)	**MANDATORY**
11		**subjectPublicKey**	Public key of the associated entity.	minimum 4096 bits for RSA keys	**MANDATORY**
12	**extensions**		Sequence of one or more certificate extensions. See **Certificate Extensions** below for details.	ASN.1 SEQUENCE	**MANDATORY**
13	**signatureValue**		Certificate signature by the Root CA private key (self signed)	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

Issuer and Subject Field of Root CA certificate

The issuer and subject field contains information from the Root CA.

	Item	Description	Value	Mandatory / Optional / Critical
1	**commonName**	Identification of the subscriber within the CA.	Banqup Root CA RSA G1	**MANDATORY**
2	**organisationName**	Organisation name where the subscriber is employed or which is represented by the subscriber.	Banqup	**MANDATORY**
3	**organisationIdentifier**	Identification number of the organisation.	NTRBE-0649860804	**MANDATORY**
4	**countryName**	Country code. Two characters based on ISO 3166	BE	**MANDATORY**

Certificate Extensions of Root CA certificate

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**AuthorityKeyIdentifier**				**NOT CRITICAL** **MANDATORY**

2		**keyIdentifier**	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1 hash function on the value of the public key of the signing Root CA certificate	
3	**SubjectKeyIdentifier**		Identification of certificates that contain a the subject public key.	160 bit SHA-1 hash function on the value of the public key of the Root CA certificate	**NOT CRITICAL** **MANDATORY**
4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	**keyCertSign** **cRLSign**	**CRITICAL** **MANDATORY**
5	**BasicConstraints**		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.		**CRITICAL** **MANDATORY**
6		**cA**	Identifies whether the subject of the certificate is a CA.	**True**	
7		**pathLenConstraint**	Identifies number of subs in hierarchy	**None**	
8	**AuthorityInformationAccess**		Indicates how to access information and services for the issuer of the certificate.		**NOT CRITICAL** **MANDATORY**
9		**id-ad-calssuers**	Access CA certificate.	URI = http://ca.pki.bangup.com/BangupRootCA.cer	

7.1.2 Root CA Certificate - ECC

Basic Fields of Root CA certificate

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v3² (0x2)	**MANDATORY**
2	**serialNumber**		Unique serial number of the certificate assigned by the CA.	Positive integer	**MANDATORY**
3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	**SHA384withECDSAEncryption** (1.2.840.10045.4.3)	**MANDATORYprivate key**
4	**issuer**		Distinguished Name of the Issuer's certificate. See **Issuer Field** below for details.	CN: Banqup Root CA ECC G1 O: Banqup Organization Identifier (2.5.4.97): NTRBE-0649860804 C: BE	**MANDATORY**
5	**validity**			ASN.1 SEQUENCE	
6		**notBefore**	The date on which the certificate validity period begins	UTCTime	**MANDATORY**
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **15 years**	**MANDATORY**

8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See **Issuer Field** below for details.	CN:Banqup Root CA ECC G1 O: Banqup Organization Identifier (2.5.4.97): NTRBE-0649860804 C: BE	**MANDATORY**
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	1.3.132.0.34 (secp384r1)	**MANDATORY**
11		**subjectPublicKey**	Public key of the associated entity.	minimum 384 bits for ECC keys	**MANDATORY**
12	**extensions**		Sequence of one or more certificate extensions. See **Certificate Extensions** below for details.	ASN.1 SEQUENCE	**MANDATORY**
13	**signatureValue**		Certificate signature by the Root CA private key (self signed)	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

Issuer and Subject Field of Root CA certificate

The issuer and subject field contains information from the Root CA.

	Item	Description	Value	Mandatory / Optional / Critical
1	**commonName**	Identification of the subscriber within the CA.	Banqup Root CA ECC G1	**MANDATORY**
2	**organisationName**	Organisation name where the subscriber is employed or which is represented by the subscriber.	Banqup	**MANDATORY**
3	**organisationIdentifier**	Identification number of the organisation.	NTRBE-0649860804	**MANDATORY**
4	**countryName**	Country code. Two characters based on ISO 3166	BE	**MANDATORY**

Certificate Extensions of Root CA certificate

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**AuthorityKeyIdentifier**				NOT CRITICAL MANDATORY
2		**keyIdentifier**	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1 hash function on the value of the public key of the signing Root CA certificate	
3	**SubjectKeyIdentifier**		Identification of certificates that contain a the subject public key.	160 bit SHA-1 hash function on the value of the public key of the Root CA certificate	NOT CRITICAL MANDATORY
4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	**keyCertSign** **cRLSign**	CRITICAL MANDATORY
5	**BasicConstraints**		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.		CRITICAL MANDATORY
6		**cA**	Identifies whether the subject of the certificate is a CA.	**True**	
7		**pathLenConstraint**	Identifies number of subs in hierarchy	**None**	

8	**AuthorityInformationAccess**		Indicates how to access information and services for the issuer of the certificate.		NOT CRITICAL MANDATORY
9		**id-ad-calssuers**	Access CA certificate.	URI = https://ca.pki.banqup.com/BanqupRootCA-ECC.cer	

7.1.3 Intermediate CA certificate - RSA

Basic Fields of Intermediate CA certificate

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v3 (0x2)	MANDATORY
2	**serialNumber**		Unique serial number of the certificate assigned by the Root CA.	Positive integer explicitly assigned by the CA	MANDATORY
3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the Root CA.	**sha512WithRSAEncryption** (1.2.840.113549.1.1.13)	MANDATORY

4	**issuer**		Distinguished Name of the Issuer's certificate. See **Root CA Subject Field** above for details.	Root CA subject name as X.501 type Name	**MANDATORY**
5	**validity**			ASN.1 SEQUENCE	
6		**notBefore**	The date on which the certificate validity period begins	UTCTime	**MANDATORY**
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **6 years**	**MANDATORY**
8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See **Subject Field** below for details.	CN: Banqup Intermediate CA RSA G1-2025 O: Banqup Organization Identifier (2.5.4.97): NTRBE-0649860804 C: BE	**MANDATORY**
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	**1.2.840.113549.1.1.1 (RSA)**	**MANDATORY**
11		**subjectPublic Key**	Public key of the associated entity.	minimum 4096 bits for RSA keys	**MANDATORY**

12	**extensions**		Sequence of one or more certificate extensions. See **Certificate Extenstions** below for details.	ASN.1 SEQUENCE	**MANDATORY**
13	**signatureValue**		Certificate signature by the Root CA private key	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

Subject Field of Intermediate CA certificate

The subject field contains information from the Intermediate CA.

	Item	Description	Value	Mandatory / Optional / Critical
1	**commonName**	Identification of the subscriber within the CA.	Banqup Intermediate CA RSA G1-2025	**MANDATORY**
2	**organisationName**	Organisation name where the subscriber is employed or which is represented by the subscriber.	Banqup	**MANDATORY**
3	**organisationIdentifier**	Identification number of the organisation.	NTRBE-0649860804	**MANDATORY**
4	**countryName**	Country code	BE	**MANDATORY**

		Two characters based on ISO 3166		

Certificate Extensions of Intermediate CA certificate

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**AuthorityKeyIdentifier**				NOT CRITICAL MANDATORY
2		**keyIdentifier**	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1 hash function on the value of the public key of the signing CA certificate	
3	**SubjectKeyIdentifier**		Identification of certificates that contain the subject public key.	160 bit SHA-1 hash function on the value of the public key of the subscriber's certificate	NOT CRITICAL MANDATORY
4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	**keyCertSign** **cRLSign**	CRITICAL MANDATORY
5	**BasicConstraints**		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.		CRITICAL MANDATORY

6		**cA**	Identifies whether the subject of the certificate is a CA.	**True**	
7		**pathLenConstraint**	Identifies number of subs in hierarchy	**None**	
8	**AuthorityInformationAccess**		Indicates how to access information and services for the issuer of the certificate.		**NOT CRITICAL** **MANDATORY**
9		**id-ad-calssuers**	Access CA certificate.	URI = http://ca.pki.banqup.com/BanqupIntermediateCA.cer	
10	**CRL Distribution point**		CRL Distribution point URI	URI=http://crl.pki.banqup.com/BanqupRootCA.crl	**NOT CRITICAL** **MANDATORY**

7.1.4 Intermediate CA certificate - ECC

Basic Fields of Intermediate CA certificate

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v3 (0x2)	**MANDATORY**
2	**serialNumber**		Unique serial number of the certificate assigned by the Root CA.	Positive integer explicitly assigned by the CA	**MANDATORY**
3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the Root CA.	**SHA384withECDSAEncryption** (1.2.840.10045.4.3)	**MANDATORY**
4	**issuer**		Distinguished Name of the Issuer's certificate. See **Root CA Subject Field** above for details.	Root CA subject name as X.501 type Name	**MANDATORY**
5	**validity**			ASN.1 SEQUENCE	
6		**notBefore**	The date on which the certificate validity period begins	UTCTime	**MANDATORY**
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **6 years**	**MANDATORY**

8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See **Subject Field** below for details.	CN: Banqup Intermediate CA ECC G1-2025 O: Banqup Organization Identifier (2.5.4.97): NTRBE-0649860804 C: BE	**MANDATORY**
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	**1.3.132.0.34 (secp384r1)**	**MANDATORY**
11		**subjectPublic Key**	Public key of the associated entity.	minimum 384 bits for ECC keys	**MANDATORY**
12	**extensions**		Sequence of one or more certificate extensions. See **Certificate Extenstions** below for details.	ASN.1 SEQUENCE	**MANDATORY**
13	**signatureValue**		Certificate signature by the Root CA private key	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

Subject Field of Intermediate CA certificate

The subject field contains information from the Intermediate CA.

	Item	Description	Value	Mandatory / Optional / Critical
1	**commonName**	Identification of the subscriber within the CA.	Banqup Intermediate CA ECC G1-2025	**MANDATORY**
2	**organisationName**	Organisation name where the subscriber is employed or which is represented by the subscriber.	Banqup	**MANDATORY**
3	**organisationIdentifier**	Identification number of the organisation.	NTRBE-0649860804	**MANDATORY**
4	**countryName**	Country code Two characters based on ISO 3166	BE	**MANDATORY**

Certificate Extensions of Intermediate CA certificate

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**AuthorityKeyIdentifier**				**NOT CRITICAL** **MANDATORY**

2		**keyIdentifier**	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1 hash function on the value of the public key of the signing CA certificate	
3	**SubjectKeyIdentifier**		Identification of certificates that contain the subject public key.	160 bit SHA-1 hash function on the value of the public key of the subscriber's certificate	**NOT CRITICAL** **MANDATORY**
4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	**keyCertSign** **cRLSign**	**CRITICAL** **MANDATORY**
5	**BasicConstraints**		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.		**CRITICAL** **MANDATORY**
6		**cA**	Identifies whether the subject of the certificate is a CA.	**True**	
7		**pathLenConstraint**	Identifies number of subs in hierarchy	**None**	
8	**AuthorityInformationAccess**		Indicates how to access information and services for the issuer of the certificate.		**NOT CRITICAL** **MANDATORY**
9		**id-ad-calssuers**	Access CA certificate.	URI = https://ca.pki.banqup.com/BanqupIntermediateCA-ECC.cer	

10	**CRL Distribution point**		CRL Distribution point URI	URI=https://crl.pki.banqup.com/BanqupRootCA-ECC.crl	**NOT CRITICAL** **MANDATORY**

7.1.5 Issuing CA certificate - RSA

Basic Fields of Issuing CA certificate

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v3 (0x2)	**MANDATORY**
2	**serialNumber**		Unique serial number of the certificate assigned by the CA.	Positive integer explicitly assigned by the CA	**MANDATORY**
3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	**sha512WithRSAEncryption** (1.2.840.113549.1.1.13)	**MANDATORY**
4	**issuer**		Distinguished Name of the Issuer's certificate. See **Intermediate CA Subject Field** above for details.	Intermediate CA subject name as X.501 type Name	**MANDATORY**
5	**validity**			ASN.1 SEQUENCE	

6		**notBefore**	The date on which the certificate validity period begins	UTCTime	**MANDATORY**
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **5 years 364 days**	**MANDATORY**
8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See **Subject Field** below for details.	CN: Banqup Issuing CA RSA G1-2025 O: Banqup Organization Identifier (2.5.4.97): NTRBE-0649860804 C: BE	**MANDATORY**
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	1.2.840.113549.1.1.1 (RSA)	**MANDATORY**
11		**subjectPublicKey**	Public key of the associated entity.	minimum 4096 bits for RSA keys	**MANDATORY**
12	**extensions**		Sequence of one or more certificate extensions. See **Certificate Extensions** below for details.	ASN.1 SEQUENCE	**MANDATORY**
13	**signatureValue**		Certificate signature by the Intermediate CA private key	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

Subject Field of Issuing CA certificate

The issuer field contains information from Intermediate CA.

	Item	Description	Value	Mandatory / Optional / Critical
1	**commonName**	Identification of the subscriber within the CA.	Banqup Issuing CA RSA G1-2025	**MANDATORY**
2	**organisationName**	Organisation name where the subscriber is employed or which is represented by the subscriber.	Banqup	**MANDATORY**
3	**organisationIdentifier**	Identification number of the organisation.	NTRBE-0649860804	**MANDATORY**
4	**countryName**	Country code. Two characters based on ISO 3166	BE	**MANDATORY**

Certificate Extensions Issuing CA

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**AuthorityKeyIdentifier**				**NOT CRITICAL** **MANDATORY**

2		**keyIdentifier**	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1 hash function on the value of the public key of the signing CA certificate	
3	**SubjectKeyIdentifier**		Identification of certificates that contain the subject public key.	160 bit SHA-1 hash function on the value of the public key of the subscriber's certificate	**NOT CRITICAL** **MANDATORY**
4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	**keyCertSign** **cRLSign**	**CRITICAL** **MANDATORY**
5	**CertificatePolicies**		Sequence of one or more policy information terms that limit the set of policies for certification paths that include this certificate	**anyPolicy value 2.5.29.32.0**	**NOT CRITICAL** **MANDATORY**
6	**BasicConstraints**		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.		**CRITICAL** **MANDATORY**
7		**cA**	Identifies whether the subject of the certificate is a CA.	True	
8		**pathLenConstraint**	Identifies number of subs in hierarchy	0	
9	**AuthorityInformationAccess**		Indicates how to access information and services for the issuer of the certificate.		**NOT CRITICAL**

					MANDATORY
10		**id-ad-calssuers**	Access CA certificate.	URI = http://ca.pki.banqup.com/BanqupIssuingCA.cer	
11	**CRL Distribution point**		CRL Distribution point URI	URI=http://crl.pki.banqup.com/BanqupIntermediateCA.crl	**NOT CRITICAL** **MANDATORY**

7.1.6 Issuing CA certificate - ECC

Basic Fields of Issuing CA certificate

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v3 (0x2)	**MANDATORY**
2	**serialNumber**		Unique serial number of the certificate assigned by the CA.	Positive integer explicitly assigned by the CA	**MANDATORY**
3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	**SHA384withECDSAEncryption** (1.2.840.10045.4.3)	**MANDATORY**

4	**issuer**		Distinguished Name of the Issuer's certificate. See **Intermediate CA Subject Field** above for details.	Intermediate CA subject name as X.501 type Name	**MANDATORY**
5	**validity**			ASN.1 SEQUENCE	
6		**notBefore**	The date on which the certificate validity period begins	UTCTime	**MANDATORY**
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **5 years 364 days**	**MANDATORY**
8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See **Subject Field** below for details.	CN: Banqup Issuing CA ECC G1-2025 O: Banqup Organization Identifier (2.5.4.97): NTRBE-0649860804 C: BE	**MANDATORY**
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	1.3.132.0.34 (secp384r1)	**MANDATORY**
11		**subjectPublicKey**	Public key of the associated entity.	minimum 384 bits for ECC keys	**MANDATORY**

12	**extensions**		Sequence of one or more certificate extensions. See **Certificate Extensions** below for details.	ASN.1 SEQUENCE	**MANDATORY**
13	**signatureValue**		Certificate signature by the Intermediate CA private key	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

Subject Field of Issuing CA certificate

The issuer field contains information from Intermediate CA.

	Item	Description	Value	Mandatory / Optional / Critical
1	**commonName**	Identification of the subscriber within the CA.	Banqup Issuing CA ECC G1-2025	**MANDATORY**
2	**organisationName**	Organisation name where the subscriber is employed or which is represented by the subscriber.	Banqup	**MANDATORY**
3	**organisationIdentifier**	Identification number of the organisation.	NTRBE-0649860804	**MANDATORY**
4	**countryName**	Country code.	BE	**MANDATORY**

		Two characters based on ISO 3166		

Certificate Extensions Issuing CA

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**AuthorityKeyIdentifier**				NOT CRITICAL MANDATORY
2		**keyIdentifier**	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1 hash function on the value of the public key of the signing CA certificate	
3	**SubjectKeyIdentifier**		Identification of certificates that contain the subject public key.	160 bit SHA-1 hash function on the value of the public key of the subscriber's certificate	NOT CRITICAL MANDATORY
4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	**keyCertSign** **cRLSign**	CRITICAL MANDATORY
5	**CertificatePolicies**		Sequence of one or more policy information terms that limit the set of policies for certification paths that include this certificate	**anyPolicy value** **2.5.29.32.0**	NOT CRITICAL MANDATORY

6	**BasicConstraints**		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.		**CRITICAL** **MANDATORY**
7		**cA**	Identifies whether the subject of the certificate is a CA.	True	
8		**pathLenConstraint**	Identifies number of subs in hierarchy	0	
9	**AuthorityInformationAccess**		Indicates how to access information and services for the issuer of the certificate.		**NOT CRITICAL** **MANDATORY**
10		**id-ad-calssuers**	Access CA certificate.	URI = https://ca.pki.banqup.com/BanqupIssuingCA-ECC.cer	
11	**CRL Distribution point**		CRL Distribution point URI	URI=https://crl.pki.banqup.com/BanqupIntermediateCA-ECC.crl	**NOT CRITICAL** **MANDATORY**

7.1.7 Qualified signature certificate - RSA

Basic Fields of qualified signature certificate

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v3 (0x2)	**MANDATORY**
2	**serialNumber**		Unique serial number of the certificate assigned by the CA.	Positive integer explicitly assigned by the issuing CA	**MANDATORY**
3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	**sha512WithRSAEncryption** (1.2.840.113549.1.1.13)	**MANDATORY**
4	**issuer**		Distinguished Name of the Issuer's certificate. See **issuing CA Subject Field** above for details.	CN: Banqup Issuing CA RSA G1-2025 O: Banqup Organization Identifier (2.5.4.97): NTRBE-0649860804 C: BE	**MANDATORY**
5	**validity**			ASN.1 SEQUENCE	
6		**notBefore**	The date on which the certificate validity period begins	UTCTime	**MANDATORY**
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **1 year**	**MANDATORY**

8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See **Subject Field** below for details.	See **Subject Field**	**MANDATORY**
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	1.2.840.113549.1.1.1 (RSA)	**MANDATORY**
11		**subjectPublicKey**	Public key of the associated entity.	minimum 4096 bits for RSA keys	**MANDATORY**
12	**extensions**		Sequence of one or more certificate extensions. See **Certificate Extensions** below for details.	ASN.1 SEQUENCE	**MANDATORY**
13	**signatureValue**		Certificate signature by the Issuing CA private key	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

Certificate Extensions of qualified signature certificate

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**AuthorityKeyIdentifier**				NOT CRITICAL MANDATORY
2		**keyIdentifier**	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1 hash function on the value of the public key of the signing CA certificate	
3	**SubjectKeyIdentifier**		Identification of certificates that contain the subject public key.	160 bit SHA-1 hash function on the value of the public key of the subscriber's certificate	NOT CRITICAL MANDATORY
4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	**nonRepudiation**	CRITICAL MANDATORY
5	**Qcstatements** **OID 1.3.6.1.5.5.7.1.3**		Qualified certificate statements	0.4.0.1862.1.1 (id-etsi-qcs-QcCompliance) 0.4.0.1862.1.6 (id-etsi-qcs-QcType) 0.4.0.1862.1.6.1 (id-etsi-qct-esign) 0.4.0.1862.1.4	

				(id-etsi-qcs-QcSSCD) 0.4.0.1862.1.5 (id-etsi-qcs-QcPDS) = [https:\\tsp.banqup.com/pds]	
6	**CertificatePolicies**		Sequence of one or more policy information terms according to the policy under which the certificate has been issued	**ETSI QCP-n-qscd 0.4.0.194112.1.2**	**NOT CRITICAL** **MANDATORY**
7		**policyQualifiers**	Pointer to a Certification Practice Statement (CPS) published by the CA.	**CPS.URI=** https://www.pki.banqup.com/repository	
8	**BasicConstraints**		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.		**CRITICAL** **MANDATORY**
12		**cA**	Identifies whether the subject of the certificate is a CA.	**False**	
13		**pathLenConstraint**	Identifies number of subs in hierarchy	**None**	
14	**AuthorityInformationAccess**		Indicates how to access information and services for the issuer of the certificate.		**NOT CRITICAL** **MANDATORY**
15		**id-ad-calssuers**	Access CA certificate.	URI = http://ca.pki.banqup.com/BanqupIssuingCA.cer	

16		**id-ad-ocsp**	OCSP access point	URI = http://ocsp.pki.banqup.com	
17	**CRL Distribution point**		CRL Distribution point URI	URI=http://crl.pki.banqup.com/BanqupIssuingCA.crl	**NOT CRITICAL** **MANDATORY**

Subject Field of qualified signature certificate

	Item	Description	Value	Mandatory / Optional / Critical
1	**commonName**	Identification of the subscriber within the CA.	Combination of given name + surname	**MANDATORY**
2	**GivenName**	The subscriber's given name (first name) as stated in their official legal identity document.	Given name in accordance with legal ID document	**MANDATORY**
3	**SurName**	The subscriber's surname (family name / last name) as stated in their official legal identity document.	Surname in accordance with legal ID document	**MANDATORY**
4	**SubjectSerialnumber**	128 bit unique identifier in accordance with RFC4122	BQID-Subject identifier 8-4-4-12 formatted UUID	**MANDATORY**

5	**countryName**	Country code. Two characters based on ISO 3166	nationality of natural person in accordance with legal ID document	**MANDATORY**

Note : BCA does not issue test certificates from production CA, but only from staging CA.

7.1.8 Qualified signature certificate - ECC

Basic Fields of qualified signature certificate

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v3 (0x2)	**MANDATORY**
2	**serialNumber**		Unique serial number of the certificate assigned by the CA.	Positive integer explicitly assigned by the issuing CA	**MANDATORY**
3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	**SHA384withECDSAEncryption** (1.2.840.10045.4.3)	**MANDATORY**
4	**issuer**		Distinguished Name of the Issuer's certificate. See **issuing CA Subject Field** above for details.	CN: Banqup Issuing CA ECC G1-2025 O: Banqup Organization Identifier (2.5.4.97): NTRBE-0649860804 C: BE	**MANDATORY**

5	**validity**			ASN.1 SEQUENCE	
6		**notBefore**	The date on which the certificate validity period begins	UTCTime	**MANDATORY**
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **1 year**	**MANDATORY**
8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See **Subject Field** below for details.	See **Subject Field**	**MANDATORY**
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	1.3.132.0.34 (secp384r1)	**MANDATORY**
11		**subjectPublicKey**	Public key of the associated entity.	minimum 384 bits for ECC keys	**MANDATORY**
12	**extensions**		Sequence of one or more certificate extensions. See **Certificate Extensions** below for details.	ASN.1 SEQUENCE	**MANDATORY**

13	**signatureValue**		Certificate signature by the Issuing CA private key	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

Certificate Extensions of qualified signature certificate

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**AuthorityKeyIdentifier**				**NOT CRITICAL** **MANDATORY**
2		**keyIdentifier**	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1 hash function on the value of the public key of the signing CA certificate	
3	**SubjectKeyIdentifier**		Identification of certificates that contain the subject public key.	160 bit SHA-1 hash function on the value of the public key of the subscriber's certificate	**NOT CRITICAL** **MANDATORY**
4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	**nonRepudiation**	**CRITICAL** **MANDATORY**
5	**Qcstatements** **OID 1.3.6.1.5.5.7.1.3**		Qualified certificate statements	0.4.0.1862.1.1 (id-etsi-qcs-QcCompliance) 0.4.0.1862.1.6 (id-etsi-qcs-QcType) 0.4.0.1862.1.6.1	

				(id-etsi-qct-esign) 0.4.0.1862.1.4 (id-etsi-qcs-QcSSCD) 0.4.0.1862.1.5 (id-etsi-qcs-QcPDS) = [https:\\tsp.banqup.com/pds]	
6	**CertificatePolicies**		Sequence of one or more policy information terms according to the policy under which the certificate has been issued	**ETSI QCP-n-qscd 0.4.0.194112.1.2**	**NOT CRITICAL** **MANDATORY**
7		**policyQualifiers**	Pointer to a Certification Practice Statement (CPS) published by the CA.	**CPS.URI=** https://www.pki.banqup.com/repository	
8	**BasicConstraints**		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.		**CRITICAL** **MANDATORY**
12		**cA**	Identifies whether the subject of the certificate is a CA.	**False**	
13		**pathLenConstraint**	Identifies number of subs in hierarchy	**None**	
14	**AuthorityInformationAccess**		Indicates how to access information and services for the issuer of the certificate.		**NOT CRITICAL** **MANDATORY**

15		**id-ad-calssuers**	Access CA certificate.	URI = https://ca.pki.banqup.com/BanqupIssuingCA-ECC.cer	
16		**id-ad-ocsp**	OCSP access point	URI = http://ocsp.pki.banqup.com	
17	**CRL Distribution point**		CRL Distribution point URI	URI=http://crl.pki.banqup.com/BanqupIssuingCA.crl	**NOT CRITICAL** **MANDATORY**

Subject Field of qualified signature certificate

	Item	Description	Value	Mandatory / Optional / Critical
1	**commonName**	Identification of the subscriber within the CA.	Combination of given name + surname	**MANDATORY**
2	**GivenName**	The subscriber's given name (first name) as stated in their official legal identity document.	Given name in accordance with legal ID document	**MANDATORY**
3	**SurName**	The subscriber's surname (family name / last name) as stated in their official legal identity document.	Surname in accordance with legal ID document	**MANDATORY**
4	**SubjectSerialnumber**	128 bit unique identifier in accordance with RFC4122	BQID-Subject identifier	**MANDATORY**

			8-4-4-12 formatted UUID	
5	**countryName**	Country code. Two characters based on ISO 3166	nationality of natural person in accordance with legal ID document	**MANDATORY**

Note : BCA does not issue test certificates from production CA, but only from staging CA.

7.1.9 Qualified seal certificate - RSA

Basic Fields of qualified seal certificates

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v3 (0x2)	**MANDATORY**
2	**serialNumber**		Unique serial number of the certificate assigned by the CA.	Positive integer self signed	**MANDATORY**
3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	**sha512WithRSAEncryption** (1.2.840.113549.1.1.13)	**MANDATORY**

4	**issuer**		Distinguished Name of the Issuer's certificate. See **Issuing CA Subject Field** above for details.	See Issuer Field	**MANDATORY**
5	**validity**			ASN.1 SEQUENCE	
6		**notBefore**	The date on which the certificate validity period begins	UTCTime	**MANDATORY**
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **3 year**	**MANDATORY**
8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See **Subject Field** below for details.	See **Subject Field**	**MANDATORY**
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	1.2.840.113549.1.1.1 (RSA)	**MANDATORY**
11		**subjectPublicKey**	Public key of the associated entity.	minimum 4096 bits for RSA keys	**MANDATORY**

12	**extensions**		Sequence of one or more certificate extensions. See **Certificate Extensions** below for details.	ASN.1 SEQUENCE	**MANDATORY**
13	**signatureValue**		Certificate signature by the Issuing CA private key	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

Certificate Extensions of qualified seal certificates

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**AuthorityKeyIdentifier**				**NOT CRITICAL** **MANDATORY**
2		**keyIdentifier**	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1 hash function on the value of the public key of the signing CA certificate	
3	**SubjectKeyIdentifier**		Identification of certificates that contain the subject public key.	160 bit SHA-1 hash function on the value of the public key of the subscriber's certificate	**NOT CRITICAL** **MANDATORY**
4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	**NonRepudiation** **digitalSignature**	**CRITICAL**

					MANDATORY
5	**Qcstatements** **OID 1.3.6.1.5.5.7.1.3**		Qualified certificate statements	0.4.0.1862.1.1 (id-etsi-qcs-QcCompliance) 0.4.0.1862.1.6 (id-etsi-qcs-QcType) 0.4.0.1862.1.6.1 (id-etsi-qct-esign) 0.4.0.1862.1.4 (id-etsi-qcs-QcSSCD) 0.4.0.1862.1.5 (id-etsi-qcs-QcPDS) = [https:\\tsp.bangup.com/pds]	
6	**CertificatePolicies**		Sequence of one or more policy information terms according to the policy under which the certificate has been issued	**ETSI QCP-l-qscd** **0.4.0.194112.1.2**	**NOT CRITICAL** **MANDATORY**
7		**policyQualifiers**	Pointer to a Certification Practice Statement (CPS) published by the CA.	**CPS.URI=** https://www.pki.bangup.com/repository	
8	**BasicConstraints**		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.		**CRITICAL** **MANDATORY**
9		**cA**	Identifies whether the subject of the certificate is a CA.	**False**	

10		**pathLenConstraint**	Identifies number of subs in hierarchy	**None**	
11	**AuthorityInformationAccess**		Indicates how to access information and services for the issuer of the certificate.		**NOT CRITICAL** **MANDATORY**
12		**id-ad-calssuers**	Access CA certificate.	URI = http://ca.pki.banqup.com/BanqupIssuingCA.cer	
13		**id-ad-ocsp**	OCSP access point	URI = http://ocsp.pki.banqup.com	
14	**CRL Distribution point**		CRL Distribution point URI	URI= https://crl.pki.banqup.com/BanqupIssuingCA-ECC.crl	

Subject Field of qualified seal certificate

	Item	Description	Value	Mandatory / Optional / Critical
1	**commonName**	Identification of the subscriber within the CA.	Trade name or Legal name	**MANDATORY**

2	**OrganisationName**	Organisation name where the subscriber is employed or which is represented by the subscriber.	Organisation name in accordance with legal register (= Legal name)	**MANDATORY**
3	**SubjectOrgIdentifier**	Identification number of the organisation.	NTR[countrycode]-[traderegisternumber] VAT [tax identification number] PDS [national authorization number of a payment service provider] LEI [global Legal Entity Identifier] For details refer to: ETSI EN 319 412-1	**MANDATORY**
4	**countryName**	Country code.	nationality of data subject - Two characters based on ISO 3166	**MANDATORY**

Note : BCA does not issue test certificates from production CA, but only from staging CA.

7.1.10 Qualified seal certificate - ECC

Basic Fields of qualified seal certificates

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v3 (0x2)	**MANDATORY**
2	**serialNumber**		Unique serial number of the certificate assigned by the CA.	Positive integer self signed	**MANDATORY**

3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	**SHA384withECDSAEncryption** (1.2.840.10045.4.3)	**MANDATORY**
4	**issuer**		Distinguished Name of the Issuer's certificate. See **Issuing CA Subject Field** above for details.	See Issuer Field	**MANDATORY**
5	**validity**			ASN.1 SEQUENCE	
6		**notBefore**	The date on which the certificate validity period begins	UTCTime	**MANDATORY**
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **3 year**	**MANDATORY**
8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See **Subject Field** below for details.	See **Subject Field**	**MANDATORY**
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	1.3.132.0.34 (secp384r1)	**MANDATORY**

11		**subjectPublicKey**	Public key of the associated entity.	minimum 384 bits for ECC keys	**MANDATORY**
12	**extensions**		Sequence of one or more certificate extensions. See **Certificate Extensions** below for details.	ASN.1 SEQUENCE	**MANDATORY**
13	**signatureValue**		Certificate signature by the Issuing CA private key	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

Certificate Extensions of qualified seal certificates

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**AuthorityKeyIdentifier**				**NOT CRITICAL** **MANDATORY**
2		**keyIdentifier**	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1 hash function on the value of the public key of the signing CA certificate	
3	**SubjectKeyIdentifier**		Identification of certificates that contain the subject public key.	160 bit SHA-1 hash function on the value of the public key of the subscriber's certificate	**NOT CRITICAL** **MANDATORY**

4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	**NonRepudiation digitalSignature**	**CRITICAL** **MANDATORY**
5	**Qcstatements** **OID 1.3.6.1.5.5.7.1.3**		Qualified certificate statements	0.4.0.1862.1.1 (id-etsi-qcs-QcCompliance) 0.4.0.1862.1.6 (id-etsi-qcs-QcType) 0.4.0.1862.1.6.1 (id-etsi-qct-esign) 0.4.0.1862.1.4 (id-etsi-qcs-QcSSCD) 0.4.0.1862.1.5 (id-etsi-qcs-QcPDS) = [https:\\tsp.banqup.com/pds]	
6	**CertificatePolicies**		Sequence of one or more policy information terms according to the policy under which the certificate has been issued	**ETSI QCP-l-qscd 0.4.0.194112.1.2**	**NOT CRITICAL** **MANDATORY**
7		**policyQualifiers**	Pointer to a Certification Practice Statement (CPS) published by the CA.	**CPS.URI=** https://www.pki.banqup.com/repository	
8	**BasicConstraints**		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.		**CRITICAL** **MANDATORY**
9		**cA**	Identifies whether the subject of the certificate is a CA.	**False**	

10		**pathLenConstraint**	Identifies number of subs in hierarchy	**None**	
11	**AuthorityInformationAccess**		Indicates how to access information and services for the issuer of the certificate.		**NOT CRITICAL** **MANDATORY**
12		**id-ad-calssuers**	Access CA certificate.	URI = https://ca.pki.banqup.com/BanqupIssuingCA-ECC.cer	
13		**id-ad-ocsp**	OCSP access point	URI = http://ocsp.pki.banqup.com	
14	**CRL Distribution point**		CRL Distribution point URI	URI= https://crl.pki.banqup.com/BanqupIssuingCA-ECC.crl	

Subject Field of qualified seal certificate

	Item	Description	Value	Mandatory / Optional / Critical
1	**commonName**	Identification of the subscriber within the CA.	Trade name or Legal name	**MANDATORY**

2	**OrganisationName**	Organisation name where the subscriber is employed or which is represented by the subscriber.	Organisation name in accordance with legal register (= Legal name)	**MANDATORY**
3	**SubjectOrgIdentifier**	Identification number of the organisation.	NTR[countrycode]-[traderegisternumber] VAT [tax identification number] PDS [national authorization number of a payment service provider] LEI [global Legal Entity Identifier] For details refer to: ETSI EN 319 412-1	**MANDATORY**
4	**countryName**	Country code.	nationality of data subject - Two characters based on ISO 3166	**MANDATORY**

Note : BCA does not issue test certificates from production CA, but only from staging CA.

7.2 CRL profile

RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Basic CRL Fields

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v2 (0x1)	**MANDATORY**

2	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	**sha512withRSAEncryption** (1.2.840.113549.1.1.13)	**MANDATORY**
3	**issuer**		Distinguished Name of the Issuer's certificate.	X.501 type Name	**MANDATORY**
4	**thisUpdate**		Issue date of the CRL	UTCTime	**MANDATORY**
5	**nextUpdate**		The date by which the next CRL will be issued.	UTCTime +24hr	**MANDATORY**
6	**revokedCertificates**		List of revoked certificates.		**MANDATORY** if there is at least one certificate revoked. Not present if the list of certificates is empty.
7		**userCertificate**	Serial number of revoked certificate	CertificateSerialNumber	
8		**revocationDate**	Time when the certificate was revoked.	UTCTime	
9		**crlEntryExtensions**	Sequence of one or more certificate revocation list extensions. See **CRL Extensions** below for details.	ASN.1 SEQUENCE	
10	**crlExtensions**		Sequence of one or more certificate revocation list extensions.	ASN.1 SEQUENCE	

			See **CRL Extensions** below for details.		
11	**signatureValue**		Signature by the Issuing CA private key	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

CRL Extensions

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**crlReason**		Reason for the revocation.	unspecified (0) keyCompromise (1) cACompromise (2) affiliationChanged (3) superseded (4) cessationOfOperation (5) certificateHold (6) removeFromCRL (8) privilegeWithdrawn (9) aACompromise (10)	**NOT CRITICAL** **MANDATORY** for certificates in the list of **revokedCertificates**
2	**AuthorityKeyIdentifier**				**NOT CRITICAL** **MANDATORY**
3		**keyIdentifier**	Identification of the public key corresponding to the	160 bit SHA-1 hash function on the value of the public key of the signing CA certificate	

			private key used to sign a certificate.		
4	**crlNumber**		Unique number of the CRL.	Incremental Value up to 20 octets	NOT CRITICAL MANDATORY
5	**expiredCertsOnCRL**		Indicates that the CRL will include revocation status information for certificates that have already expired.	**True**	

7.3 OCSP profile

OCSP Responder Basic Certificate Fields

	Field	Sub-fields in SEQUENCE	Description	Value	Mandatory / Optional / Critical
1	**version**		Version of the certificate that complies with X.509 standard, version 3.	v3 (0x2)	MANDATORY
2	**serialNumber**		Unique serial number of the certificate assigned by the CA.	Positive integer explicitly assigned by the CA	MANDATORY

3	**signatureAlgorithm**		Cryptographic algorithm identifier, describing the algorithm used to sign the certificate by the CA.	**sha512WithRSAEncryption** (1.2.840.113549.1.1.13)	**MANDATORY**
4	**issuer**		Distinguished Name of the Issuer's certificate. See **Issuing CA Subject Field** above for details.	X.501 type Name	**MANDATORY**
5	**validity**			ASN.1 SEQUENCE	
6		**notBefore**	The date on which the certificate validity period begins	UTCTime	**MANDATORY**
7		**notAfter**	The date on which the certificate validity period ends.	notBefore + **1 year**	**MANDATORY**
8	**subject**		Identification of the entity associated with the public key stored in the SubjectPublicKeyInfo field. See **Subject Field** below for details.	X.501 type Name	**MANDATORY**
9	**subjectPublicKeyInfo**			ASN.1 SEQUENCE	
10		**algorithm**	Identifies the algorithm with which the key is used.	1.2.840.113549.1.1.1 (RSA)	**MANDATORY**

11		**subjectPublicKey**	Public key of the associated entity.	minimum 4096 bits for RSA keys	**MANDATORY**
12	**extensions**		Sequence of one or more certificate extensions. See **Certificate Extensions** below for details.	ASN.1 SEQUENCE	**MANDATORY**
13	**signatureValue**		Certificate signature by the Issuing CA private key	Signature value using the declared signature algorithm, represented as BIT STRING	**MANDATORY**

Subject Field of OCSP responder certificate

	Item	Description	Value	Mandatory / Optional / Critical
1	**commonName**	Identification of the subscriber within the CA.	Banqup OCSP responder signingcertificate	**MANDATORY**
2	**organisationName**	Organisation name where the subscriber is employed or which is represented by the subscriber.	O: Banqup	**MANDATORY**
3	**organisationIdentifier**	Identification number of the organisation.	NTRBE-0649860804	**MANDATORY**

4	**countryName**	Country code.	BE Two characters based on ISO 3166	**MANDATORY**

Certificate Extensions of OCSP responder certificate

	Extension	Sub-fields in SEQUENCE	Description	Content	Mandatory / Optional / Critical
1	**AuthorityKeyIdentifier**			From CA	**NOT CRITICAL** **MANDATORY**
2		**keyIdentifier**	Identification of the public key corresponding to the private key used to sign a certificate.	160 bit SHA-1 hash function on the value of the public key of the signing CA certificate	
3	**SubjectKeyIdentifier**		Identification of certificates that contain a the subject public key.	160 bit SHA-1 hash function on the value of the public key of the subscriber's certificate	**NOT CRITICAL** **MANDATORY**
4	**KeyUsage**		Defines the purpose of the key contained in the certificate.	**digitalSignature**	**CRITICAL** **MANDATORY**
5	**ExtendedKeyUsage**		Indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension.	**id-kp-OCSPSigning**	**CRITICAL** **MANDATORY**

6	**id-pkix-ocsp-nocheck**		No revocation check of the OCSP responder certificate. OCSP client can trust a responder for the lifetime of the responder's certificate.	True	**NOT CRITICAL** **MANDATORY**
8	**Certificate Policies**	**policyIdentifier**	Identification of the policy.	**CPS.URI=** https://www.pki.bangup.com/repository	
9	**BasicConstraints**		Identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.		**CRITICAL** **MANDATORY**
10		**cA**	Identifies whether the subject of the certificate is a CA.	False	
11	**AuthorityInformationAccess**		Indicates how to access information and services for the issuer of the certificate.		**NOT CRITICAL** **MANDATORY**
12		**id-ad-calssuers**	Access CA certificate.	**CPS.URI=** https://www.pki.bangup.com/repository	

8 Compliance Audit and other assessments

8.1 Frequency or circumstances of assessment

PKI undergoes an external audit every two years by a Conformity Assessment Body (i.e., CAB), or whenever a major change is made to Trust Service operations, based on the applicable ETSI standards.

In all cases, PKI shall always:

- comply with the requirements of this CP/CPS;
- comply with the latest approved versions of *ETSI EN 319 401*, *ETSI EN 319 411-1*, *ETSI EN 319 411-2*.

In addition, BQCA performs internal self-audit to ensure the trustworthiness of PKI Certification Services.

8.2 Identity/qualifications of assessor

BQCA compliance audits are performed:

- By appropriately accredited auditor, in accordance with applicable local laws and ETSI standards (i.e. ETSI EN 319 403) requirements.
- Regulation (EU) No 910/2014, as amended by Regulation (EU) 2024/1183, including any further amendments and applicable implementing acts.
- The Supervisory Body
- Internal compliance officers

8.3 Assessor's relationship to assessed entity

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

The Accredited Conformity Assessment Body (i.e., CAB) is an independent third-party auditor.

8.4 Topics covered by assessment

The scope of audits and other assessment includes compliance with applicable law, with this CP/CPS, and other rules, procedures and processes (especially those related to key management operations, resources, management and operation controls and life cycle certificate management).

8.5 Actions taken as a result of deficiency

Issues and findings resulting from the assessment are reported to the PKI Board.

Regarding compliance audits of PKI operations, any notable exceptions or deficiencies discovered during the audit process prompt a decision on necessary actions. This decision is made by the TSP authority with input from the auditor.

Additionally, in the event of a result of the assessment by the Conformity Assessment Body, showing deficiency, the Supervisory Body requires BQCA to remedy any failure to fulfil requirements within a time limit (if applicable) set by the Supervisory Body. BQCA makes efforts to stay compliant and fulfil all requirements of the deficiency on time. TSP authority is responsible to implement a corrective action plan. TSP authority evaluates the significances of deficiencies and prioritizes appropriate actions to be taken at least during the time limit declared by Supervisory Body or reasonable period of time.

8.6 Communication of results

The results of audits and evaluations of compliance must be delivered to TSP authority within the contractually stipulated deadlines.

The information about the corrective actions performed and / or to be performed shall be sent to the Supervisory Body in the shortest time possible (when applicable).

8.7 Notification to the Supervisory Body

Banqup shall notify the supervisory body of any significant changes to its qualified trust services, in the following cases and using the following procedures:

The supervisory body shall be notified when Significant changes occur to:

- Service descriptions, policies, practice statements, or associated terms and conditions.
- Technical architecture of the trust services, or any trustworthy systems or products in use.
- Hosting or technical services of any components used to provide the qualified trust services.
- Cryptographic techniques or materials used in the provision of the services.
- Registration and identification procedures.
- Organisational structure or governance.
- Termination plans.
- Financial resources or liability insurance.
- Elements affecting the content of the national trusted list.
- Third parties involved in providing the qualified trust services, including subcontractors or changes to contractual terms.

Notifications to the supervisory body shall be made in a structured and timely manner. Each notification shall include:

- A description of the change or planned cessation of services.
- The scheduled date and time for the implementation of the change.
- The reasons for the change, supported by evidence where applicable.
- Any updated or amended documentation relevant to the change.

Notifications shall be submitted sufficiently in advance of the planned implementation to allow the supervisory body to review and assess potential compliance impacts. Submissions may be made electronically or in writing, in accordance with the supervisory body’s preferred communication method.

9 Other Business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Applicable fees, if any, are to be agreed upon by BQCA and subscribers.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

Access for certificate revocation or status information is free of charge.

9.1.4 Fees for other services

PKI may charge for other services depending on business needs.

9.1.5 Refund policy

No refunds for any charged fees.

9.2 Financial responsibility

9.2.1 Insurance coverage

BQCA respects the legislation in force regarding insurance coverage and ensures that the PKI is covered by the existing insurance provisions.

9.2.2 Insurance or warranty coverage for end-entities

Refer to section 9.6.1.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

BQCA considers the following as confidential information:

- All personal information supplied to PKI during the registration process of certificate subscribers that are not part of certificates or CRLs, unless there is an explicit authorization for its disclosure.
- Correspondence between and the RA function during the certificate management processing (including the collected subscriber's data)
- Contractual agreements between PKI and its suppliers
- BQCA internal documentation (business processes, operational processes, Business continuity and recovery plans…)

- Employees confidential information
- Certification Authorities private keys;
- certificate holders' private keys;
- All information concerning parameters of security,
- control and audit procedures;
- Information not within the scope of confidential information

Any information not defined as confidential by PKI shall be deemed public. This includes the information published on the BQCA public repository.

9.3.2 Responsibility to protect confidential information

BQCA protects confidential information through training and policy enforcement with its employees, contractors, and suppliers.

9.4 Privacy of personal information

BQCA, acting as a TSP, operates within the boundaries of the European General Data Protection Regulation (GDPR). Personal data communicated to BQCA's RA by the applicant are kept in a suitably protected file held by BQCA.

9.5 Intellectual property rights

BQCA owns and reserve all intellectual property rights associated with its own databases, web sites, the CAs' electronic certificates and any other publication whatsoever originating from the PKI, including this CP/CPS.

When BQCA uses software from third party suppliers, this software remains the intellectual property of the product suppliers, and its usage by BQCA CAs bound by license agreements between BQCA and these suppliers.

9.6 Representations and warranties

9.6.1 CA representations and warranties

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

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

- The Subscriber that is a party to the Subscriber Agreement
- All Application Software Suppliers with whom the BQCA will enter into a contract for inclusion of its Root certificate in software distributed by such Application Software Supplier; and
- All Relying Parties who reasonably rely on a valid certificate.

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

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

- **Authorization for certificate:** That, at the time of issuance, BQCA:

    i. implemented a procedure for verifying that the Subject authorized the issuance of the certificate, and that the Applicant Representative is authorized to request the certificate on behalf of the Subject,

    ii. followed the procedure when issuing the certificate, and

    iii. accurately described the procedure in this CP/CPS.

- **Accuracy of Information:** That, at the time of issuance, BQCA:

i. implemented a procedure for verifying the accuracy of all of the information contained in the certificate according to this CP/CPS and the Baseline requirements (with the exception of the subject:organizationalUnitName attribute),

ii. followed the procedure when issuing the certificate, and

iii. accurately described the procedure in this CPS.

- **No Misleading Information:** That, at the time of issuance, PKI:

i. implemented a procedure for reducing the likelihood that the information contained in the certificate's subject:organizationalUnitName attribute would be misleading,

ii. followed the procedure when issuing the certificate, and

iii. accurately described the procedure in this CPS

- **Identity of Applicant:** That, if the certificate contains Subject Identity Information, BQCA:

i. implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2,

ii. followed the procedure when issuing the certificate,

iii. accurately described the procedure in this CPS.

- **Subscriber Agreement:** That, if the PKI and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use.

- **Status:** That BQCA maintains a 24×7 publicly accessible Repository with current information regarding the status (valid or revoked) of all unexpired certificates.

- **Revocation:** That BQCA will revoke the certificate for any of the reasons specified in these Requirements.

9.6.2 RA representations and warranties

BQCA warrants that it performs RA functions as per the stipulations specified in this CP/CPS. In particular, RA's obligations include:

- Ensure that Subjects (applicants) are properly authenticated and identified.
- Ensure that certificate requests are valid, complete and properly authorized.
- Enforce and respect the present CP/CPS.
- Submit certificate requests with complete and valid information to the CA.
- Alert the CA in the event of a security incident.
- Collect and verify the supporting documents that allow the authentication of the Subject and the creation of the Subject's identity.
- Protect the personal data of the applicant.
- When applicable, manage the RA and RA Operators (maintain a list of RAs).
- Retain logs and evidence files as required by the present CP/CPS.

9.6.3 Subscriber representations and warranties

BQCA implements a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the certificate to be issued pursuant to the certificate request. A separate Agreement is used for each certificate request. The Subscriber Agreement or Terms of Use contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

- **Accuracy of Information:** An obligation and warranty to provide accurate and complete information at all times to BQCA, both in the certificate request and as otherwise requested by BQCA in connection with the issuance of the certificate(s) to be supplied by the PKI

- **Protection of Private Key:** An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly always protect the Private Key that corresponds to the Public Key to be included in the requested certificate(s) (and any associated activation data or device, e.g., password or token)

- **Acceptance of certificate:** An obligation and warranty that the Subscriber will review and verify the certificate contents for accuracy

- **Use of certificate:** To use the certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement

- **Reporting and Revocation:** An obligation and warranty to: (a) promptly request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the certificate, and (b) promptly request revocation of the certificate, and cease using it, if any information in the certificate is or becomes incorrect or inaccurate

- **Termination of Use of certificate:** An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the certificate upon revocation of that certificate for reasons of Key Compromise.

- **Responsiveness:** An obligation to respond to BQCA instructions concerning Key Compromise or certificate misuse within a specified time period.

- **Acknowledgment and Acceptance:** An acknowledgment and acceptance that BQCA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if revocation is required by this CPS, or the Baseline Requirements.

9.6.4 Relying party representations and warranties

Relying Parties who rely upon the certificates issued under BQCA shall:

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

9.6.5 Representations and warranties of other participants

External RA's (see 1.3.2) are bound to the same obligations as RA's (9.6.2).

The common obligations of the external organization supporting UPCA's services are:

- Agree to have the audit team conduct compliance audits and provide them with all relevant information.
- Accept the result and consequences of these audits and remediate any non-conformity that may be revealed.
- Ensure the integrity and confidentiality of the private keys in their custody, as well as the activation data of said private keys, if any.
- Use the public and private keys in their custody only for the purposes for which they were issued and with the appropriate means.
- Implement the adequate technical means and employ the human resources necessary for the realization of the services to which they commit themselves.
- Document and provide the internal operating procedures to the personnel in charge of supporting UPCA's services.
- Respect and apply the terms of this CP/CPS.
- Respect the agreements that bind them to the other entities of UPCA's services.

9.7 Disclaimers of warranties

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

- The accuracy of any information contained in certificates except as it is warranted by the subscriber that is the party responsible for the ultimate correctness and accuracy of all data transmitted to BQCA with the intention to be included in a CA certificate,
- Indirect damage that is the consequence of or related to the use, provisioning, issuance or non-issuance of certificates or electronic signatures,
- Wilful misconduct of any third-party participant breaking any applicable laws, including, but not limited to those related to intellectual property protection, malicious software, and unlawful access to computer systems,
- For any damages suffered whether directly or indirectly because of an uncontrollable disruption of the PKI services,

- Any form of misrepresentation of information by the subscribers or relying parties on information contained in this CP/CPS or any other documentation made public by the BQCA and related to the PKI services.

9.8 Limitations of liability

- BQCA will not incur any liability to Subscribers to the extent that such liability results from their negligence, fraud, or wilful misconduct,
- BQCA assumes no liability whatsoever in relation to the use of certificates or associated Public-Key/Private-Key pairs issued under this CPS for any use other than in accordance with this document. The Subscribers will immediately indemnify BQCA from and against any such liability and costs and claims arising there from,
- BQCA will not be liable to any party whosoever for any damages suffered whether directly or indirectly because of an uncontrollable disruption of its services,
- Subscribers are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been accepted by BQCA,
- Subscribers to compensate a Relying Party which incurs a loss because of the TSP's breach of Subscriber's agreement.
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations; and
- BQCA denies any financial or any other kind of responsibility for damages or impairments resulting from the PKI operations.

9.9 Indemnities

Not applicable

9.10 Term and termination

9.10.1 Term

This CP/CPS comes into force from the moment of its publication at the PKI repository and after its approval, on the terms of this document.

9.10.2 Termination

This CP/CPS will remain in force until expressly revoked by publication of a new version in the BQCA public repository, under the terms of this document. Upon publishing on the BQCA public repository, the newer version becomes effective. The older versions of this document are archived by BQCA on its public repository.

9.10.3 Effect of termination and survival

The BQCA GB shall communicate the conditions and effect of this CPS termination via appropriate mechanisms.

9.11 Individual notices and communications with participants

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

9.12 Amendments

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

9.12.1 Procedure for amendment

Refer to Section 9.12.

9.12.2 Notification mechanism and period

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

The TSP authority coordinates communication in relation to the amendments of this CPS and related effects.

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

In cases of major enhancement that may affect the acceptability of certificates for the purposes that they have been issued, it will be tried the notification to interested parties that a change or correction was made.

9.12.3 Circumstances under which OID must be changed

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

9.13 Dispute resolution provisions

All disputes arising from the interpretation or application of this CP/CPS, shall be first addressed to the TSP authority legal function. If mediation by the TSP authority legal function is not successful, then the dispute shall be adjudicated by the relevant courts of Belgium.

9.14 Governing law

The laws of the state of Belgium shall govern the enforceability, construction, interpretation, and validity of this CPS.

9.15 Compliance with applicable law

This CPS and provision of PKI services are compliant to relevant and applicable laws.

Trust services provided and end user products used in the provision of those services are made accessible for persons with disabilities, where feasible.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Force majeure

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