THE BENEFIT COMPANY

BENEFIT TRUST SERVICES

CERTIFICATE POLICY & CERTIFICATE PRACTICE STATEMENT (CP/CPS)

Approved by: BENEFIT Certificate Authority Governance Committee

PUBLIC

Version: 1.1

Effective Date: 01/07/2021

Domain:	Subdomain:	Reference:	Status:
Security	PKI	1.3.6.1.4.1.56818.1.1.1.1	Approved
Validated by:	**Role:**	**Date:**	**Signature:**
Shafaq Al Kooheji	Member of CAGC	1 July 2021	
Approved by:	**Role:**	**Date:**	**Signature:**
Riyad Al Maraj	Chairman of CAGC	1 July 2021	
Diffusion:	.....		
Access:	Public. Available on the website: https://www.benefit.bh/MediaHandler/GenericHandler/documents/CertificationAuthorityforDigitalCertificates/CertificatePracticeStatement.pdf		
Localisation:	EN		

Table of Content

Version	Date	Modifications	Author
0.9	9 March 2021	Draft Version	Yaqoob Al Balooshi
1.0	6 April 2021	First Official Version	Yaqoob Al Balooshi
1.1	1 July 2021	Update Trusted roles	Yaqoob Al Balooshi

Table of Content

COPYRIGHT NOTICE

1. INTRODUCTION

1.1 GENERAL PRESENTATION

As a part of its current expansion of its digital solution portfolio and trust service offerings, BENEFIT (The Trust Service Provider (TSP)) provide an Electronic Cheque Platform (E-Cheque) that provide the business applications for Electronic Cheques. BENEFIT also operates a Certification Authority available to individual natural persons referred to as Subscribers, BENEFIT CA. Additionally, BENEFIT provides the services that manage private keys of the Subscribers and operate remote QSCD device for remote advanced signature creation on behalf of the signer (natural person).

BENEFIT operates as a trust service provider issuing advanced certificates and advanced electronic signatures that are used in the E-Cheque Platform.

In this context, this document constitutes the Certification Policy (CP) and Certificate Practice Statement (CPS) of the Certification Authority (CA) - BENEFIT CA- and management of signature private keys, and remote signature creation. This document serves as the TSP statement. This document, “BENEFIT Trust Services Certificate Policy / Certificate Practice Statement” (hereinafter: CP/CPS or TSP Statement) corresponds to the document called “Certification Practice Statement CPS” according to IETF RFC 3647.

BENEFIT CA is intended to issue Electronic signature Certificates in accordance ETSI EN 319 411-1 under Extended Normalized Certificate Policy (NCP+). These certificates are issued to BENEFIT subscribers (natural person for private or professional use) for Electronic Cheques Electronic Signing. For the scope of these certificates, BENEFIT runs its own Registration Authority for its subscribers (see section 3.4in this CP/CPS for details).

This CP/CPS specifies organizational and technical measures for BENEFIT trust services in practice during identity validation, certificate issuance on QSCD, certificate lifecycle, management of private keys used for E-Cheque digital signature.

This CP/CPS describes the organizational and technical measures applied by BENEFIT, as the TSP, for the fulfillment of the requirements of Server Signing Application Service Component Practice Statement (SSASC CP) as per ETSI TS 119 431-1. Additionally, This CP/CPS describes the organizational and technical measures applied by BENEFIT, as the TSP, for the fulfillment of the requirements of components supporting the AdES digital signature creation service (SCASC) to provide the remote electronic signature service as per ETSI TS 119 431-2.

BENEFIT, by providing a remote electronic signature service, acts as a service provider providing a server signing/remote signing application (SSASP), and a service provider providing a signature creation/remote signature creation application (SCASP).

In all phases of their life cycle. The Subscribers, the owners of such a certificate, will be able to authenticate during an identification process performed by the registration authority of BENEFIT

to, digitally sign electronic messages, documents or forms, thus ensuring their origin, integrity, and non-repudiation. Implementation of this certificate is provided by an automated service (set of computer servers) duly authorized to use the private key that represents the natural person (Certificate Subscriber).

This CP/CPS complies with the latest versions of the below ETSI standards. Additionally, Section 10(ANNEX 1: REFERENCE DOCUMENTS) provides list of references to technical standards.

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.
- ETSI TS 119 431-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.
- ETSI TS 119 431-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting Advanced Electronic Signature (AdES) digital signature creation.
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements. - Extended Normalized Certificate Policy (NCP+).

The issued certificates respect the X.509v3 standard and their use is dedicated to the electronic signature mechanism for natural persons.

The structure of this CP/CPS is based on the following references: IETF RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, and RFC 3647, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”.

The following next illustrates the value of these Certificates in the case of the electronic signature Service offered by BENEFIT.

1.1.1 Signature Service Description

BENEFIT offers an Electronic Cheque Service, that’s a:

- A paperless cheque
- Negotiable instrument (can be transferred and endorsed)
- Has the same functionalities and feature of the paper cheques
- Same legal power
- Can be issued as post dated
- Valid for 6 months from the date of the cheque
- Can be used as a security or guarantee
- An added service to the market. Customers can use either paper or electronic cheques.

To enable the electronic cheques, BENEFIT provides an electronic signature solution to its business partners (subscribers) who then can be offered an electronic signature certificate for signing purposes of electronic cheques.
E-Cheque solution supports PAdES signatures with LTA (as per ETSI EN 319 142-1), which defines an advanced electronic signature format based on PDF (Portable Document Format). The format allows electronic signing of PDF files only.

The remote signature creation services supports RSA 2048/3072/4096. For the purposes of this CP/CPS the solution supports RSA 2048. Signature format supported is PKCS #1 v1.5/v2.1 (PSS) | v2.1 is used. Hashing algorithm supported is SHA-256 with RSA 2048. The SSASC in place is Cryptomathic Signer 5.1. The remote signing solution supports ETSI TS 119 431-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev, with Normalized SSASC policy (NSCP).

SUPPORTED SIGNATURE CLASSES

The signature structure common to all signature classes consists of the signer's document, the signed attributes that are included in the calculation of the signature value, the signature value, and all unsigned attributes that are also included in the signature.

The E-Cheque signing service provides a signature with time to prove that the signature already existed at a certain point in time. E-Cheque solution supports PAdES signature with Time PAdES-B-LTA as per ETSI EN 319 142-1.

1.2 DOCUMENT NAME AND IDENTIFICATION

1.2.1 Document Name

This document is the CP/CPS of the aiming at issuing signature certificates for natural persons, provide key management and creation or remote digital signatures on remote QSCD.

- Document Name: BENEFIT Trust Services Certificate Policy / Certificate Practice Statement (CP/CPS), Version: 1.1
- Publication Date: 1 July 2021
- BENEFIT Trust Services Website: https://www.benefit.bh/Services/CertificationAuthorityforDigitalCertificates/
- CP/CPS Publication Address: https://www.benefit.bh/MediaHandler/GenericHandler/documents/CertificationAuthorityforDigitalCertificates/CertificatePracticeStatement.pdf
- This CP/CPS is applicable for certificates/signatures issued After 1 July 2021 till next version of this CP/CPS.
- Subscribers and Relying parties must verify the applicable CP/CPS and related documents for the certificate in use by visiting BENEFIT Trust Services Website.
- Related Documents:

- Subscriber Agreement V1.1
  (https://www.benefit.bh/MediaHandler/GenericHandler/documents/CertificationAuthorityforDigitalCertificates/SubscriberAgreement.pdf)
- PKI Policy Disclosure Statement V1.0
  ((https://www.benefit.bh/MediaHandler/GenericHandler/documents/CertificationAuthorityforDigitalCertificates/PolicyDisclosureStatement.pdf))

1.2.2 Identification code

The Private Enterprise Number OID for BENEFIT Company is iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1): 56818:

OID: 1.3.6.1.4.1. 56818.

This CP/CPS is defining the certificates with the following OID: 1.3.6.1.4.1. 56818.1.1.2.1.1. This reference appears in all Signature Certificates for subscribers who receive certificates issued by the BENEFIT CA (cf. section 9.13.2).

Certificate Name	OID
Natural Person Signing Certificate	1.3.6.1.4.1. 56818.1.1.2.1.1

According to the section 5.3 of the ETSI EN 319 411-1, the rules, according to which personal identification certificates BENEFIT are issued, pursuant to rules of NCP+, whose identification code is:

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)

According to the section 5.2, ETSI TS 119 431-1, the rules, according to which BENEFIT implements signing solution which operates remote QSCD for remote digital signature creation on behalf of the signatory, pursuant to rules of Normalized SSASC policy (NSCP) SSASC Policy whose identification code is:

itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops(1) policy-identifiers(1) normalized (2)

According to the section 4.2.2, ETSI TS 119 431-2 , the rules, according to which BENEFIT implements the service component supporting AdES digital signature creation (signature creation application service component) Policy is:

itu-t(0) identified-organization(4) etsi(0) CREATION SERVICE-policies(19431) ades (2) policy-identifiers(1) eu-advancedx509 (2)

1.3 PARTICIPANTS

The functional decomposition of the BENEFIT trust services which is used in this CP/CPS is as follows:

- **Root Certification Authority (Root CA)- The trust anchor for BENEFIT PKI.** ALMERYS ROOT CA is not connected to any network and is only started when required. The Root-CA only issues certificates for subordinate Certificate Authorities (CA).
- **BENEFIT Certification Authority (BENEFIT CA) - Certificate Generation/Issuance Function))** – This function generates Subscriber Certificates based on the information transmitted by the Registration Authority and the Subscriber's public key from the Subscriber's secret elements generation function responsible for the creation of the Subscriber's key pair. Within the scope of this CP/CPS, the keys are generated on a cryptographic device.
- **Subscribers -** The Subscriber is a natural person who has been issued a valid certificate From BENEFIT CA and is owner of the issued certificates (Certificate Holder and Signatory.
- **Governance Authority (GA)** - The Governance Authority (GA) is the responsible authority for all the services of the BENEFIT PKI and Trust Services.
- **Registration Authority (RA)** - The Registration Authority (RA) is a collection of resources (computer and human) aiming at managing the relationship between the CA and the Subscriber. The RA verifies the identity of the future Certificate holder (Subscriber), and possibly other specific attributes, before transmitting the corresponding request to the PKI function (CA). It is also responsible, where necessary, for Subscriber re-verification BENEFIT renewal of his/her Certificate. Within the framework of this CP/CPS and scope of E-Cheque service, BENEFIT acts as a registration authority and ensure identity registration and verification.
- **Relying Parties -** A Relying Party means an individual or legal entity who relies on the remote electronic signature certification service provided by BENEFIT.
- **Server Signing Application Service Provider – SSASP** – BENEFIT E-Cheque and supporting services implements and manages a service for remote advanced signature. Certificates for remote signing service are issued and managed by Benefit CA.
- **Other Participants**
-

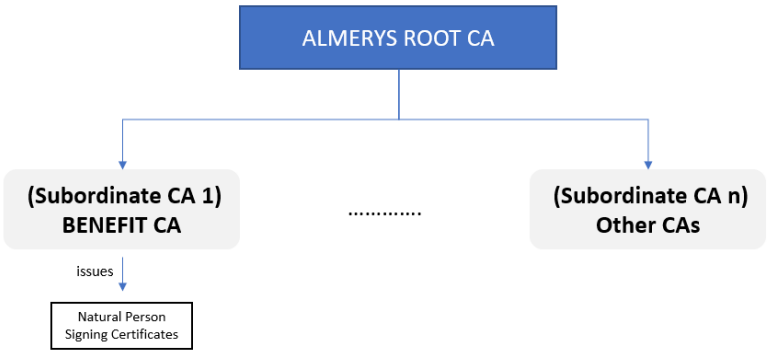
1.3.1 Root-CA

The ROOT CA is not connected to any network and is only started when required. The Root-CA only issues certificates for subordinate Certificate Authorities (CA).

1.3.2 BENEFIT Certification Authority (BENEFIT CA)

The Certification Authority (CA) "BENEFIT CA" oversees the provision of services for Certificates throughout their lifecycle (generation, diffusion, renewal, revocation). Therefore, the CA is identified as the issuer within the Certificates. BENEFIT CA issues for natural persons. Meets the requirements of certificates for advanced electronic signatures for natural persons.

BENEFIT CA is a subordinate CA signed by ALMERYS ROOT CA
http://pki.almerys.com/root/almerysrootca/certificatePolicy/almerysrootca.pdf)



PKI hierarchical model

BENEFIT CA issues certificates to natural and persons for use within the E-Cheque system purposes.

BENEFIT CA provides the following additional functions:

- **Publication Function -** This function publishes the CA's policies, certificates, and any other relevant information available to the different parties, Clients/carriers and/or Applications using certificates, excluding status information of the certificates. The complete list of Valid Subscriber Certificates is not publicly available. Transmission to the Subscriber s of the general terms and conditions of use of the Certificates is carried out through authentication process. The creation of this form and the signature of the latter by the Subscriber is made during the secure identification process with the Registration Authority.
- **Revocation Management Function -** This function of BENEFIT CA handles revocation requests (including identification and authentication of the applicant) and determines the actions to be carried out. The processing results are published via the certificate status information function.
- **Certificate Status Information Function -** This function provides information on the status of the certificates (revoked, suspended, etc.) to applications using the issued certificates.
- **Time Stamp Authority (TSA)** - BENEFIT uses the following Time Stamp Authority (TSA) as provide for time stamps: BE INVEST TIMESTAMP UNIT 10 (https://pki.be-ys.com/horodatage.html)

1.3.3 Subscribers

The Subscriber is a natural person who submitted a valid certification services application, and upon approval has been issued the certificate and became the owner of the issued certificates (Certificate Holder). The Subscriber (Signatory) is a user of the remote electronic signature provided by BENEFIT. The Subscriber has the sole control over the use of the data related to the creation of its electronic signature in accordance with this CP/CPS.

1.3.4 Governance Authority (GA)

The **Governance Authority (GA)** is the responsible authority for all the services of the BENEFIT PKI and Trust Services. This authority has decision-making power within the PKI. It defines and validates the CP/CPS. Concretely, it is one or more representatives of BENEFIT with a specific mandate to ensure this function.

1.3.5 Registration Authority (RA)

The Registration Authority (RA) is a collection of resources (computer and human) aiming at managing the relationship between the CA and the Subscriber.

the RA ensures:

- the information verification, in particular personal information, presented by the future certificate holder (Subscriber), and the filing of his registration record;
- the preparation and transmission of the Certificate Application to the appropriate function of the BENEFIT CA;
- the archiving of the documents in the registration record (or sending to the component responsible for archiving);
- the preservation and protection in privacy and integrity of the Subscriber r entrusted personal data (in particular, it complies with the legislation on the protection of personal data). This is ensured when exchanging such data with the other functions of the PKI.

At a minimum, BENEFIT requires from its Registration Authorities that:

- Verification of applicant identity for a certificate shall follow the BENEFIT identification process and be compliance with central Bank accepted identity verification. The subscriber is aware of and signs the certificate's General Terms and Conditions "Subscriber Agreement Terms & Conditions V1.1".

The RA therefore establishes the procedures necessary to ensure this level of assurance and ensures its operational implementation.

1.3.6 Relying Parties

A Relying Party means an individual or legal entity who relies on the remote electronic signature certification service provided by BENEFIT. The current e-cheque environment including trust services are totally owned and managed by BENEFIT. Only registration services done by other entities (Banks).

Since this CP/CPS is dealing with signature certificate of a natural person, a relying application is an application that aims either at:

- Consuming digital certificates;
- Verifying an electronic signature;

Both of the above-mentioned applications are provided through e-Cheque system which is owned by BENEFIT. For example these applications include (but are not limited to):

- the BENEFIT signature verification service or an BENEFIT partner that allows information or a document or E-Cheque signed with a certificate issued by the BENEFIT CA, to verify and display the status of the used certificate or signature.
- the Adobe™ Acrobat Reader ™ application that allows to view a document in PDF format signed by a certificate issued by the BENEFIT CA, as well as the cartridge of information about the signatures associated with the document. This application must be configured to accept CA certificates of BENEFIT CA.

Relying Parties shall have knowledge and skills regarding the use of the certificates and signatures. Replying parties shall:

- Rely on this CP/CPS on the circumstances and restrictions of using BENEFIT certificates and digital signatures.
- Rely on this CP/CPS regarding the restrictions of using the certificates and signatures
- Maintain a permanent access to the BENEFIT repository ad certificate status services to verify the validity of the qualified certificates.
- Validate the certificate path
- Ensure that the key is appropriate for the intended use as set forth in this CP/CPS and that such use is consistent with the applicable certificate content including, but not limited to, the key usage, extended key usage, certificate policies extension fields
- Check the status of the certificate in accordance with the requirements stated in Section 4.9.6 of this CP/CPS. As part of the validation process, the authenticity of the revocation must be validated as follows:
    - In case of using CRLs, the digital signature of the CRLs is validated
    - In case of using OCSP, the digital signature of the OCSP response is validated

- Ensure that reliance was reasonable and made in good faith in light of all the circumstances that were known or should have been known to the relying party at the time of reliance
- If a party relying on the BENEFIT trust services accepts a certificate or signature that cannot be validated through the BENEFIT CA OCSP or CRL, it decides to do so completely at it's own risk.

1.3.7 Server Signing Application Service Provider – SSASP

BENEFIT E-Cheque and supporting services implements and manages service for remote advanced signature. Certificates for remote signing service are issued and managed by Benefit E-Cheque environment. BENEFIT E-Cheque service provides the following services:

- Signing key generation service – generates signing keys in the remote device. The proof of possession of generated signing keys are passed to the E-Cheque identity management system.
- Certificate linking service - links the certificates generated by the E-Cheque Service with the corresponding signing keys and users.
- Electronic ID means linking service - links Electronic ID means references with the corresponding signing keys in order to provide sole control. Only Benefit user registered Electronic ID means are used.
- Signature activation service - verifies the signature activation data and activates the corresponding signing key in order to create a digital signature.
- Signing key revocation service – revokes signing keys certificates in a way that ensures that the signing keys cannot be used anymore.
- Electronic ID means provision service –makes Electronic ID means available to the signers. Only Benefit Identity registered two-factor Electronic ID means are used.

1.3.8 Other Participants

1.3.8.1 Trusted Service Provider Operator (TSPO)

The BENEFIT delegates to its Trusted Service Provider Operator the set of tasks of:

- Defining the technical infrastructure of the PKI and signing solution;
- Ensuring the configuration and administration of the PKI and signing solution components
- Ensuring operation, maintenance in operational condition and supervision of components.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

1.4.1.1 Natural Person Signing Certificate

(OID: 1.3.6.1.4.1. 56818.1.1.2.1.1)

Certificates issued by BENEFIT CA are electronic signature certificates in compliance with ETSI EN 319411-1 NCP+. These certificates are used by natural person to generate Advanced Electronic Signature in remote mode. This CP conforms to the following standards::

- ETSI EN 319 401,
- ETSI TS 119 431-1,
- ETSI TS 119 431-2, and
- ETSI EN 319 411-1 - Extended Normalized Certificate Policy (NCP+)

The issued certificates may be used by Third Parties application for verifying electronic signatures. These applications are under the responsibility of BENEFIT or its clients within the E-Cheque platform.

These certificates can be used only for signing purposes by the Subscribers to sign documents provided by BENEFIT or BENEFIT business partners.

Persons and relying parties should be aware of the rules of use of the signing certificate:

- Natural personal signing certificate is a certificate for electronic signature, which meets requirements set out in ETSI EN 319 411-1 - Extended Normalized Certificate Policy (NCP+).
- The issuer of the natural personal signing certificate is a licenced trust service provider, and which had been granted the status by the supervisory body in Kingdom of Bahrain.
- An external auditor performed the conformity assessment of the trust service provider in order to confirm the fulfilment of the requirements of the above-mentioned standards.
- The natural personal remote signing certificate is issued by E-Cheque through a service on the remote QSCD, which is a qualified electronic signature creation device.
- The natural person, certification subject, is named in the personal signing certificate and this person uses it for private and for business purposes within E-Cheque platform.

1.4.1.2 CA or Components Certificates and Key Pairs

The BENEFIT CA Certificate and Key Pair cannot be used for a purpose other than for the signature of end-user Certificates and CRL.

Key pair and Certificates of the BENEFIT CA are only used for:

- Issuing certificates for end-users
- Issuing CRL
- Optionally issuing certificates for OSCP servers.

1.4.2 Prohibited Certificate Uses

Any usage that is not explicitly described in the above section is prohibited.
Persons and relying parties must be aware of the limitations concerning the certificate's use:

- Certificates are not intended for data encryption.

The signing certificate may not be used for any other purpose other than to support the advanced electronic signature

1.5 POLICY ADMINISTRATION

1.5.1 Organization Managing the Document

The entity responsible for the administration and management of the certification policy is the GA. The GA is responsible for the development, monitoring, and modification of this CP/CPS as soon as necessary. To this end, it implements and coordinates a dedicated organization, which decides at regular intervals on the need to make changes to this CP.

1.5.2 Contact

The GA is the entity to contact for any questions concerning this CP.

Riyad AlMearaj | Assistant General Manager
The BENEFIT Company
Kingdom of Bahrain / Manama
P.O.BOX 2546
Phone: +973 17 500414
Fax: +973 17 500401
Email: riyadm@benefit.bh

1.5.3 Entity Determining CPS Suitability for The Certificate Policy

To determine the suitability of this CP/CPS, the GA must review and approve any changes to this document before publication. In addition, BENEFIT relies on internal or external audit specialists specialized in auditing and evaluating the suitability of this CP/CPS.

BENEFIT has implemented several approval phases in every pre-publishing phase of this CP/CPS, ensuring a high quality of CP/CPS content and in minimum at least a four eyes

principle before a new version of this CP/CPS may be published. This is achieved through the review by the GA and approval from same committee before publication.

Since BENEFIT is also acting as the RA then the GA also ensure practices performed by the RA is in conformity to this CP/CPS.

1.5.4 CP/CPS Approval Procedure

The approval of the compliance of the CP/CPS is an internal procedure. The GA is responsible for the management (updating, revision) of the CP/CPS. Any request to update the CP/CPS must be submitted to the GA for approval before the change takes place.

CP/CPS modification approval may follow a formal procedure targeting the scope of the CP/CPS concerned by the modification.

The procedure to update and secure approval of the CP/CPS is described as follows:

- The Updated CP/CPS is submitted to the GA
- The function/unit that is requesting the change present the scope of changes to the GA
- The GA reviews the changes and consult with internal and external parties (RA, Service Provider, Application Teams, Banks, etc) if needed
- GA approves or disapproves the change
- IF approved, the CP/CPS is updated, and the new version is published.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Acronyms

ARL	Authority Revocation List
CA	Certification Authority
CC	Common Criteria
CEN	Comité Européen de Normalisation [European Standardisation Committee]
CO	Certification Operator
CP	Certification Policy
CPS	Certification Practice Statement
CR	Certification Representatives
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
DN	Distinguished Name
EAL	Evaluation Assurance Level
ETSI	European Telecommunications Standards Institute
GA	Governance Authority

HRA	Head of Registration Authority
HSM	Hardware Security Module
KC	Key Ceremony
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OR	Organization Representative
PP	Protection Profile (PP)
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure – X.509
RA	Registration Authority
RSA	Rivest Shamir Adelman
SPC	Single Person Company
TA	Time-stamping Authority
TSP	Trust Service Provider
URL	Uniform Resource Locator

1.6.2 Definitions

Third Party Applications:
Application services using Certificates issued by the CA, for example, for electronic signature or signature verification purposes.

Authentication:
Action aiming at verifying the identity of a natural person or/and the origin of a communication.

Certificate Authority (CA):
Entity issuing certificates and which is responsible for the electronic Certificates Issued and signed on its behalf in accordance with rules defined in its CP/CPS.
Note:
The CA may operate itself its own infrastructure or have it managed by a Certification Services Operator (CSOs or CO) with secure facilities, staff, and technical infrastructure to enable it to perform all the certificate management tasks on behalf of the CA.

Root Certification Authority (RCA):
An entity that has a PKI enabling it to register, generate, issue and revoke Certificates for CAs, in accordance with own CP/ CPS defined by its GA.

Registration Authority (RA):

An entity with a set of resources (IT and human resources) to manage the relationship between CA and Certificate Holders in accordance with paragraph 1.3.5 of this CP. The role of the RA is to verify the identity of the future Certificate Holder.

Governance Authority (GA):
Entity responsible for all functions of the BENEFIT PKI with decision-making authority.

Key Pair:
Public key / private key couple.

Key Ceremony (KC):
Special meeting of authorized persons to generate the CA or Client Certificate (KC Client). The key pair of this Certificate must be generated with all necessary precautions (see CPS) to avoid any compromise.

Digital Certificate:
Electronic file attesting that a key pair belongs to the natural person or to the material element identified, directly or indirectly (pseudonym), in the Certificate. This file is issued by a CA. By signing the certificate, the CA validates the link between the identity of the physical person or the material element and the key pair. The Certificate is valid for a specific period specified in it.

Encryption:
Cryptographic transformation of a (clear) data set to produce an encrypted set (called cryptogram).

Client:
A client is an entity that has decided to subscribe to the BENEFIT Service for its own purposes or in a way to make the service available to its own customers.

Component of the PKI:
A platform operated by an entity consisting of at least one computer station, an application and, where appropriate, a means of cryptology and playing a determined role in the operational implementation of at least one function of the PKI.

Confidentiality:
Property of information or resource to be accessible only to authorized users (creation, dissemination, backup, archiving, destruction).

Decryption:
Transformation of a cryptogram to retrieve the original data in plain text.

Certification Practice Statement (CPS):
A document that identifies the practices (organization, operational procedures, technical and human resources) that a CA applies in the provision of its electronic certification services to and in compliance with the PC(s) it has undertaken to comply with.

Timestamping:

A service that reliably associates an event and a time to reliably establish the time at which that event has occurred.

Public Key Infrastructure (PKI):
A set of components, functions, and procedures dedicated to the management of cryptographic keys and their Certificates used by trusted services. A PKI can be composed of a CA, a CO, a centralized and / or local RA, a CR, an archiving entity, a publishing entity.

Integrity:
Property of accuracy, completeness, and inalterability over time of the information and functions of the processed information.

List of revoked CA certificates (ARL)
A list of revoked CA certificates that have been revoked before the end of their period of validity.

Certificate Revocation List (CRL):
A list of revoked end-user certificates that have been revoked before the end of their period of validity.

Hardware Cryptographic Module (HSM):
An electronic hardware providing a security service consisting of generating, storing and protecting cryptographic keys.

Online Certificate Status Protocol (OSCP):
A protocol that allows a person or an application to verify the validity of a certificate in real time, especially if it has been revoked.

Non-repudiation:
Impossibility for a Holder, User or User Application to deny participation in an exchange of information; this participation concerns both the origin of information (accountability) and its content (integrity).

PKIX (Public Key Infrastructure – X509):
IETF (Internet Engineering Task Force) working group aiming to facilitate the development of PKIs based on the X.509 standard for internet applications. PKIX has produced standards such as X.509 extensions for the Internet, OCSP, etc.

Certificate Policy (CP):
A set of rules, identified by a name (OID), defining the requirements that a CA follows in setting up and providing its services and indicating a Certificate's applicability to a particular community and/or a class of applications with common security requirements. A CP/CPS may also, if necessary, identify obligations and requirements for other stakeholders, including Holders and Third-Party Applications.

Subscriber:

A natural person that is registered in E-Cheque Service and is requesting to be a certificate holder.

Certificate Holder (Subject)/Subscriber: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.

Security product:
Software and/or hardware device, which is required to implement security functions securing dematerialized information (during an exchange, processing and/or storage of this information). This generic term covers electronic signature devices, authentication devices and confidentiality protection devices.

Application developer:
Supplier of a secure service offer (dematerialized exchanges).

Customer Representative:
An individual who has a contractual/hierarchical/regulatory relationship with the client entity and is the representative of the legal entity identified in the Certificate.

Head of Registration Authority (HRA):
Individual in charge of the RA.

BENEFIT Service:
One of the digital trust services provided by BENEFIT, that may be partially or completely deployed.

Electronic signature or Signature:
"Use of a reliable identification process guaranteeing its connection with the act to which it relates", in accordance with the French Civil Code.

Uniform Resource Locator (URL):
A website address.

User:
See « Third Party Application»

2 PUBLICATIONS AND REPOSITORY RESPONSIBILITIES

2.1 IDENTIFICATION OF ENTITIES OPERATING REPOSITORIES

For providing availability the published information to Subscribers and Applications that use certificates and to Certificate Holders, the BENEFIT CA implements a publication function and a certificate status information function.

The provision of certificate status information is based on an CRL and OCSP mechanisms. Publication addresses are provided in Section 7 « CERTIFICATES, OCSP And CRL Profiles ».

CP/CPS modification approval may follow a formal audit procedure targeting the scope of the CP/CPS concerned by the modification. The procedure of update and approve of the CP/CPS is described in section 1.5.4.

2.2 INFORMATION TO BE PUBLISHED

BENEFIT publishes the following information on its PKI and Trust Services website:
https://www.benefit.bh/Services/CertificationAuthorityforDigitalCertificates/

- This CP/CPS, which contains, in particular, the certificate and CRL profiles, the delays and frequencies of publication, the glossary containing acronyms and applicable definitions, main publication addresses);
- PKI Disclosure Statement;
- The Subscriber Agreement (Terms & Conditions) for the use of the Certificates and trust services.

The BENEFIT CA publishes the following information on the site:
https://pki.almerys.com/BENEFITca.cer
https://pki.almerys.com/BENEFITca.crl

The repositories are available 24/7. In the event of a system failure, service failure or any other factors beyond the control of BENEFIT, the best practices will be applied to ensure that the E-Cheque PKI and trust services disruption or non-availability is no longer than the maximum period allowed, as defined in the Terms and Conditions (incl. SSASC and SCASC).

The initial publication procedure of the documents named above is generally orientated on the main approval process of BENEFIT, as described in Section 1.5.3. A Difference occurs in additional review and approval steps of external experts and auditors before its initial publications.

The PKI and Trust Services website is made available to the public, with the following information:

- Rules for providing certification services and certification practices procedure (Certificate Policy (CP) and Certificate Practice Statement for PKI and SSASC), both included in this document
- PKI Policy Disclosure Statement (PKI PDS)
- Terms and Conditions for PKI and Trust Services
- Announcements and other information relevant to Subscribers and relying parties
- Contact information for user support.

2.3 TIME OF FREQUENCY OF PUBLICATION

For the CP/CPS, publication is effective as soon as necessary to always ensure between the published information and the actual commitments, means and procedures of the CA. The valid CP/CPS is published before the first creation of a Subscriber certificate.

CA certificates are published at least 72 hours prior to any corresponding issuance of any Subscriber certificates and/or CRLs.

Certificate status information, *i.e.*, the Revoked Certificate Lists, is updated within a maximum of 24 hours. Once the update is complete, the CRL is published within a maximum of 60 minutes.

Time of frequency of publication depends on the type of information:

- CP and CPS are published as soon as the document is validated, and in a maximal delay of 72 opening hours after the formal validation of documents. The valid CP/CPS is published before the first transmission of a Subscriber certificate.
- CA certificates are published 72 hours prior to any corresponding transmission of certificates and/or CRLs.
- In case of revocation of a Subscriber certificate, a new CRL is generated by the CA. In absence of revocation for 24 hours, the CRL is automatically updated.
  - Upon generation, a CRL is sent to the publication service within a maximum delay of 30 minutes.
  - After receipt by the publication services, the CRL is published within a maximum delay 30 minutes.

Certificate status information, *i.e.*, the Revoked Certificate Lists, is available 24/7.

2.4 ACCESS CONTROL TO PUBLISHED INFORMATION

The level of confidentiality of all information published is the «public distribution».

The publication function and the certificate status information function ensure the integrity of the published information.

Modification access to publishing systems (addition, deletion, modification of published information) is strictly limited to the authorized internal functions of the CA BENEFIT CA, and to persons duly authorized after authentication by strong authentication means.

Published information is available to third parties on read-only mode. All other operations such as adding, deleting, modifying, or updating information is only allowed to authorized person or system of the BENEFIT CA.

The right management of the repository and in particular the list of people authorized to perform such operation is described within BENEFIT's "BCTS and E-Cheque Roles and Responsibilities" document under the BENEFIT CA part.

3 IDENTIFICATION AND AUTHENTIFICATION

3.1 NAMING

3.1.1 Types of Names

The names used in the Certificates issued by BENEFIT CA comply with the specifications of X.500.
Each entity is identified by a "Distinguished Name" (DN), within the subject field of the certificate. This DN allows distinguishing a subject easily to one another and this DN is unique for a given CA.

In each X.509v3 Certificate, the issuing CA and the Subject (Subscriber and/or the Holder) are identified by a "Distinguished Name" (DN). The format of the DN is specified in section 7 « CERTIFICATES, OCSP And CRL Profiles ».

DN is encoded in printable string or Utf8string may use specific ARABIC characters and is not empty.

3.1.2 Need for Names to be Meaningful

BENEFIT CA issues certificates to natural person (private or associated with an organization), in the case of “professional use” certificates, the management of the signer attribute (role, organisation, etc..) are managed by E-Cheque application, and not by the BENEFIT CA.

This information is written in the "Subject" field of the DN.

"Natural person" certificate, the Subscriber's identity information is explicit and corresponds to the elements presented on the Subscriber's proof of identity provided at the time of the certificate request during the registration process. This information is written in the "Common Name" field of the DN.

The SerialNumber field is used for the DN unicity guaranty in the domain of the present CA application.

The exact format of the "Subject DN" of the Holder’s Certificates is specified in Section 7 « CERTIFICATES, OCSP And CRL Profiles ».

3.1.3 Anonymity or Pseudonym of Subscribers

Certificates of the Holders cannot be anonymous. The use of a pseudonym is prohibited.

3.1.4 Rules for Interpreting Various Name Forms

The rules for interpreting the various forms of names are explained in Section 7 CERTIFICATES, OCSP And CRL Profiles describing the profile of Certificates and CRLs. Names are explicit and therefore no specific rules are needed to interpret the various name forms.

3.1.5 Uniqueness of Names

BENEFIT maintains a repository identifying on a unitary basis each of the Certificate Subscriber issued by the BENEFIT CA.

This identifier is an integral part of the DN of a certificate and is in accordance to ETSI 319 411-1 in the field “SERIALNUMBER”.

BENEFIT ensures that this identifier cannot be assigned to any other Holder.

It should be noted that the uniqueness of a Certificate is based on the uniqueness of its serial number within the CA domain but that this number is specific to the Certificate and not to the Subscriber and therefore does not ensure a continuity of the identification in the successive Certificates of a given Subscriber.

3.1.6 Recognition, authentication, and role of trademarks

The RA ensures as much as possible the suitability of the names and trademarks appearing in a certificate application, in particular information relating to the company in the case of a « business » certificate.

3.2 INITIAL IDENTITY VALIDATION

Registration of a certificate application is made directly by the Registration Authority. The identity of the future holder (Subscriber) must be verified in a secure identification process with the registration authority.

The registration authority must be trusted and authenticated by the CA; in particular, BENEFIT as the registration authority has implemented all the necessary security measures through regular reviews administered by the GA.

The practical procedures for validating the identity of the Subscriber are defined by BENEFIT. The operational implementation of these modalities remains the responsibility of BENEFIT and Identity Providers but must guarantee the elements mentioned in paragraph 1.3.3.

BENEFIT CA issues certificates to the following types of Subscribers:

- Natural Person with a unique identifier linking his/her KYC data and profile with the E-Cheque

System.

The E-Cheque System manages the profile and the authorized IBANs the Subscriber has access to be an Electronic Transferable Record Management Information System (ETRMIS) as defined in the Resolution Number 13 of 2020 regarding the regulation of Operating Electronic Transferable Cheques.

A Natural Person with Automated Registration with The Bank:

- A natural person representing himself/herself can self-enrol as his/her identity is verified and authenticated with the Bank in automated process. Only customers maintaining active Bank accounts with previous face to face KYC with their Banks, can register using BenefitPay.
- The Subscriber uses BenefitPay for registering current account to issue E-Cheques or other accounts for deposits.
- Request sent from BenefitPay to the Bank.
- The Bank validates the data and authenticates the Subscriber using OTP/OAUTH.
- BenefitPay only allows the customer using the same registered device (in the first step) to key in the OTP sent by the Bank.
- Bank validates the OTP “Accept/Reject” in real time.
- If OAUTH is used, the Subscriber is directed to Bank’s OAUTH interface for authentication. Based on successful authentication by the Bank, the Subscriber registration is complete at BenefitPay.
- BenefitPay sends the registration information to the E-Cheque system.
- E-Cheque system subscribes the customer to the Certification Authority.

A Natural Person with Face to Face KYC with The Bank:

- Any account relationship that has more than authorized signatory or its KYC cannot be validated with the Bank using the above defined method on BenefitPay, shall be registered by face-to-face KYC with his/her Bank.
- Banks will depend on face-to-face KYC for registration in the E-Cheque Service and the Certification Authority in the below conditions:
  - Acting as an authorized signatory for registered entity in E-Cheque Service.
  - Having more than one authorized signatory over the same IBAN. For example, joint accounts and power of attorney.
- The Subscriber submits the request to its bank.
- Subscriber can register their current account to issue E-Cheques or other accounts for deposits.
- All branches / account officer(s) must be able to receive the request.
- Banks can enable their online channels to receive requests instead of branches.
- All branches and call centre staff must be aware which channels customers can use for

registration requests.

- The bank shall allow any customer able to request paper cheque books to register in the E-Cheque Service and Certification Authority.
- The Bank will send the customer information to the E-Cheque System.
- Authorized Signatory Activation:
- The authorized signatories will download the E-Cheque mobile app to activate his/her account.
- The authorized signatories will provide the system with his/her information:
- Identity type (Enterprise, joint, etc)
- Signatory ID
- Bank
- Corporate ID
- After successful validation of the authorized signatory data and credentials, the system will generate OTP and based on successful OTP validation the user will be activated.

3.2.1 Method to Prove Possession of Private Key

The key generation and the certificate issuance operations occur only after identifying the user at the Registration Authority. A proof of possession of the private key is not required, because the key pair is generated on behalf of the certificate holder by the CA Services. Delivery of certificate and control over the private key is confirmed by signatory in E-Cheque service by activating the key with previously set PIN.

Private keys of the natural personal signing certificates used for remote signature are generated in the HSM device and are entered on to a qualified electronic signature creation device (QSCD) operated by the BENEFIT as Trust Service Provider through a TSPO signing service. The remote HSM device is QSCD device and meets the requirements set out in ISO IEC 15408 Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5

Private keys and natural personal signing certificates used for remote signature are generated only if the Subscriber is authenticated and authorized. Authentication is with BENEFIT E-Cheque Platform uses two-factor authentication means registered in BENEFIT E-Cheque platform. Upon complete registration Subscribers are forced to generate a PIN to be used for private key activation before creating the digital signature to ensure Subscriber control of the private keys.

3.2.2 Authentication of Organization Identity

No Stipulation.

3.2.3 Authentication of Natural Person Identity

The validation of the identity of the certificate Subscriber is necessarily carried out through multiple steps depending on the type of the subscriber. Face-to-face or equivalent mechanisms are used to authenticate the subscriber when registering the subscriber and before issuing any certificates.

3.2.3.1 Online Registration for a « Natural Person » Certificate

For obtaining a "natural person" certificate, the validation of the identity of the Subscribers is performed as follows:

- Individual user “natural person” must be registered at a recognized Bank in Kingdom of Bahrain following KYC process that is in line Central Bank of Bahrain guidelines and regulations, which is based on face-to-face validation of identity.
- When the Subscriber wants to issue E-Cheque he/she must register on BenefitPay service which sends an identity validation request to the Subscriber’s Bank.
- The Bank challenges the Subscriber by sending OTP to the Subscriber registered phone at the Bank.
- If the Subscriber provides the correct OTP, BenefitPay completes the registration of the user and allows him/her to use E-Cheque service and at that moment BenefitPay requests the Subscriber certificate after he/she accepts the Subscriber Agreement Terms & Conditions V1.1.

3.2.3.2 Offline Registration of a "Natural Person" Certificate

When the natural person is acting as an authorized signatory for a commercial registered entity, non-governmental organisations, or a governmental entity; the validation of the identity of the Subscriber is performed as follows. Moreover, the same is as well applicable to accounts of natural person having more than one authorized signatory such as joint accounts and power of attorney.

- The entity registers with the Bank
- Provide all required documentation that confirms the legal status of the entity
- Register the authorized person with the bank with his personal info
- Once registration is completed, the authorized person downloads E-Cheque application and start registration process
- E-Cheque will validate the identity against the data registered by Bank
- If the authorized person validates his/her identity successfully and accepts terms and conditions (Subscriber Agreement Terms & Conditions V1.1), E-Cheque service requests his/her digital certificate.

3.2.4 Non-Verified Subscriber Information

Not applicable in the scope of this CP/CPS.

3.2.5 Criteria for Interoperation

Recognition agreements with CAs outside the BENEFIT's security domain is the responsibility of the Root CA "ALMERYS ROOT CA."

3.3 Identification and Authentication for Re-Key and Update Requests

The renewal of the signature key pair of the Client automatically results in the generation and provision of a new signature Certificate and a new associated key pair.

Verification of identity in the context of a key renewal is the same as the initial registration. A new Certificate cannot be issued to the Client without renewal of the Certificate Holder's key (see Section 4.6 Certificate Renewal).

3.3.1 Identification and Authentication for Routine Re-Key and Update

In the case of renewals, the RA must identify the Client according to the same procedure as for the initial registration, a new certificate application record is then implemented, and a new activation code will be given to the Holder.

3.3.2 Identification and Authentication for Re-Key After Revocation

In the case of renewals, the RA must identify the Client according to the same procedure as for the initial registration, a new certificate application file is then implemented, and a new activation code will be given to the Holder.

3.4 Identification and Authentication for Revocation Request

3.4.1 Request Originated by the Holder, or the Subscriber

Subscribers can deactivate their user accounts on E-Cheque service by contacting all Banks he/she has a relationship with. Once the Subscriber has been deactivated on the E-Cheque Service from all the Banks, meaning no existing relationship with the Subscriber is active, E-Cheque will automatically revoke the Subscriber certificate. If the Subscriber decides to reactivate, he/she shall ask all Banks he/she has relationship with to reactivate his/her profile in E-Cheque. The Subscriber will receive new certificate.

3.4.2 Request Originated by the RA

NA

3.4.3 Request Made by the Support Centre

In case of the mobile device holding BenefitPay or E-Cheque Application is compromised, the Subscriber can download the application from another device and login from the new mobile device. BenefitPay and E-Cheque Application will deactivate the old device after successful login. If the Subscriber wants to revoke the certificate, the Subscriber shall contact the call center of all banks he/she has relationship with and request to deactivate his profile on E-Cheque.

3.4.4 Request From the CA or GA

In case of emergency, the Certification Authority or the Governance Authority may revoke a certificate.

- The CA, or GA send revocation request to certification service operator. Then the Certification service operator Authorized personnel connect to the PKI interface, research of the certificate to be revoked, and start the revocation operation of the selected certificate.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 Origin of an Application for a Certificate

See sections 3.2.3.1 Online Registration for a « Natural Person » Certificate and 3.2.3.2 Offline Registration of a "Natural Person" Certificate

4.1.2 Enrolment Process and Responsibilities

The applicant is responsible for the information and evidence provide to the Registration Authority. Based on this information, the RA:

- completes the application form as defined in section 3.2 Initial Identity Validation.
- validates the submitted evidence.
- ensures applicant signs the application form and the Terms and Conditions.
- validates the request and triggers the technical procedures for requesting a certificate.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Implementation of the Identification Process and Application Validation

The Registration Authority must validate the identity of the applicant by ensuring the consistency of the evidence presented. It validates the provided Subscriber information with the registered bank that manages the user account.

The registration procedure and the steps to validate the certificate are described in CA internal procedures.

4.2.2 Acceptance or Rejection of Application

See section 3.2 Initial Identity Validation for registration and validation process.

4.2.3 Time to Process Certificate Application

Once the application form is validated by the Registration Authority, the key pair generation and certificate issuance is triggered. This phase is carried out by the Registration Authority.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance.

On a certificate request, the RA triggers the following processes:

- Generating a key pair on the QSCD;
- Generating certificate request for the PKI;
- Signature of the Certificate Holder's public key by the BENEFIT CA;
- Installing the certificate on the QCSD.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The Subscriber will receive a pop-up message from BenefitPay or E-Cheque, depending on Subscriber type, notifying him/her that registration is completed. Registration process cannot be completed before certificate is issued. If, for any reason, the certificate is not issued then the registration process will not be considered as completed and Subscriber must try to register again.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

The BENEFIT CA consider that the no complaint about the content of the certificate within 24 hours by the holder as an implicit acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

Signature certificates are not published.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.5 KEY PAIR AND CERTIFICATE USAGE

The private key can be used for signing a document.

Relying parties can use the certificate contained in the signed document to verity the validity of the signature.

4.5.1 Subscriber Private Key and Certificate Usage

The use of the Subscriber's Private Key and the associated Certificate is strictly limited to the usage that described in paragraph 1.4.

The authorized use of the Subscriber's key pairs, and the associated Certificate is specified in the Certificate itself, via extensions concerning the uses of the keys (see Section 7.2 Natural Person Signing Certificate) for details of the Certificate profile.

The use of Electronic Certificate necessarily requires the use of the QSCD provided by the BENEFIT for the signature to be declared in conformity with EN 319411-1 NCP+.

The Subscriber must strictly respect the authorized uses of the key pair and the Certificates. Otherwise, their liability would be incurred.

In general, any unauthorized use is prohibited.

4.5.2 Relying Party Public Key and Certificate Usage

See previous sections 1.4 «Certificate Usage» and 1.3.6 «Relying Parties» .

Applications using certificates must strictly respect the authorized usage of the Certificates.

Otherwise, their liability may be incurred.

4.5.3 Root CA Public Key and Certificate Usage

Root CA private key is used to sign:
- Sub CA certificates
- ARL (Authority Revocation List).

Root CA certificate is used to.
- Verify SubCA certificates
- To verify the origin and integrity of the ARL.

4.5.4 CA Public Key and Certificate Usage

CA private key is used to.
- Sign end-user certificates

- To sign certificates for OCSP servers
- To sign CRL

CA Certificate is used to.

- Verify the issued certificates and the electronic signature generated with the associated Subscriber's private keys.
- Verify the integrity and origin of the issued CRL.
- Verify the integrity and origin of an OCSP server.

4.6 CERTIFICATE RENEWAL

The renewal of a Certificate - i.e., issuance of a new Certificate for which only the validity dates are modified, all other information remaining identical to the previous Certificate (including the public key of the bearer), cf. [RFC3647] - is not permitted in the scope of this CP/CPS.

4.7 CERTIFICATE RE-KEY

A change of key pair may be performed following the revocation of an existing Certificate (see Section 4.9 « Revocation and suspension of Certificates»).

4.7.1 Possible Cause of a Re-Key

Certificate and key-pair validity of holders is not permanent and shall be renewed before expiration of old certificate, or after a revocation.

The possible causes of re-key and Certificate renewal are therefore as follows:

- Valid certificate will expire, or already expire,
- Certificate revocation for any reasons

The E-Cheque System will automatically renew all certificates of active customers on E-Cheque Service. Non-active customers certificates are revoked automatically by the E-Cheque System.

4.7.2 Origin of a Re-Key Application

Same as Section 4.1.1.

4.7.3 Processing of a Re-Key Application

Same as Section 4.2.

4.7.4 Notification of the Issuance of the New Certificate

Same as Section 4.3.2.

4.7.5 Acceptance Procedure for the New Certificate

Same as Section 4.4.1.

4.7.6 Publication of the New Certificate

Same as Section 4.4.2.

4.7.7 Notification by the CA to Other Entities

Same as Section 4.4.3 (first issuance).

4.8 CERTIFICATE MODIFICATION

Certificate modification - *i.e.* modification of certificate information without change of the public key, excluding the modification of validity dates, see [RFC3647] - is not permitted in the scope this CP/CPS.

4.9 REVOCATION AND SUSPENSION OF CERTIFICATES

The BENEFIT CA has implemented a process to revoke Certificates.

4.9.1 Circumstances for Revocation

4.9.1.1 End-User Certificates

The following circumstances may be the cause of revocation of the Holder's Certificates:

- The Certificate has become obsolete due to a change in the Subscriber's information contained in the Certificate.
- The Subscriber’s information (including its title or attribute) no longer complies with the identity or usage of the Certificate.
- The Certificate’s applicable terms of use have not been respected by the Subscriber.
- The Holder, the subscriber, the Registration Authority, or the Certification Authority have not respected their obligations defined by this CP/CPS.
- An error (intentional or not) has been detected in the Certificate application record.
- The Subscriber 's private key is suspected of compromise, is compromised, is lost or is stolen.
- subscriber or certificate holder complaint about wrong content of certificate.

When any of the above circumstances occurs and BENEFIT CA or the Registration Authority becomes aware of it (*i.e.*, it is informed or obtains the information during verification when issuing a new Certificate), the relevant Certificate must be revoked as per section 3.4 Identification and Authentication for Revocation Request.

4.9.1.2 PKI Component Certificates

The following circumstances may result in the revocation of a certificate from a PKI component (this may include a certificate from the BENEFIT CA used for the generation of Certificates and CRL):

- Suspicion of compromise, compromise, loss or theft of the private key of the component.
- Decision to change the PKI component following the detection of a non-conformity of the procedures applied within the component with those announced in the CPS (e.g. following a qualification audit or a non-conformity report).
- End of activity of the entity operating the component.

4.9.2 Origin of a Revocation Request

4.9.2.1 End-user Certificate

See Section Request Originated by the Holder, or the Subscriber

4.9.2.2 PKI Component Certificate

The revocation of a CA certificate can only be decided by the CA's GA or by the judicial authorities via a court decision.

The revocation of other certificate components shall be decided by the entity operating the relevant component, which must notify the CA without delay.

4.9.3 Procedure for Processing a Revocation Request

4.9.3.1 End-User Certificate

The requirements for identifying and validating a revocation request are described in Section 3.4 «Identification and Authentication for Revocation Request».

The following minimum information must be included in the Certificate revocation request:

- The identity of the Subscriber as described in the Certificate.
- Identification of the applicant for revocation.

- Any information enabling the Certificate to be revoked quickly and without error (serial number).
- The cause of revocation. This cause of revocation is not recorded in the CRL but can be recorded in the Service database.

See Section 3.4 Identification and Authentication for Revocation Request for certificate revocation process.

Events related to revocation life cycle are logged. Details of revocation procedures are documented in the CA internal procedures.

The revocation applicant will be notified of the effective revocation of the Certificate by his/her Bank once he/she successfully deactivate his/her profile with all. The customer will no longer be able to access the E-Cheque Service.

The occurrence of the operation associated to the revocation is kept in the event logs with, where appropriate, enough information about the initial causes that have implied the revocation of the Certificate.

The causes of revocation of the Certificates are not published.

4.9.3.2 Revocation of a PKI Component Certificate

BENEFIT CA specifies the procedures to be followed in the case of revocation of a PKI Component Certificate, it is included:

- BENEFIT GA order to the TSO for CA BENEFIT revocation
- Publication of Authority Revocation List by the TSO

In the case of revocation of a Certificate within certification chain, the CA must inform (and if possible, in anticipation) all the concerned Holders that their Certificate is no longer valid.

4.9.4 Delay for Requesting a Revocation

As soon as an authorized entity (see Section 4.9.2 « Origin of a Revocation Request ») is aware of any possible cause of revocation, within its scope of operation, it must perform its request for revocation without delay.

4.9.5 Delay for Processing a Revocation Request

BENEFIT ensure that a revocation request is effectively processed within a 60-minute delay after the validation of the request. The computation of the delay is based on a schedule that is synchronized with UTC at least one time per day.

4.9.5.1 End-User Revocation

By nature, a revocation request must be performed urgently. Therefore, the revocation function must have an unavailability period after service interruption (breakdown or maintenance) that is in line with the contractual commitments established between BENEFIT and the Client.

In all cases the support services of this function are insured 24/7 and the processing of the request of revocation is ensured during the working days and hours.

4.9.5.2 Revocation of a PKI Component Certificate

A PKI Component Certificate must be revoked upon detection of an event described in the possible revocation causes for this type of Certificate.

Revocation of a Certificate is effective when the serial number of the Certificate is entered in the revocation list of the CA that issued the Certificate, and the list is available for download. The revocation of a CA Signature Certificate must be done immediately, especially in the case of key compromise.

4.9.6 Revocation Checking Requirement for Relying Parties

A third-party application using an end-user certificate is required to verify, prior to its use, the state of the of the entire certification corresponding to the certificate, including the end-user Certificate itself.

4.9.7 CRL Issuance Frequency

The CRLs are issued with maximum frequency of 24h, and its validity period is 72H.

4.9.8 Maximum Delay for CRL Publication

The CRL is published at most 60mn maximum delay upon its generation.

4.9.9 On-line Revocation Status Availability

An OCSP service is in place. The address of the service is specified within the profile of the issued certificates.
OCSP access is not available on the internet. The access is only granted through VPN access to TSPO IT systems.

4.9.10 On-line Revocation Status Requirement

See Section 4.9.6 « Revocation Checking Requirement for Relying Parties » above.

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Special Requirements Regarding Key Compromise

For end-user Certificates, personnel authorized to make a revocation request are required to perform the revocation as soon as possible after notification of the compromise of the private key.

In case of compromise of the private key of a CA, the revocation of the corresponding certificate is revoked.

In this case, the BENEFIT CA will inform the RAs concerned as soon as possible and will revoke all the certificates issued by the CA whose certificate is to be revoked.

BENEFIT will also publish on its website clear information concerning the revocation of this certificate. This publication will be validated by the BENEFIT communication department.

The relevant parties such as Banks, Central bank, and government entity managing trust service provides in Kingdom of Bahrain are notified by the BENEFIT within 24 hours following the procedure published by the supervisory body.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Processing a Suspension Application

Not applicable

4.9.16 Limits of Certificate Suspension Period

Not applicable

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

The CA provides to Third Party Applications the means to verify and validate prior to its use the status of an issued certificate together with its certification chain (*i.e.* checking the signatures of the chain's certificates, signatures that guarantee the origin and integrity of OCSP and the status of the CA Certificates).

4.10.2 Service Availability

The certificate creation, status, electronic signature creation, validation services are available 24/7. These function must have a maximum duration of unavailability per service interruption (breakdown or maintenance) in conformity with the contractual commitments established between BENEFIT and the Client.

The above-mentioned services status information feature is available 24/7.
The architecture in place has been setup to target.

- a minimal 99,5% availability of the Publication server,
- a minimal 99% availability of the OCSP server.

The architecture in place to ensure such availability rate is described in the E-Cheque, CA, and signer internal documentation.

The above-mentioned availability may be affected by the practices, policies and services of other service providers, not under the control of Benefit E-Cheque platform.

4.10.3 Optional features

Not applicable

4.11 END OF SUBSCRIPTION

In case of end of the contractual relationship between the CA and the corresponding certificate holder before the end of the certificate's validity, the certificate is revoked.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Recovery and Practices in Case of Key Escrow

Not applicable.

4.12.2 Recovery and Practices in Case of Session Key Encapsulation

Not applicable

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

The head of BENEFIT CA ensures that the operating premises of the components of the PKI are implemented and maintained at the required level of physical safety.

Physical controls are setup on the operational site. This site hosts:

- The PKI "Bunker". The critical PKI services are operated within this bunker.
- The Secured Key management service of the CA. This critical service is also operated within the bunker.
  The person responsible for this operation site shall respect the rules and principle that are defined in the security policy of the physical site.

The operational site is declared in conformity with APSAD R81 rule (Intrusion Detection System).

Operational procedure derived from the above rule and from the PKI list of requirements is documented in an internal document. This document describes:

- General principles of protection of the site
- General principles of protection of the facilities
- General principles of the protection of the restricted areas
- Access control mechanism and access modalities
- Fire protection mechanism
- Protections against flooding
- Power supply
- Air conditioning

5.1.1 Site Location and Construction

Depending on the sensitivity of the components of BENEFIT internal PKI, the sites are defined in level 1 of the TSPO security policy: vital impact (major for the company).

In this respect, the safety of the building site meets the level 1 physical security measures for peripheral, perimeter and interior protection and in particular measures relating to:

- power supply and air conditioning;
- vulnerability to water damage;
- fire prevention and protection.

The measures also make it possible to respect the commitments made in this CP/CPS or in the contractual commitments with the TSPO, regarding the availability of services.

5.1.2 Physical Access

To avoid loss, damage and compromise of the resources of the BENEFIT CA, access to the premises is controlled according to the level 1 zoning level: "very restricted access", or comparable.

For the functions of Certificate generation, generation of secret elements of the Client, and management of the revocations, access is strictly limited to the only persons authorized to enter the premises and the traceability of the accesses is ensured. Security is reinforced by the implementation of physical and logical intrusion detection means. In addition, the control in input and output is permanent in hours not worked (HNO). These requirements are also deferred contractually with the Client when the Client is responsible for these functions.

To ensure the availability of systems, access to machines is limited only to those authorized to perform operations requiring physical access to the machines. For this purpose, the relevant components of the PKI define a physical security perimeter where these machines are installed. Any room used in common between the component concerned and another component (from or outside the PKI) is outside that perimeter.

The opening of the door is controlled by an access control system.

Root CAs are operated in perimeter that is physically isolated from the other operations. This environment is restricted to the person allowed to access to root CA keys.

5.1.3 Power and Air Conditioning

Power and air conditioning supplies are scaled to ensure that the CA is operated in correct conditions and to ensure the availability of the services provided by the CA. The detailed description of these measures is confidential and documented in the CA internal documentation.

5.1.4 Water Exposures

The protection measures of BENEFIT CA ensures a protection of the infrastructure against water damage. The detailed description of these measures is confidential and documented in the CA internal documentation.

5.1.5 Prevention and Protection Against Fire

BENEFIT CA is set up protection measures against fire. The detailed description of these measures is confidential and documented in the CA internal documentation.

5.1.6 Media Storage

The media (paper, hard disk, floppy disk, CD, etc.) used in the BENEFIT CA are processed and stored in accordance with security requirements for sensitive assets (confidentiality, integrity and availability).
Particularly, security measures are in place to protect media against theft, damage, lost, unauthorized access and obsolescence. These measures are applicable for the whole retention period of these media.

All media containing sensitive data (e.g. disk, CD-ROM) along with sensitive paper documents (Key Ceremony script and reports, registration folder …) are stored within secure vault and safe that protect them from potential external attacks (including fire and humidity).
The CA also ensures that sensitive data are backed up in a way that ensures:

- Access to the data during the whole retention period;
- Availability and integrity of the data, allowing to replay them during the whole retention period;
- Protection against obsolescence of media
- Availability of the stored evidence, if necessary.

The detailed description of the applicable measures is confidential and documented in the CA internal documentation.

5.1.7 Waste Disposal

At the end of life, the media will either be destroyed or reinitialized for reuse, depending on the level of confidentiality of the corresponding information.
The procedures related to destruction and to the reuse of media are confidential and documented in the CA internal documentation.

Hard disks involved in the Key Ceremony are in the scope of these procedures. Documents in paper forms, and particularly confidential documents are destroyed in a systematic way with a shredder before being sent to the waste-disposal system of the site.

Destruction and resetting procedures and means are compliant to TSPO Security Policy.

5.1.8 Off-Site Backup

In addition to site backups, the PKI components implement offsite backups of their applications and information. These backups are organized to ensure the fastest recovery of incident services.
Backup is tested on a regular basis and allows the execution of the disaster recovery plan.
Details of backup management is provided in the disaster recovery plan.

5.2 PROCEDURAL CONTROLS

The following procedural safeguards are in addition to those set out in the Key Ceremony during which the BENEFIT CA Key Pair is created.
Procedure and policies are communicated to authorized employees.
Procedures are documented and applied for all operation involving Trusted Roles and impacting the provision of service.

5.2.1 Trusted Roles

The trust roles defined below are those required for the PKI components, irrespective of the trust roles defined in the key ceremony.

- PKI Security Officer - The Security Officer is responsible for the implementation of the security policy of the BENEFIT CA. It manages the physical access controls to the entity's equipment systems. It is empowered to look at the records kept, and is responsible for the analysis of the event logs to detect any incident, anomaly, attempted compromise, etc.
- Application manager - The application manager is responsible, within the component of the PKI concerned, for the implementation of the various CPs and CPSs of the CA BENEFIT CA. Its responsibility covers all the functions rendered by the applications and the corresponding performances.
- System engineer - It is responsible for the start-up, configuration, and technical maintenance of the IT equipment of the entity. It provides technical administration of the entity's systems and networks.
- Operator - An operator within the component of the PKI concerned carries out, within the scope of his attributions, the operation of the applications for the services delivered by the component of the PKI.
- Controller - A designated person whose role is to analyse logs and incidents related to the PKI. The controller is independent of other trust roles.

Although BENEFIT has full owner ship and responsibility over management, security and delivery of trusted services, BENEFIT uses third party service providers to manage the above-mentioned Trusted Roles. All third-party contractors have formal contracts in place and go under annual review by BENEFIT to ensure compliance to the contract terms. BENEFIT delegates the above roles to the contractors according to their role and tasks. The third-party contractor is responsible for compliance when its personnel acting as Trusted Roles.

5.2.2 Number of Persons Required Per Task

BENEFIT CA operations requiring the intervention of several persons and the constraints that these persons must respect (positions in the organization, hierarchical links, etc.). It specifies the persons required for the key ceremony.

When dual control is required, at least two security officers are required to execute a task. All critical tasks relating to the management of intermediate CAs, root CAs and cryptographic authority keys require a dual control of two security officers.

The restoration of an HSM is only possible if a minimal number of Key Custodian is present. Access to the bunker area is only possible with dual control of authorized trusted role.

5.2.3 Identification and Authentication for Each Role

Each entity operating a component of the PKI shall have the identity and authorizations of each member of its personnel verified before assigning to it a role and the corresponding rights, including:

- That his name is added to the access control lists for the premises of the entity hosting the systems concerned by the role
- that his name be added to the list of persons authorized to physically access those systems,
- that an account be opened in his name in those systems
- if applicable, cryptographic keys and/or a certificate are issued to him to fulfil the role assigned to him in the PKI.
- These checks are described in the BENEFIT CA`s CPS and comply with TSPO Security Policy.

Operator, administrator, and auditor role are under direct TSPO management. Administrators oversee user account management. Modification or deletion of a user account is performed without delay.
All operation performed by Trusted Role are kept in event logs.

5.2.4 Roles Requiring Separation of Duties

Several roles can be assigned to the same person, to the extent that cumulation does not compromise the security of the services offered.

The attributions associated with each role are described in BENEFIT CA CPS and are consistent with TSPO Security Policy.

The same physical person may perform several roles, under the condition that the cumulative effect of the role does not impact the security of the PKI functions. However, it is recommended that the same physical person does not cumulate several Trusted Roles. The following rules concerning the segregation of duties shall at least prohibit the following cumulative:

- Security officer and systems engineer/operator,
- Controller and any other role,
- System engineers and operators.

The CA maintains a nominative inventory of the roles in the CA internal documentation. This inventory is confidential.

5.3 PERSONNEL CONTROLS

The following procedural safeguards are in addition to those set out in the Key Ceremony during which the BENEFIT CA key pair is created.

5.3.1 Qualifications, Experience, and Clearance Requirements

All personnel required to work within the PKI components are subject to a confidentiality clause.

The Governance Authority of the CA must ensure that the attributions of his/her personnel, who are required to work within the PKI, correspond to their professional competencies.

Supervisory staff must have the expertise appropriate to their role and be familiar with the security procedures in place within the PKI and the measures related to personal data protection.

BENEFIT CA informs any persons involved in the PKI's trust roles of:

- His/her responsibilities relating to the services of the PKI,
- The procedures related to security and control of the system to which he or she must comply.

Personnel in Trusted Role are formally appointed by Head of CA via a written agreement form which is signed by the Trusted Role for acceptation.

The qualifications, skills and clearances required for the key ceremony are defined in specific procedures. Responsibilities of Trusted Roles are attributed in a way that separation of duties is applied to avoid conflict of interest and to limit the opportunities of misuse (malicious or accidental) of PKI components.

Access and habitation are provided based on least privilege policy.

5.3.2 Background Check Procedures

Personnel required to work within a component of the PKI, and depending on the applicable context, are required to submit a certificate on the honour of non-conviction, a criminal record, or a confidentiality undertaking.

Persons with Trust Role must not have conflicts of interest that are prejudicial to the impartiality of their tasks.

In particular, the certification operator ensures that that person in Trusted Role provides:
- A valid copy of an ID document
- An extract of Criminal record (in France, “extrait du bulletin n°3 du casier judiciaire”)

The background checks are:
- Performed before the access and authorization are granted.
- Reviewed at least every 3 years.

5.3.3 Training Requirements

Personnel are trained in the software, hardware and internal operating and security procedures that they implement and which they must comply with within the component of the PKI in which they operate. CA provides a set of documents, including policies and procedures, to all personnel involved in the PKI.

Staff have knowledge and understanding of the implications of the operations for which they are responsible.

5.3.4 Re-training Frequency and Requirements

The CA ensures that the concerned staff shall receive adequate information and training in line with the staff tasks. Ca employees may also express their needs regarding training during a face-to-face meeting with management. This face-to-face meeting is performed every six month and allows planning the future training.
Moreover, a yearly training targeting the new threat and the security procedure is performed to all Trusted Role.

5.3.5 Job Rotation Frequency and Sequence

Job rotation mainly occurs when a change of position or function of an employee in Trusted Role or in an operational role.
Job attribution is reviewed at each internal audit.

5.3.6 Sanction for Unauthorized Actions

Sanction for unauthorized actions is described in the CA internal documentation and are confidential.

5.3.7 External Contractors' Requirements

The staff of external service providers working on the premises of BENEFIT CA and/or on the components of the PKI shall also comply with the requirements of this Section 5.3. This is translated into appropriate clauses in the contracts with the providers.

When applicable, the following clauses may be added to the contract between BENEFIT and its subcontractors.

- The subcontractor shall employ for the whole duration of the contract qualified personnel with the adequate professional competencies.
- The subcontractor ensures to maintain an up-to-date knowledge and know-how of its field of operations. The subcontractor shall implement the appropriate information awareness principle to be informed of the best practices to be implemented. The subcontract shall set up training session for its personnel each time the best state-of-the-art practices evolved in a significant way. At least, a yearly training related to new threat and security measures shall be setup.

The subcontractor shall take any necessary measures, in particular regarding its employees, to maintain the confidentiality of any confidential information provided by BENEFIT or any entity involved in the BENEFIT CA.

5.3.8 Documentation Supplied to Personnel

Each staff member has at least adequate documentation concerning the operational procedures and the specific tools that it implements, as well as the general policies and practices of the component in which it works, more specifically the Security Policy affecting it.

Security policies and procedures are communicated to BENEFIT CA staff, as soon as the authorization is granted and before they perform their tasks. The subset of communicated policies and procedures is selected with respect to the tasks to be performed. Any person performing an operational task within the BENEFIT CA has access to the adequate documentation to perform its tasks.

5.4 AUDIT LOGGING PROCEDURES

Event logging involves recording events in manual or electronic form by input or by automatic generation. The resulting files, in paper or electronic form, must make possible the traceability and the accountability of the performed operations.

Audit logging procedures are described in CA internal documentation. This documentation is confidential.

5.4.1 Type of Events to be Recorded

Each entity operating a component of the PKI logs at least the following events, automatically from the start of a system and in electronic form:

- Creation / modification / deletion of the authentication data (passwords, certificates, etc.),
- starting and stopping of computer systems and applications,
- events related to logging: starting and stopping the logging function, modifying the logging parameters, actions taken following a logging failure,
- Connection / disconnection of users with trusted roles, and unsuccessful attempts.
- Change in the security policy configuration.
- Unexpected stops, crash, and system failure
- Network component and firewall activity

Other events are also gathered by electronic or manual means. These are those relating to security and are not produced automatically by the computer systems, in particular:

- physical access,
- maintenance and changes to the configuration of systems,
- changes to personnel,
- Destruction and resetting of media containing confidential information (keys, activation data, personal information about holders, etc.).

In addition to these logging requirements common to all components and functions of the PKI, events specific to the various functions of the PKI are also logged, including:

- receipt of a Certificate request (initial and renewal),
- validation of a certificate request
- events related to signature keys and CA certificates (generation (key ceremony), backup/recovery, revocation, renewal, destruction, etc.),
- publication and updating of information related to the CA (CP, CA certificates, general conditions of use, etc.),
- generation of Holders' Certificates,
- of a request for revocation,
- validation/rejection of a request for revocation,
- generation and publication of the CRL

Each entry in the event journal contains, where applicable, the following fields:

- event type,

- name of the executant or system reference triggering the event,
- date and time of the event,
- result of the event (failure or success).

The accountability of an action rests with the person, organization or system that performed it. The name or identifier of the executant is explicitly entered in one of the fields of the event log.

In addition, depending on the type of the event, each record also contains the following fields:

- as far as possible: requestor and recipient of the operation or reference of the system creating the request,
- names of persons present (If it involves more than one person),
- cause of the event,
- any information characterizing the event (for example, for the generation of a Certificate, the serial number of this Certificate).

Logging operations are performed during the process. In case of manual entry, the writing is made, except in exceptional cases, on the same business day as the event.

5.4.2 Frequency of Processing Event Logs

The PKI event logs are analysed 2 to 3 times each week on average. Moreover, automatic analysis of event logs is performed to identify abnormal behaviours and to alert PKI personnel of potential critical security events.

5.4.3 Retention Period for Audit Log

Event logs are kept on-site for at least one month.
Event logs are archived for a retention period compliant with applicable Regulation, even in case of end of activity of the CA.

5.4.4 Protection of Audit Log

The CA implements event log protection appropriate to the level of sensitivity of the information contained in these logs. This level of sensitivity is the result of a risk analysis.

5.4.5 Audit log Backup Procedures

All events are written to a database that is in the scope of BENEFIT or its suppliers infrastructure backup procedures.

5.4.6 Audit Collection System

All events are written centrally in a database.

5.4.7 Notification to Event-Causing Subject

The CP/CPS does not have specific requirements for this.

5.4.8 Vulnerability Assessment

The CA implements system vulnerability management BENEFIT CA. This is done in accordance with TSPO Security Policy.

Event logs are monitored regularly in accordance with the procedures set out in Section 5.4.2 Frequency of Processing Event Logs.

The logs are analysed as soon as an anomaly is detected. This analysis gives rise to a summary in which important elements are identified, analysed, and explained. The summary shows the anomalies and falsifications found.

Any critical vulnerability is handled by BENEFIT with 48 hours after its discovery. Depending on the results of the analysis BENEFIT may either:

- Setup a correction plan, or
- Document the reasons why no correction will be performed.

5.5 RECORDS ARCHIVAL

5.5.1 Type of Records Archived

This archiving ensures the conservation of the event logs generated by the various components of the PKI. It also allows the storage of the paper-form documents related to the certification operations, as well as their availability in case of necessity.

The data to be archived are at least the following:
- CP/CPS
- contractual agreements with other CAs;
- CRLs as issued or published;
- the registration documents of the Subscribers.

5.5.2 Retention Period for Archive

All information of the following types will not be archived for more than one year if those data is not related to the Subscribers Digital Certificates and Signatures:

- Personnel
- Traffic,
- Connection
- And resulting from an automatic process of data processing.

The duration of the archive is as follows:

- CP/CPS: until the end of life of the CA,
- organizational documents for key ceremonies: until the end of life of the CA,

This information is archived for 10 years once the electronic cheque has reached the end of its lifecycle:

- Holder registration record and evidence,
- Certificates issued by the CA,
- Last CRL issued by the CA,
- Event logs after generation.

The electronic cheque lifecycle ends in the below conditions:

- Electronic cheque has been successfully paid
- Electronic cheque presentment cycle reached the maximum cycle
- Electronic cheque is expired
- Electronic cheque is cancelled

BENEFIT has set up measures to ensure the conservation of the documents for the above period, event in case of end of activity.

5.5.3 Protection of Archive

During all the retention period, archive and back-up of archive shall

- be protected in integrity;
- be accessible to only authorized persons;
- be readable and able to be processed.

The CPS specifies the means used to securely archive these elements.

5.5.4 Archive Backup Procedures

The procedure is specified in the CPS. The level of protection of backups is at least equivalent to the level of protection of the archives.

5.5.5 Requirements for Timestamping of Records

Certificate's issuance date is the time of their generation and this information is archived with the corresponding certificate.

Section 6.8 Timestamping specifies the dating/timestamping requirements.

5.5.6 Archive Collection System

The CPS specifies the means used to safety collect archives.

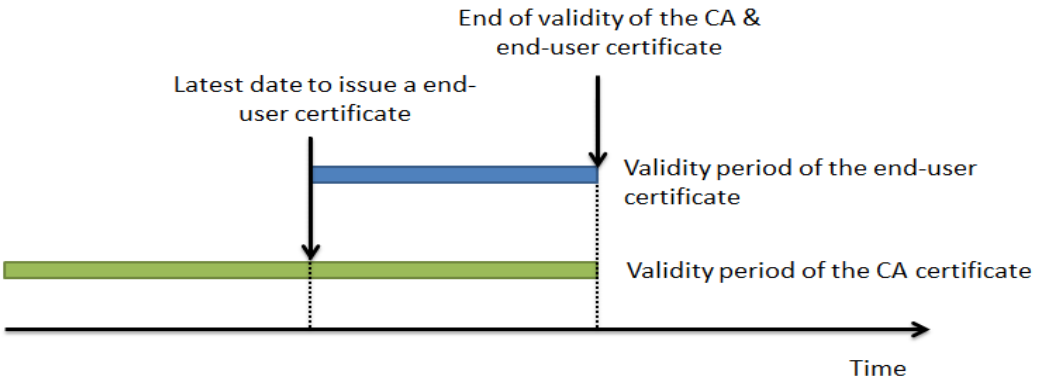
5.5.7 Procedure to Retrieve and Verify Archive Information

The archives (paper and electronic forms) are retrievable within 2 working days, it being noted that only the CA can access all the archives (as opposed to an entity operating a component of the PKI which cannot retrieve and consult the archives of the component concerned).

Archive Retrieval conditions are specified in the CPS.

5.6 KEY CHANGEOVER

The CA can not generate a certificate with an end date that is later than the expiration date of the corresponding CA certificate. For this purpose, the period of validity of the CA certificate must be longer than that of the certificates it signs.



CA Keys shall be changed at most 8 year after their generation during the key Ceremony.

Taking into account the expiry date of this certificate, its renewal must be requested within a period of at least 6 months before reaching 8-year validity.

As soon as a new key pair is generated and operated, only this new key pair is used to sign certificates. For that, after the successful execution the renewal procedures, the certificate requests are automatically redirected to be signed by the new private key of the CA.

The old CA certificate is afterwards still available to verify the certificates issued with its associated private key, at least until the expiration or revocation of the last certificate issued with this key. Therefore, during this transition period, two CA certificates will be available:

- The old certificate to validate the end-user certificate issued with the associated private key;
- The new certificate to sign and issue new end-user certificates and to be able to validate them.

5.7 COMPROMISE AND DISASTER RECOVERY

BENEFIT CA maintains a Disaster Recovery Plan that covers the requirements regarding the compromise and the disaster recovery. This documentation is confidential.

5.7.1 Incident and Compromise Handling Procedures

Each PKI component implements reporting and incidence response procedures and measures in accordance with the requirements of TSPO Security Policy.

In the case of a major incident, such as loss, suspicion of compromise, compromise, theft of the private key of BENEFIT CA, the triggering event is the recognition of this incident. The BENEFIT PKI GA is immediately informed. The case of the major incident is imperatively dealt with upon detection and publication of certificate revocation information, where applicable, must be made in the utmost urgency, or even immediately, by any useful and available means.

In the case of a major security incident or integrity loss that may have a major impact on TSPO operation or on personal data of the users of the service, BENEFIT will notify the impacted parties. In particular, BENEFIT will notify the local regulation authority.

5.7.2 Recovery Procedures in Case of IT Disaster (Hardware, Software, and Data)

In accordance with the TSPO Security Policy, BENEFIT CA has a business continuity plan to meet the availability requirements of its sensitive functions and specified in:

- This CP.
- Commitments in terms of quality of service of the various PKI components, as regards the functions related to the publication and/or related to the revocation of the Certificates. This plan is tested at least once every 3 years.

5.7.3 Entity Private Key Compromise Procedures

The case of compromise of an infrastructure key or control of a component of the BENEFIT PKI is treated in accordance with Section 5.7.2 « Procedures in Case of IT Disaster (Hardware, Software, and Data) ».

In case of CA Key compromise, BENEFIT:

- will notify all the impacted Clients and Certificate Holders and will also notifies the impacted third parties.
- will provide in the published information on the status of the certificates that these certificates are no longer valid.
- will immediately revoke the compromised CA certificate.

In case of algorithm compromise, BENEFIT will apply all the above actions excepting the immediate revocation of the CA Certificate. Instead, BENEFIT will setup a planned revocation date for this certificate that will be in line with the state of the art related to the weaknesses of the compromised Algorithm.

In the event where BENEFIT experience any material technical or operational problems or any other emergency situation which will prevent BENEFIT from performing its functions, it shall inform the regulator in the Kingdom of Bahrain of the issue at the same day of the issue. An incident report will be shared if required detailing the root cause and corrective actions and measures that were taken to assure such issue is not encountered in the future.

5.7.4 Business Continuity Capabilities After a Disaster

The various components of the BENEFIT PKI have the means reasonably necessary to ensure the continuity of their activities in accordance with the requirements of this CP/CPS (See Section 5.7.2 « Procedures in Case of IT Disaster (Hardware, Software, and Data) »).

BENEFIT has an up-to-date Business Continuity Plan that allows the CA to treat in an effective manner in case of disaster by restoring the IT systems in the delay specified within the Business Continuity Plan. This plan includes the CA Key compromise scenario and the loss of activation data scenario.

5.8 TERMINATION

One or more services of the BENEFIT trust services may be required to cease all or part of its business or transfer it to another entity.

BENEFIT has forecasted means in case of CA termination. These means are described in the up to date BENEFIT termination plan.

The compromise of the BENEFIT CA key pair immediately implies the cessation of its activity and the revocation of all valid Certificates issued. To regain the level of service, the creation of a new CA and new Certificates are mandatory.

In case of termination of trust services such as subscriber key management and digital signature services, BENEFIT shall ensure availability of all digital signature validation data for at least 10 years. Before termination, BENEFIT shall communicate with all Subscribers and regulator.

Transfer of activity or cessation of activity affecting a component of the BENEFIT PKI.

To ensure a constant level of confidence during and after such events, the BENEFIT CA undertakes, among other obligations:

- to set up procedures aiming at ensuring the continuity of the service, particularly in terms of archiving (in particular, archiving of Holder Certificates and information relating to Certificates);
- to ensure the continuity of the revocation service (considering a request for revocation and publication of the CRL), in accordance with the availability requirements for its functions defined in this CP.

BENEFIT CA ensures the following points:

- in the case where the planned changes may have an impact on the commitments with the Customers or the Third Parties using certificates, BENEFIT CA must notify them as soon as necessary and, at least, within 3 months.
- BENEFIT CA must communicate to the Clients and Certificates Holders the principles of the action plan that will implement the technical and organizational measures intended manage activity termination or to organize the activity transfer. It will present the arrangements in place for archiving (keys and information relating to certificates) to ensure this function this be ensured for the duration originally planned in the CP. BENEFIT CA shall communicate to the Clients and Certificates Holders the terms and conditions of the changes. BENEFIT CA will estimate the impact and will analyse the consequences (legal, economic, functional, technical, communication, etc.) of this event. It will present an action plan to remove or reduce the risk to the Third Parties and the discomfort to Customers and Holders.
- BENEFIT CA shall keep Clients and other entities informed of any additional barriers or delays encountered in the change process.
- BENEFIT CA will notify the Supervisory Body, and all appropriate authorities, in case of PKI Termination and will publish the information to notify the Trust Party Applications. BENEFIT CA will follow the regulator requirements related to the trust services termination.

Termination affecting BENEFIT CA

The termination of activity may be total or partial (for example: cessation of activity for a given family of Certificates only). Partial discontinuance of activity must be phased in such a way that the obligations referred below are to be performed by BENEFIT CA, or a third-party entity which resumes the activities, at the expiration of the last Certificate issued by it.

In the case of a complete termination of activity of BENEFIT CA or, in the case of impossibility for BENEFIT CA to perform the action, any entity that is substituted for it by the law, a regulation, a court decision or an agreement previously entered into with that entity, revokes the Certificates and publishes the CRLs in accordance with the commitments made in this document.

Upon termination of the Service, BENEFIT CA:

- deletes the private key used to issue Certificates, and all copies of this key
- take all necessary measures to destroy the key or to made it inoperative;
- revokes his Certificate;
- revokes all the issued Certificates and which are still valid;
- notifies (e.g. by receipt) all Holders of revoked certificates (or to be revoked).
- Notifies all relying parties and regulator
- transfers to a third party the requirement regarding the publication of information, in particular the publication of the public key. Transfer will also include all information necessary to provide evidence of the operation of BENEFIT for a reasonable period.
- Transfer of data will be in compliance with the regulator requirements.
- Terminates authorization of all subcontractors to act on behalf of Benefit in carrying out any functions relating to the process of issuing trust services.

5.8.1 PKI Transfer

If BENEFIT decides to transfer the BENEFIT CA activity, the following organizational steps will be performed:

In the specific case where the transfer implies to stop the operations, for example a change of the Certification Operator, the following steps will be performed:

- The CA will first ensure that CRL and ARL are up to date before starting the transfer procedure.
- The CA will notify regulator, subscribers, client and third parties the temporary non-availability of the certificate issuance service.
- The CA will stop the CA certificate issuance infrastructure.
- The CA will start the new CA infrastructure.
- If applicable, transfer of the secret elements will be securely transferred to new Key Custodians.
  - The technical operation shall be performed in such a way that the CRL publication is maintained during the whole transfer procedure.
- Transfers authorization of all subcontractors to act on behalf of Benefit in carrying out any functions related to the transferred services.
- Agree with regulator on transfer plan.

In the specific case where the transfer is simply a transfer of responsibility of the PKI between two entities without any impact on the Certification Operator, only the transfer of secret element to new key custodians shall be performed.

In any case, any activity transfer implies a review and an update of the CA documentation.

In case of transfer of trust services such as subscriber key management and digital signature services, BENEFIT shall ensure availability of all digital signature validation data and signature creation information. Before transfer, BENEFIT shall communicate with all Subscribers, relying parties, and regulator.

5.8.2 End of Activity

In case of the end of activity, the CA must perform the operation described in the Termination Plan.
The Termination Plan is in line with the requirements in CP Section 5.8. This Termination Plan is confidential.

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 of a new key pair by a CA is only performed during a Key Ceremony (KC).

The CA signature keys are generated onboard of an HSM (Hardware Security module) CC certified according to ETSI EN 419 221-5, see also Section 6.2.1 Cryptographic Module Standards and Controls.
The cryptographic algorithms used for the CA key pair generation, and CA certificate signature is described in Section 7.1 Profiles of the certificate of the BENEFIT CA.

The generation of CA signature keys is done under perfectly controlled circumstances by personnel in trusted roles as part of a Key Ceremony (KC). This ceremony takes place according to previously defined organizational and technical scripts.

All KC tasks are done under controlled circumstances that include:

- Restricted physical Access to the Key ceremony room within the trust centre,
- Only trusted roles can take part of the KC,
- All critical tasks on the CA require dual electronic signature of 2 security officers,
- All critical tasks on the HSM require Dual authentication of 2 security officers,
- Key Backup is performed in compliance with HSM Backup procedure using hardware backup device and require Dual authentication of 2 security officers,
- The actions to be performed during a Key Ceremony are described within a Key Ceremony Script.

The script of the Key Ceremony identifies:

- roles participating in the ceremony (internal and external from the organization);
- functions to be performed by every role and in which phases;
- responsibilities during and after the ceremony; and
- requirements of evidence to be collected of the ceremony.

The details of the script are confidential.

The Key Ceremony is performed in the presence of:

- The Security Officer for a CA Key
- A Security Officer and a Bailiff for a Root CA.

A key ceremony report is signed by all participants who testify that the ceremony has been processed in conformity with the pre-defined script. Thus, the report provides evidence that the integrity and confidentiality of the key pair generation has been ensured.

Together with the generation of CA keys, various secrets and sensitive elements are generated. These secrets are data that are managed in a secured way (nobody can possess the entirety of the secret). These secrets are needed, after the Key Ceremony, to perform the operations on the HSM to be able to restart, save, and restore the backup of the HSM partition.

Following their generation, the secrets are handed over to Key Custodian in advance and entitled to this Trusted role.

All secrets used for CA Key generation and backup are managed in a secured way (nobody can possess the entirety of the secret). These secrets are needed to perform the operations on the HSM to be able to restart, save, and restore the backup of the HSM partition.

The renewal of the CA Certificate and Keys follows the same principles as the first generation of CA keys.

The root CA KC is performed in the presence of security officers and a Bailiff within the bunker. The root CA uses a dedicated offline HSM, and all actions require dual electronic signature of 2 security officers.

The issuance of a Certificate by the root CA is performed in dual control by two authorized persons in Trusted Role.

6.1.1.2 End-Users' Keys

The end-user keys are generated on personalization sites whose contractual security conditions are established between the CA and the RA. Generation of the keys is done on a hardware cryptographic device that is a QSCD consisting of a SAM (as defined in ETSI 419 241-2) inside of a certified HSM, according to 419 221-5.

This module is hosted within the Certification Operator premises with strictly restricted access. The keys are of the type of RSA and they are generated automatically on request for the user.

Generation of the end-user signature keys is carried out under perfectly controlled circumstances by authorized personnel of the Registration Authority.

6.1.2 Private Key Delivery to Subscriber

The end-user private key is generated and used within onboard within the QSCD. The QCSD qualification of this medium ensures that the private key cannot be exported in plain text outside the QSCD.

6.1.3 Public Key Delivery to Certificate Issuer

The public key is transmitted to BENEFIT CA within the certificate generation request. The key is protected in integrity and the origin is authenticated thanks to a PKCS #10 format that is signed by the private key associated with the public key.

6.1.4 CA Public Key Delivery to Relying Parties

The public CA signature verification keys are made available to certificate users and publicly viewable as defined in Section 2Publications and Repository Responsibilities.

6.1.5 Key Sizes

The key sizes are as follows:

- BENEFIT CA Certificate: 4096 bits (RSA algorithm)
- End-user Certificates: 2048 bits (RSA algorithm)

6.1.6 Validation of the Key Pair Parameters

The Key Pair generation equipment uses parameters respecting the security standards specific to the algorithm corresponding to the Key pair. These parameters are recalled in Section 7 « CERTIFICATES, OCSP And CRL Profiles ».

6.1.7 Key Usage Purposes

The use of the CA private key and the associated Certificate is strictly limited to the Certificate signatures and CRL.

The use of the Holder's private key and the associated certificate is strictly limited to the Advanced Electronic Signature

(See Sections 1.4 « Certificate » et 7.2).

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

6.2.1.1 Cryptographic Module of the CA

The cryptographic modules used by the CA to generate and implement its signature keys are certified in conformity with ETSI EN 419 221-5 and ETSI EN 419 241-2.

6.2.1.2 End-user Signature Creation Device

The devices used for the Holders key pair are QSCDs under one or more references published by the EU on the EU QSCD List.

6.2.2 Private Key Multi-Person Control

Control of the private key of the CA is ensured for the following actions:

- for export/import out/in a cryptographic module: the systems are configured to prohibit the unencrypted export of the private key, thus ensuring its non-compromise;
- for the generation of the key pair (see section 6.1.1.1 Key Pair Generation): use of a secure cryptographic hardware module for the generation and storage of the private key, and the sharing of secrets ensures that no alone actor can access or interpret one of the secrets;
- to activate the private key (see section 6.2.8 Method for Private Key Activation): the requests for certificates and revocation (updating the CRL) flows are controlled to ensure that only the authorized services can be registered;
- The authorization and configuration of these flows requires the presence of at least 2 PKI officers;
- for destruction (see section6.2.10 Method for Private Key Destruction): destruction procedures ensure that nobody can use the private key.

6.2.3 Private Key Escrow

Neither the CA private keys nor the Holder's private keys are escrowed.

6.2.4 Private Key Backup

6.2.4.1 CA Private Keys

Backup copy of the CA is performed. The media and mechanism used to handle the private key ensure a level of protection that is at least equal to the one of the private keys. This mechanism is confidential and is described within the CA documentation. In particular, backup procedure is described in the Key Ceremony Script (see 6.1.1.1 - CA Key Pair).

The partition containing the CA private key is backed up from cryptographic modules in encrypted form and with an integrity check mechanism. Installation and Restoration of CA keys within a cryptographic module can only be performed under the dual control of two authorized employees in Trusted Role.

6.2.4.1 End User Private Keys

The private keys of the end-users are backed up in an encrypted and integrity protected form in the Signer database. This database is backed up. Only this QSDC of this installation can decrypt these keys.

6.2.5 Private Key Archival

The private keys of the CA are not archived. The private keys of the Holders are not archived, either by the CA, nor by any of the components of the PKI.

6.2.6 Private Key Transfer into or From a Cryptographic Module

For CA private keys, all transfers are made in encrypted form, as described in section 6.2.4 «Private Key Backup». The procedure for transferring the private key requires the presence of at least 2 trust roles.
The private keys of the Holders cannot be transferred for any use outside QSCD.

6.2.7 Private Key Storage on Cryptographic Module

See section 6.2.1 « Cryptographic Module Standards and Controls ».

6.2.8 Method for Private Key Activation

6.2.8.1 CA keys

See. 6.2.2 « Private Key Multi-Person Control »

6.2.8.2 End-User Keys

Activation of the Holder's private key is controlled via activation data (see section 6.4 Activation Data) that are specific to the holder. Activation is performed in a secure way.

6.2.9 Method for Private Key Deactivation

6.2.9.1 CA Keys

Deactivation of the CA private key in the cryptographic modules is automatic as soon as the environment of the module evolves in a sensitive way: shock, disconnection, etc. The deactivation modalities are specific to the module's technology; they are detailed in the Vendor documentation. In this case, it is necessary to disable the partition containing the corresponding private key.

6.2.9.2 End-User Keys

When an end-user key is revoked through the RA, the access of the QSCD to the private key is removed permanently.

6.2.10 Method for Private Key Destruction

6.2.10.1 CA Keys

At the end of the life of a private CA key, either normal or anticipated (revocation), the key is destroyed, as well as any copy and any element allowing its reconstitution. The key destroy is performed using hardware security module procedure, all backup of CA private key is destroyed using HSM key backup hardware procedure.

6.2.10.2 End-User Keys

The destruction of the private key is carried out by the QSCD after its use.

6.2.11 Cryptographic Module Rating

See section 6.2.1 « Cryptographic Module Standards and Controls ».

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The public keys of the CA and the Holders are archived as part of the archiving of the corresponding Certificates. See more information in section 5.5 Records Archival.

6.3.2 Key Pair and Certificate Usage Period

The usage period of a key pair and certificate are specified in the CPS.

6.4 ACTIVATION DATA

6.4.1 Generation and Installation of Activation Data

6.4.1.1 Generation and Installation of Activation Data for the CA Keys

The generation and installation of activation data for a cryptographic module of the PKI takes place during the initialization and personalization phase of this module. See more information in section 6.2.8.1 CA keys.

6.4.1.2 Generation and Installation of Activation Data for the End-User Keys

The signature activation data are generated on behalf of the end-user. They are provided to the end-user via SMS. The signature activation data has a length of six characters.

6.4.2 Activation Data Protection

6.4.2.1 Activation Data Protection of the CA Keys

Activation data that is generated by the CA for the cryptographic modules of the PKI are protected in integrity and confidentiality until their delivery to their Key Custodian. The Key Custodian is responsible for ensuring confidentiality, integrity, and availability.

Rules and practiced regarding the protection of the secret elements is described within the CA Documentation. This documentation is confidential.

6.4.2.2 Activation Data Protection of the End-User Keys

Activation data of the end-user private key are created on request inside an HSM (Hardware Security Module). They are delivered to the mobile phone of the end-user by SMS.
For each signature operation, a new activation data is created. The mobile phone number of the end-user is protected with a key that is stored on the HSM. This key is generated during a Key Ceremony under dual control.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Computer-Specific Technical Security Requirements

A minimum level of assurance of security on the computer systems of the PKI is defined in the CPS of BENEFIT CA. It meets the following security objectives:

- strong identification and authentication of users for access to the system (two-factor authentication, physical and/or logical);

- management of user rights (to implement the access control policy defined by the CA, in particular to implement the principles of lower privileges, multiple controls and separation of roles),
- management of user sessions (disconnection after a period of inactivity, access to files controlled by role and username);
- protection against computer viruses and all forms of compromising or unauthorized software and software updates;
- management of user accounts, including the modification and rapid deletion of access rights;
- protection of the network against intrusion by an unauthorized person;
- protection of the network to ensure the confidentiality and integrity of the data transiting it;
- audit functions (non-repudiation and nature of the actions carried out);
- Possibly, error recovery management.

Confidentiality and integrity protection of private or secret keys for infrastructure and control must be consistent with the Security Policy.

To meet these objectives, TSPO use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by the PKI.
Security requirement are taken into account in the choice and/or the development of systems and products.

Monitoring systems (with automatic alarm features) and audit procedure of system configuration are in place. That allows:

- To detect and record any non-authorized access or attempt of access to the PKI systems and to react in a timely manner;
- To monitor the volume of service and requests;
- To trigger alarms in case of detection of potential security violation;
- To monitor start-up and shutdown of the logging functions;
- To monitor the availability and utilization of needed services with the TSP network.

Monitoring activities take account of the sensitivity of any information collected or analysed. Alert and critical security events follow-up is performed by employees in Trusted Roles. These ensures that relevant incidents are analysed and reported in line with the TSP's procedure.

6.5.1.1 Identification and Authentication

All system administrators can only connect to PKI infrastructure after a strong authentication based on a certificate stored on a smart card. All system administrators are engaged to respect the rules and practices that are described within the CA Documentation. Thus, documentation is confidential.

6.5.1.2 Access Control

Physical and logical access control management is performed. Details regarding this management are confidential.

6.5.1.3 Administration and Operation

The software that operates the PKI is confidential and is not disclosed in this public document.
The team operating the software has access to all the needed documentation to operate the system and is also aware of all the operational rules and procedures.

6.5.1.4 PKI Component integrity

Penetration testing campaign is performed on PKI components to ensure the application of the security practices and the absence of vulnerabilities.

6.5.1.5 Information flow control

The CA has setup security measures to ensure control of the information flow. These measures are described in detail in the CA internal documentation.

6.5.1.6 Events Journaling and audit

Dashboards are generated and reviewed on a regular basis. These dashboards show the following information:

- Operation performed on certificates (issuance, revocation, renewal…)
- Incidents occurring on the PKI components and systems.

6.5.1.7 Monitoring

Monitoring of the PKI components and system is performed by the teams of the Certification Operator in charge of the operation.

6.5.1.8 Security Awareness

The CA has written a set of documents in the aim of developing the security awareness of the employees. This set of documents covers various topics such as:

- Good practices and security measures
- Classification of information and assets
- Protection of the information (in particular confidential information and personal data)

This documentation is confidential.

6.5.2 Level of Qualification of Computer Systems

Not applicable.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 Security Measures Related to System Development

Implementation of a system participating to a function of the BENEFIT CA PKI is documented.

The configuration of the BENEFIT CA PKI components system as well as any modifications and upgrades are documented. Change management procedures are in place and are applied for each system update (either planned or urgent) or configuration update.

Any development must be consistent with the TSPO Security Policy and the requirements contained in this CP.

6.6.2 Security Management measures

Any planned significant change in a PKI component or system shall be notified to the GA to be validated.
The change is documented.

6.6.2.1 Update of PKI components

Any significant evolution of a component system of the BENEFIT CA PKI must be reported to the GA for validation. It must be documented.

Security Patch management procedure have been defined and implemented by TSPO, such that security patches are applied as soon as possible. If security patches may introduce additional vulnerabilities or instabilities that outweigh the BENEFITs of applying them, then TSPO may not apply them and will document the reasons for not applying a patch.

6.6.2.2 Risk Assessment

BENEFIT CA a carried out a risk assessment to analyse and evaluate trust service risks considering business and technical issues. Base on the result of this risk assessment, TSPO has selected the appropriate risk treatment measures and the associated operational measures, such that the level of security is commensurate to the degree of risk.

The Risk assessment is approved by the Governance Authority of CA, who accepts, through this approbation procedure, the residual risk that has been identified.

The risk assessment is regularly reviewed and revised, at least annually and each time significant evolution of system or component of the PKI is performed.

6.6.2.3 Vulnerability Scan

TSPO performs regular vulnerability scan on public and private IP addresses. Scans are performed by a qualified and independent person or organization.

6.6.2.4 Penetration Test

BENEFIT or its suppliers undergoes a penetration test when new infrastructures are set up or when a component is modified in a significant manner. Evidence of qualification and independence of the person performing the test is kept by BENEFIT.

6.7 NETWORK SECURITY

For security reason, the network architecture and the details of the flow matrix cannot be disclosed in a public document and are part of the CA internal documents that are confidential. This documentation is in line with all the rules and requirements described in the CP 6.7. In particular, the architecture respects:

- The principle of network segmentation.
- The security requirements regarding the connection between PKI components and the interconnection with external systems.
- The redundancy measures ensuring the availability of the critical components of the PKI.

6.7.1 Network Segmentation

Based on the risk assessment result, BENEFIT CA has segmented its systems into separated networks (separation is functional, logical, or physical). BENEFIT CA applies the same security controls to all systems co-located in the same zone.

Each PKI component is operated in a secured network area. The component is installed following procedures and configurations guidance ensuring the security of the operation. The most critical components, such as Root CAs, are operated in the most secured areas.

The BENEFIT CA production systems are separated from other systems (development and testing, qualification)

6.7.2 Interconnections

Interconnection to public networks and Interconnection between network area are protected by security gateways configured to accept only the protocols necessary for the functioning of the component within the PKI.

The CA ensures that components of the LAN (e.g. routers) are maintained in a physically and logically secure environment.

Moreover, exchanges between components within the BENEFIT CA PKI are subject to the implementation of distinct and logically secured channels that ensures identification of its end points and protection of the channel data from modification or disclosure.

6.7.3 Connections

Only employees in Trusted roles can establish an access to the secured network area.

Any connection with a user account able to directly create a certificate is only allowed after a multi-factor authentication. Operational and administrative network are separated. Administrative network is dedicated to administrative functions and is not used for another purpose.

BENEFIT CA has configured all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

6.7.4 Availability

To ensure availability of components, BENEFIT has implemented redundancy measures allowing a high availability of critical services.

6.8 TIMESTAMPING

The systems are synchronized with respect to a reliable source of universal time (UTC) with a time synchronization protocol (NTP) with an accuracy of at least one minute. Details about the synchronization mechanism of the server operated by the CA are described in the CA documentation. This information is confidential. The mechanism in place ensures the requirements described in CP 6.8.

7 CERTIFICATES, OCSP AND CRL PROFILES

7.1 PROFILES OF THE CERTIFICATE OF THE BENEFIT CA

The following table provide the values of the attributes of the certificate of BENEFIT CA issued by « ALMERYS ROOT CA ».

The format of this certificate and its attributes are compliant with the X.509v3 specification described in RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », ref. [RFC5280].

tbsCertList		Value
version		2 (meaning version 3)
serialNumber		
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN=ALMERYS ROOT CA OU=0002 432701639 O=ALMERYS C=FR
validity		
▶ notBefore		Creation Date
▶ notAfter		notBefore + 10 years
subject CN=commonName OI=organizationIdentifier O=organizationName C=countryName		CN=BENEFIT CA OI=NTRBH-39403-1 O=The BENEFIT Company BSC C=BH
subjectPublicKeyInfo		
▶ algorithm ➥ algorithm ➥ parameters		rsaEncryption) RSAParams : NULL
▶ subjectPublicKey		DER encoded RSAPublicKey (4096 bits)
issuerUniqueID		This field is not used
subjectUniqueID		This field is not used
Standard extensions	Critique :	
▶ authorityKeyIdentifier	No	Hash of the public key of the issuer
▶ subjectKeyIdentifier	No	Hash of the public key of the subject
▶ keyUsage	Yes	keyCertSign (5), cRLSign (6)
▶privateKeyUsagePeriod		This Extension is not used
▶certificatePolicies	No	certificate policy: identifier of the policy = 1.3.6.1.4.1.56818.1.1
▶ basicContraints ➥ cA ➥ pathLenConstraint	Yes	 True None
▶ cRLDistributionPoints	No	Distribution point of the CRL

		Name of the distribution point: Complete Name: URL=http://pki.almerys.com/almerysrootca.crl
Private extensions		
▶ authorityInfoAccess	No	[1]: accessMethod: id-ad-caIssuers accessLocation: URL=http://pki.almerys.com/almerysrootca.cer
▶subjectInfoAccess		This Extension is not used
signatureAlgorithm		
algorithm		Sha256withRSAEncryption, 4096 bits key length
parameters		NULL

7.2 END-USER CERTIFICATES

The following tables provide the default values of end-user certificates issued by BENEFIT CA. Format of this Certificate and its attributes are compliant with X.509v3 profile described in RFC 5280 « Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile », ref. [RFC5280].

7.2.1 Natural Person Signing Certificate

tbsCertList		Value
version		2 (meaning v3)
serialNumber		Random number of fixed length
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams: NULL
issuer CN=commonName OI=organisationIdentifier O=organizationName C=countryName		CN= BENEFIT CA OI= NTRBH-39403-1 O= The BENEFIT Company BSC C=BH
validity		
▶notBefore		Creation Date
▶notAfter		Creation date + 2 years
subject CN=commonName SerialNumber=unique_value C=countryName		CN = <first name> <last name> SerialNumber = UI:BH-<unique identifier> C = BH
subjectPublicKeyInfo		
▶algorithm ➥algorithm ➥parameters		 rsaEncryption RSAParams: NULL
▶subjectPublicKey		DER encoded RSAPublicKey (2048 bits)
issuerUniqueID		This field is not used
subjectUniqueID		This field is not used
Standard extensions	Critical:	
▶authorityKeyIdentifier	No	hash of the issuer public key
▶ subjectKeyIdentifier	No	hash of the subject public key

▶keyUsage	Yes	Electronic Signature Certificate nonRepudiation (contentCommitment)
▶certificatePolicies	No	Certificate Policy: Policy Identifier=1.3.6.1.4.1.56818.1.1.2.1.1 Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.benefit.bh/MediaHandler/GenericHandler/documents/CertificationAuthorityforDigitalCertificates/CertificatePracticeStatement.pdf
▶ Qualified Certificate Statements	No	- - -
▶basicContraints ➥cA ➥pathLenConstraint	No	false None
▶extKeyUsage	No	This Extension is not used
▶cRLDistributionPoints	No	Distribution point of the CRL Name of the distribution point: URL= https://pki.almerys.com/BENEFITca.crl
Private extensions		
▶authorityInfoAccess	No	[1] accessMethod: id-ad-caIssuers accessLocation: URL= https://pki.almerys.com/BENEFITca.cer [2] accessMethod: id-ad-ocsp accessLocation: URL= http://ocsp.almerys.com/
▶subjectInfoAccess		This Extension is not used
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

7.3 CERTIFICATE REVOCATION LIST (CRL)

tbsCertList		Value
version		
signature		

▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams : NULL
issuer CN=commonName OU=organizationalUnitName O=organizationName C=countryName		CN= BENEFIT CA OI= NTRBH-39403-1 O= The BENEFIT Company BSC C=BH
thisUpdate		Creation date
nextUpdate		thisUpdate + 72 hours
revokedCertificates		
▶ userCertificate		Serial of revoked certificate
▶ revocationDate		Revocation date
▶ crlEntryExtensions		
↪ reasonCode		unspecified (0) (*default value)*
crlExtensions	Critical:	
▶authorityKeyIdentifier	No	Issuer Public key hash
▶ issuerAltName	-	Not used
▶ cRLNumber	No	Incremental
▶ deltaCRLIndicator	-	Not used
▶ freshestCRL	-	Not used
▶ ExpiredCertsOnCRL	No	Value from the issuer certificate (valid from)
signatureAlgorithm		
algorithm		Sha256withRSAEncryption (OID = 1.2.840.113549.1.1.11), 4096 bits
parameters		NULL

7.4 OCSP CERTIFICATE PROFILE

tbsCertList		Value
version		2 (meaning v3)
serialNumber		Random number of fixed length
signature		
▶ algorithm		Sha256withRSAEncryption
▶ parameters		RSAParams: NULL
issuer CN=commonName OI=organisationIdentifier O=organizationName C=countryName		CN= BENEFIT CA OI= NTRBH-39403-1 O= The BENEFIT Company BSC C=BH
validity		
▶notBefore		Creation date
▶notAfter		notBefore + 1 years Maximum
subject CN=commonName OI= organisationIdentifier O=organizationName C=countryName		CN= BENEFIT OCSP UNIT X OI= NTRBH-39403-1 O= The BENEFIT Company BSC C=BH
subjectPublicKeyInfo		
▶algorithm ➥algorithm ➥parameters		 rsaEncryption RSAParams: NULL
▶subjectPublicKey		DER encoded RSAPublicKey (2048 bits)
issuerUniqueID		This field is not used
subjectUniqueID		This field is not used
Standard extensions	Critical:	
▶cRLDistributionPoints	No	Distribution point of the CRL Name of the distribution point: URL= https://pki.almerys.com/BENEFITca.crl
▶authorityKeyIdentifier	No	**hash of issuer public key**
▶ subjectKeyIdentifier	No	**hash of subject public key**
▶keyUsage	yes	digitalSignature, nonRepudiation
▶certificatePolicies	No	

		Certificate profile Policy identifier = 1.3.6.1.4.1.56818.1.1.1.1 https://www.benefit.bh/MediaHandler/GenericHandler/documents/CertificationAuthorityforDigitalCertificates/CertificatePracticeStatement.pdf
▶extKeyUsage	No	OCSPSigning
signatureAlgorithm		
algorithm		Sha256withRSAEncryption
parameters		NULL

7.5 OCSP RESPONSE PROFILE

Comment		**Value**	**Note**
Response Status		As specified in RFC 6960	
Response Type		id-pkix-ocsp-basic	
Version		V1 (0)	
Responder ID		Octet String (equaL to subject key identifier within the OCSP Certificate) or DN of the OCSP server.	
Produced At		Generalized Time	Signature Date of the response
List of Responses		Each response contains the following: certificate id; certificate status, thisUpdate, nextUpdate.	
Signature		sha256 WithRSAEncryption	
Certificates		The certificates	
Extensions			
Field	**CRITICAL**	**VALUE**	**Note**
Nonce	No	Value of the nonce attribute in the request (mandatory if nonce attribute is present within the request)	Optional

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

This Section deals with audits and evaluations of the CA or RA management to ensure the adequate operation of its PKI.
The audit of BENEFIT CA shall adhere to Kingdom of Bahrain audit requirements for Trusted Services providers.

8.1 FREQUENCIES AND/OR CIRCUMSTANCES OF EVALUATIONS

Following any significant modification of a component of the PKI, the GA carries out a security analysis and, if necessary, changes the technical and organizational measures to maintain or improve the expected level of security. The GA also regularly checks the compliance of the PKI, through a complete or partial audit of the PKI part. The frequency of this audit is at least one every year.

8.2 IDENTITY/QUALIFICATION OF EVALUATORS

The GA selects and assigns a team of auditors competent in the security of information systems and in the field of activity.

8.3 RELATIONSHIP BETWEEN EVALUATORS AND EVALUATED ENTITIES

The audit team shall not belong to the entity operating the PKI component, and shall be duly authorized to carry out the audits concerned.

8.4 SCOPE OF EVALUATION

Security audits cover all or part of the PKI and are intended to verify compliance with the commitments and practices set out in this CP/CPS.

8.5 ACTIONS TAKEN ON THE CONCLUSIONS OF EVALUATIONS

At the end of a security audit, the audit team provide to the GA a report. Status on the report can either be "success", "failure", or "to be confirmed". According to the status, the consequences of the audit are as follows:

- In the case of failure and depending on the type and critical level of non-conformities, the audit team issues recommendations to the GA which may be cessation (temporary or permanent) of activity, revocation of the component Certificate, revocation of all Certificates issued since the last positive control, etc. The choice of the measure to be applied is under the responsibility of the GA and must respect its internal security policies;

- in the event of a "to be confirmed" result, the GA submits a notice to the component specifying how long the non-conformities must be corrected. Then, a "confirmation" check will verify that all the critical points have been solved;
- if successful, the GA confirms compliance with the requirements of the CP/CPS to the controlled component.

8.6 COMMUNICATION OF RESULTS

The procedures for communicating the results of conformity audits are specified in BENEFIT internal audit procedure.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

The following information is provided in the various contractual documents drawn up between the parties: (i.e. BENEFIT, Clients of the service, and possibly suppliers performing some or all of the functions of BENEFIT CA or of the RA:

- the billing conditions of the Service proposed by BENEFIT
- the responsibilities
- the financial responsibilities
- the amount of the indemnities.

Access to the function on the state of the certificates is not subject to pricing.

9.2 FINANCIAL RESPONSIBILITY

See 9.1 «Fees ».

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

The classification of information is broken down into:

- secret (level 4 in the Security Policy);
- confidential (level 3 in the Security Policy);
- internal (level 2 in the Security Policy).

The information considered to be "secret" is at least the following:

- the private keys of the CAs of the BENEFIT PKI, of the PKI components and of the certificate Holders
- all the secrets of the PKI, in particular the information related to the management of the cryptographic modules (HSM);
- the activation data associated with the private keys of CA and of the Holders

The information considered to be "confidential" is at least the following:

- the CPS of the CA;

- the event logs of the PKI components;
- causes of revocation, unless explicitly agreed to publication by the Holder
- the registration records of the subscribers.

9.3.2 Information not considered as confidential

By default, in addition to the information already explicitly listed in paragraphs 9.3.1 Scope of Confidential Information and 9.4 Protection of personal data, information is considered confidential except for the published information listed in section 2.2 Information to be Published. Dissemination of information is only permitted with the explicit consent of the GA of BENEFIT PKI and only to people or organization who need to be aware about it.

9.3.3 Protection of confidential information and responsibilities

In particular, the CA respects the laws and regulations in force in Bahrain. In particular, it may have to make the Holders' registration record available to third parties in the case of legal proceedings.

9.4 PROTECTION OF PERSONAL DATA

9.4.1 Personal data Protection Policy

Any collection and processing of personal data by the RA and the CA BENEFIT CA are performed in conformity with the applicable regulation, in particular, with local personal Data protection regulations in the Kingdom of Bahrain.

9.4.2 Personal data

Information considered to be personal data is at least the following:

- causes of revocation of the Holder's Certificates (which are considered confidential unless expressly agreed by the Holder);
- The registration record.

They must be handled in strict compliance with the applicable law and regulations (see 9.4.1).

9.4.3 Responsibilities related to the protection of personal data.

The Holder and the Client are responsible for compliance with the applicable law (see 9.4.1).
The processing of personal data is the responsibility of BENEFIT, and TSPO board. For compliance with the Law, BENEFIT has set up an organization centred on the Personal Data Processing Manager.

In particular, Personal Data protection is ensured by BENEFIT for the following processes or area:

- Registration process
- Confidentiality of archived information
- Personal data access protection

- User consent

9.4.4 Notification and consent to use personal data use

In accordance with the applicable laws and regulations in Bahrain, the personal data provided by the subscriber to the RA is not disclosed or transferred to a third party except in the following cases: prior consent of the person concerned, Judicial decision or authorization by legal authority. Moreover, sending a direct notification to the concerned person whenever his/her personal data is used is not mandated in Bahrain.

9.4.5 Conditions for the disclosure of personal information to the judicial or administrative authorities

Any dissemination and communication of personal data to authorized third parties must comply with the applicable laws.

9.4.6 Other circumstances of disclosure of personal information

Not applicable

9.5 INTELLECTUAL PROPERTY RIGHTS

All intellectual property rights held by the BENEFIT PKI are protected by applicable law, regulations and other international conventions. They may lead to civil and criminal liability in case of non-compliance. For example, according with the applicable law the databases operated by the components of the PKI are protected by intellectual property right.

The infringement of trademarks, commerce and services, designs, distinctive signs, copyrights (e.g. software, web pages, databases, original texts, etc.) is punishable by Articles of the Code of the intellectual property.

9.6 WARRANTIES

The common obligations of the PKI components are:

- to protect and guarantee the integrity and confidentiality of their secret and/or private keys,
- to use their cryptographic keys (public, private and/or secret) for the purposes for which they were issued and with the tools specified under the conditions laid down in this CP/CPS and the documents resulting therefrom
- to respect and apply the part of the CP/CPS applicable to them (this part must be communicated to the corresponding component)
- to comply with the security audits and conformity checks requested by the duly identified and authorized stakeholders,
- to comply with the agreements or contracts binding them to each other or with the Clients,
- to document their internal operating procedures,

- to implement the technical and human means required to carry out the services under applicable conditions guaranteeing quality and safety.

9.6.1 Certification Authority

BENEFIT CA has the obligation to:

- be able to demonstrate to the Third Party Applications using its Certificates, that Certificate issuance and acceptation by the Holder Certificate has been performed in conformity with the requirements of the Section 4.4 Certificate Acceptance
- ensure and maintain the consistency between this CP/CPS.

9.6.2 Governance Authority

The GA acknowledges its responsibility in the event of fault or negligence of the CA BENEFIT CA or any of the components of the PKI, whatever their nature and gravity, which would result in the divulgation, alteration or fraudulent use of the Holder's personal data, whether this data is contained or in transit in the applications of CA BENEFIT CA systems.

In addition, the GA acknowledges that it has a general duty to oversee the security and integrity of the Certificates issued by BENEFIT CA or one of the components of the PKI. The GA is responsible for maintaining the level of security of the technical infrastructure on which the provision of services relies.

9.6.3 Registration Authority

In addition to the responsibilities described in the introduction to section 9.6 and in sections 1.3.5 and section Certificate Life-CYCLE OPERATIONAL REQUIREMENTS, the RA shall :

- maintain and protect the manipulated information in integrity and confidentiality
- ensure that Certificate registration operational processes are in line the rules set out by the CA. This rule applies in particular in the case where the RA is one of BENEFIT Client
- take all reasonable measures to ensure that the Applicants who perform certificate request are aware of their rights and obligations with respect to the use and management of keys, certificates, equipment and software.

9.6.4 Certificate Holders

A Certificate Holder shall :

- provide accurate and up-to-date information when requesting or renewing the Certificate,
- meet, during an identification process the Registration Authority to allow the verification of identity information

- manage the security of sensitive elements which are handed to it at the end of the procedure for generating his certificate. In particular, the certificate holder shall keep the private key under its sole control.
- accept the conditions of use of his private key and the corresponding certificate,

The relationship between the Holder and the CA or its components is formalized by a service contract between the Client and BENEFIT.

9.6.5 Third Party Applications

The Third-Party application shall:

- verify and respect the key usage for which a Certificate has been issued;
- check that the Certificate issued by the BENEFIT CA has a security level that is adequate for the service provided by the application;
- verify the electronic signature of BENEFIT CA that has issued the Certificate by verifying the complete certification chain until the « Almerys Root CA » certificate;
- verify and respect the obligations of the Third-Party applications described in this CP;
- check the validity of the Certificates (validity dates, revocation status).

9.6.6 Other participants

Not applicable.

9.7 DISCLAIMERS OF WARRANTIES

See 9.1« Fees ».

9.8 LIMITATIONS OF LIABILITY

See 9.1« Fees ».

9.9 INDEMNITIES

See 9.1« Fees ».

9.10 TERM AND TERMINATION OF THIS CP

9.10.1 Validity Period

The CP/CPS BENEFIT CA is applicable at least until the end of the life of the last Certificate issued under this CP.

9.10.2 Anticipated end of validity

Following the internal publication, a new version of this CP/CPS within the PKI, the CA BENEFIT CA has a 1-year period for implementing the changes needed for ensuring the compliance.

In addition, such changes do not require the early renewal of Certificates already issued, except in exceptional cases related to security issues.

9.10.3 Effects of the end of validity and clauses remaining applicable

In case of BENEFIT CA end of activity and therefore, end of validity of this CP/CPS, the requirements of the following sections shall remain applicable until the end of the life of the last certificate issued:

- 2 « Publications and Repository Responsibilities »
- 3.4 « Identification and Authentication for Revocation Request »
- 0 « Key pair and Certificate Usage »
- 4.7 « Certificate re-key »
- 4.8 « Certificate Modification »

  4.10 « Certificate Status Services»

9.11 CERTIFICATE ACCEPTANCE

9.11.1 Conduct Constituting Certificate Acceptance

The BENEFIT CA consider that the no complaint about the content of the certificate within 24 hours by the holder as an implicit acceptance of the certificate.

9.11.2 Publication of the Certificate by the CA

Signature certificates are not published.

9.11.3 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

Key pair and Certificate Usage

9.12 INDIVIDUAL NOTIFICATIONS AND COMMUNICATIONS BETWEEN PARTICIPANTS

In the case of any change in the PKI participants, the GA must, one month before the start of the operation at the latest, validate the change in order to assess the impacts on the quality level and on the functions of BENEFIT CA and its various components.

9.13 AMENDMENTS ON THIS CP

9.13.1 Procedures for amendments

Any proposed amendments to this CP/CPS shall remain in compliance with the security policy requirements of the BENEFIT PKI, and shall also respect the existing commitments with Clients and Certificate Holders. In the case of a significant change, the GA of BENEFIT PKI may have the support of technical expertise to monitor the impact of the changes.

The amendment procedure should take into account notification and the associated delay for communicating the amendments. Details are provided in the CPS associated with this CP.

This CP/CPS should be reviewed at least annually, with or without an amendment.

9.13.2 Circumstances under which the OID is to be changed

The OID of the family of Certificate issued by BENEFIT CA is part of the issued certificates, therefore, any evolution of the CA that have a major impact on the already issued certificates (for example, stronger requirements for the registration of Holders, which therefore cannot apply to Certificates already issued) must result in an evolution of the OID, so that Third Party Applications can clearly distinguish the certificates families and the associated requirements.

9.14 DISPUTE

In the event of a dispute over the interpretation of the content or the execution of this CP, an amicable resolution of conflicts is preferred. In case of complaints, subscribers can call the support centre as first step, submit complaints form (https://www.benefit.bh/Complaints/), or send an email to complaints@benefit.bh . In case of escalations, subscribers can contact the regulator.

In the absence of conciliation, any dispute concerning the validity, interpretation or execution of the present Terms & Conditions will be submitted to the qualified courts of “MANAMA city” .

9.15 GOVERNING LAW AND JURISDICTION

The law applicable to any dispute relating to the interpretation and execution of this CP/CPS is Bahrain law.
The laws and regulations applicable to this CP/CPS are, in particular, those set out in Appendix 1.
BENEFIT respects the applicable law and regulations and keeps evidence of this conformity. In particular, each time it feasible, BENEFIT:

- Provide access for persons with disabilities.
- Ensures the protection of personal date in line with the applicable laws and Regulation.

10 ANNEX 1: REFERENCE DOCUMENTS

10.1 LAWS AND REGULATIONS

Reference	Document
[REG_eIDAS]	eIDAS European Regulation

10.2 TECHNICAL DOCUMENTS

Reference	Document
[ETSI_NQCP]	ETSI TS 102 042 V2.1.1 (2009-05) Policy Requirements for Certification Authorities issuing public key certificates
[ETSI_101456]	ETSI TS 101 456 Policy Requirements for Certification Authorities qualified certificates
[ETSI_319401]	ETSI EN 319 401 General Policy Requirements for Trust Service Providers
[ETSI_319411-1]	ETSI EN 319-411-1 Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - 11/2003
[CC]	ISO/IEC 15408: Common Criteria version 2.1
[X.509]	Information Technology–Open Systems Interconnection – The Directory: Authentication Framework, Recommendation X.509, version 3
[RFC822]	Standard for the format of Arpa internet text messages, August 13, 1982, Revised by David H. Crocker
[RFC5280]	Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 5280 May 2008
[CWA14167-1]	CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
[CWA14167-2]	CWA 14167-2 (2004-02) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP)

Reference	Document
[CWA14167-4]	CWA 14167-4 (2004-02) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSO-PP)
[CWA14169]	CWA 14169 (2003-08) Secure Signature Creation Device, version « EAL 4 +»