version v 1.0, « 6 April 2021 », Public
Approved by : BENEFIT CA Governance Authority (GA)

Introduction

This document services the purpose of the Subscriber Agreement (Terms and Conditions) for the use of Natural Person Signing Certificate issued by BENEFIT Certification Authority (BENEFIT CA) under the OID: 1.3.6.1.4.1. 56818.1.1.2.1.1, and other trust services based on this certificate : Remote Digital Signature, and Certificate private key management using a QSCD, within the environment of BENEFIT Electronic Cheque (E-Cheque).

The BENEFIT Company as the owner of The Benefit CA, private key management and Signing Solutions will be referred to hereinafter as TSP (Trust Service Provider).

By agreeing to the below Terms and Conditions of the use of BENEFIT trust services.. The below Terms and Conditions summarize the key points of the applicable Certificate Policy (CP) and Certificate Practice Statement (CPS) governing the certification services for the issuance, maintenance, and management of certificates and remote digital signature.

Any collection and processing of personal data by the E-Cheque System service are performed in conformity with the applicable regulations, in particular, with local personal Data protection regulations in the Kingdom of Bahrain.

BENEFIT offers Subscribers with the possibility to sign E-Cheques with the means of Advanced Electronic Signature through the use of BenefitPay and E-Cheque mobile applications. These applications are extended by digital certificate issuing CA, remote signing solution, which conforms to the Advanced Electronic Signature standards.

Electronic cheques are paperless cheques which contains the same functionalities of the physical cheques. It contains the same following features:

- A negotiable instrument
- Has the 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 a guarantee

It is an added service to the market and not a replacement of the physical cheques. Customers can either use physical or electronic cheques. Electronic Cheques It is considered more secure since it is signed with private keys using Public Key Infrastructure technology. Moreover, it Is traceable so it can be tracked through its enter cycle and also considered to be more convenient since it can be deposited remotely via the E-Cheque applications or portal.

The overall E-Cheque Application with supporting services provide a solution that offers centralized remote digital signature services in a secure and convenient fashion.

The digital signature component (The Signer) is the cornerstone of the solution and offers a unique signing experience where issuance and management of digital certificates becomes transparent to the end-user and integrated into the business workflow. Users no longer need to carry around smart cards and worry about interoperability; the signing keys are deposited in a central safe and protected by Hardware Security Modules (HSMs). Signatories seamlessly retain sole control over the signing process using strong authentication techniques.

- The Signer allows for the Introduction of a central signing service
- Offering a unique signing experience for mobile platforms
- Conformant with European standards for issuing advanced signatures (AdES)
- Leveraging existing 2-Factor Authentication deployment through SMS OTP

- Offering non-repudiation (PDF signing)

The use of an Electronic Signature is an official and recognized way to sign documents. It is a safe method to declare your consent digitally. Your thereby applied Electronic Signature is legally binding. By accepting the agreement, i twill be considered as accepted and signed in the form provided to you. Furthermore, in case a document contains a reservation regarding amendments in writing, you acknowledge to accept such amendments also by means of the Electronic Signature. For each agreement you intend to e-sign, a One-Time-Password (OTP) is provided.

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)

E-Cheque solution supports PAdES signatures, which defines an advanced electronic signature format based on PDF (Portable Document Format). The format allows electronic signing of PDF files only. Only the enveloped signature type is supported. The allowed file extension after signing is (pdf).

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. It utilizes an Utimaco CP5.

The Subscriber has the activation data which allows the Subscriber to use the private key by using an authentication method associated with the Subscriber identity (PIN). As soon as the Subscriber enters the activation data after being requested to do so, BENEFIT creates the advanced electronic signature for the Subscriber based on the appropriate certificate.

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.

Due to the applicable banking secrecy provisions, personal data will only be transmitted in exceptional circumstances if necessary under the applicable laws of Kingdom of Bahrain. In this situation you release BENEFIT from its bank client confidentiality obligations with regard to data transmitted.

Detailed information about the processing of Subscriber Data is set out in the Privacy Notice of BENEFIT published on the Internet under the following link: https://www.benefit.bh/privacypolicy/.

version v 1.0, « 6 April 2021 », Public
Approved by : BENEFIT CA Governance Authority (GA)

BENEFIT reserves the right to amend the Privacy Notice from time to time. If the Privacy Notice has been updated, BENEFIT will take steps to inform you of the update by appropriate means, depending on how BENEFIT normally communicates with you as Account Holder.

In case of questions regarding Electronic Signature or if you wish to revoke your electronic certificate, please contact your Benefit call center or your bank call center.

The BENEFIT Trust Services Certificate Policy / Certificate Practice Statement (CP/CPS or TSP Statement) can be found at:
(https://www.benefit.bh/MediaHandler/GenericHandler/documents/CertificationAuthorityforDigitalCertificates/CertificatePracticeStatement.pdf)).

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 such as Mobile operators for SMS and internet service providers.

- TSP Contact Information
  - The BENEFIT Company
  - NBB Tower, 16th Floor, Rd No 1605, Manama Center, Kingdom of Bahrain
  - Phone: 17506065
  - Email contact: riyadm@benefit.bh

Terms & Conditions

- These Terms and Conditions of use shall apply in the relationship between The BENEFIT Company (The TSP) and the Subscriber within the E-Cheque system for your use of the BENEFIT trust services with advanced certificates for advanced electronic signatures.
- If the registered mobile device of the Digital Certificate Holder referred to above as the customer was deactivated, the Digital Certificate will not be accessible.
- Each Digital Certificate Holder can have only one registered device under his/her account.
- The Digital Certificate Holder has access to a remote signing service. The private and public keys associated with Digital Certificate are securely stored.
- Should the device holding the E-Cheque Application gets compromised, the digital certificate holder shall deactivate the compromised device and register from new device then log in from the new device.
- The Digital Certificate Holder has no direct access to the revocation service. For revoking the Digital Certificate, he/she shall contact all bank(s) having relationship with to deactivate their signatory profile at E-Cheque.
  - BenefitPay users shall contact all related banks support centers (available 24x7) and request to deactivate their account.
    - The bank will identify the Digital Certificate Holder prior revoking the Digital Certificate.

- E-Cheque application users shall contact all related banks support centers (available 24x7) and request to deactivate their accounts.
  - The bank will identify the customer owning the Digital Certificate prior revoking the Digital Certificate.

In both cases above customers can also contact BENEFIT Customer Support Center for guidance on how to revoke certificates.

- BENEFIT Company (also acts as the registration authority) checks the identity of subscribers in the identity verification process. In the verification process for electronic certificate and advanced electronic signatures, the user provided identity information is compared to data provided earlier to subscriber corresponding bank during bank account opening face-to-face identification process. If information matches and validated then user can be registered in the platform.
- Digital Certificates issued by the TSP are certificates aiming at Signature of natural persons representing themselves or a natural person using the digital certificate for professional use and act as an authorized signatory of the accounts of entity it belongs to.
- The Digital Certificate/Signing Key (private key) is created on Qualified Electronic Signature Creation Device (QSCD) hardware with 2048-bit key size. The maximal validity period of the certificate is “two years”.
- The Digital Certificate issued by the TSP may only be used for the purpose of signature as defined in the key usage of the CP/CPS.
- The Digital Certificates are not usable beyond their period of validity of two years.
- Benefit E-Cheque platform creates the advanced certificate and the cryptographic pair of keys for the signing process on a special server (Hardware Security Module, HSM). The advanced certificate is a certificate validates the assignment of a public key (of the asymmetrical cryptographic pair of keys) to the Subscriber. The Subscriber has activation data which allows to use the private key that belongs to the same subscriber by using an authentication method associated with the subscriber identity (SMS One Time Password). As soon as the subscriber enters the activation data after being requested to do so, E-Cheque platform creates the advanced electronic signature for the Subscriber based on the certificate assigned to the same Subscriber.

- TSP Responsibilities :
  - Ensure the CP/CPS, publication is effective as soon as necessary to always ensure consistency between the published information and the actual commitments, means and procedures of the CA and signing solutions. The valid CP/CPS is published before the first creation of a Subscriber certificate or issuance of digital signatures or private keys for E-Cheque customers.
  - At its own discretion and without giving any notice has the right to temporary suspend or restrict Subscriber access to the services, provide it has evidence or has doubts that the Subscriber is using the E-Cheque and its provided services in violation of the applicable laws and this document.
  - Shall publish its services CP/CPS
  - A conformity assessment of the TSP to the applicable certificate policy and certificate policy statement may be carried out at the request of Benefit PKI Governance Authority (GA).
  - The GA ensures that such conformity assessment is performed at least once every 1 year. The TSP keeps registration data and event logs for at least ten years.
  - The TSP has the right to amend and supplement these Terms and Conditions but shall make them available publicly available at all time on: https://www.benefit.bh/MediaHandler/GenericHandler/documents/CertificationAuthorityforDigitalCertificates/SubscriberAgreement.pdf

  - Shall record and keep accessibility to these records for 10 years, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service shall be recorded and kept.
- The customer/subscriber shall:
  - Use the issued digital certificates and created digital signatures within the E-Cheque system
  - Securely manage the secrets and elements, in particular the customer shall keep his/her passwords, private key/Digital Signature activation code (PIN) under his/her sole control.
  - Accept the terms and conditions listed in this document.
  - Inform the TSP of any changes concerning the information contained in their Certificate.
  - Without delay, the customer shall request device de-activation and certificate revocation in the event of loss, or suspected compromise of his/her private key (or activation data). The Subscriber shall also Immediately cease creating signatures.
  - Use the Certificate in a way that does not violate applicable laws in the Kingdom of Bahrain.
  - Upon termination of this Agreement, revocation, or expiration of the Certificate the Subscriber must immediately cease any use of the Digital Certificate And shall immediately cease creating new digital signatures.
  - agree that any use of the Certificate to sign or otherwise approve the contents of any electronic record or message is attributable to Subscriber. Subscriber agrees to be legally bound by the contents of any such electronic record or message.
  - The Subscriber, being the certificate holder, is responsible of providing accurate information when registering to the service. A natural person must have a valid and active relationship with his/her bank where face to face KYC has already been established by the bank. The bank shall authenticate and authorize a natural person for registration purpose. A natural person using the certificate for professional use must fill the registration forms available in his/her bank branches for face-to-face KYC.
  -
- The server signing shall ensure:
  - the private key shall not be used for signing except within a QSCD.
  - the subject's private key shall be used under the subject's sole control.
  - the subject's key pair should be used only for electronic signatures
- Relying parties are obligated to:
  - verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party through the Online Certificate Status Protocol (OCSP) service: http://ocsp.almerys.com/
  - take account of any limitations on the usage of the certificate indicated to the relying party in the certificate policy
  - take any other precautions prescribed in the CPS and applicable CP
- Subscribers, Relying Parties, Application Software Suppliers, and other third parties should call Benefit call Centre for any complaints, reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates and digital signatures. Benefit Call center can be reached at 00973 17 506065, or by email or by phone via the contact information published above.
- In case of complaints, subscribers can call BENEFIT support centre as first step or by sending an email to complaints@benefit.bh . In case of escalations, subscribers can contact the regulator.
-

- Subject to the provisions of applicable law and regulations, the TSP is not responsible for any unauthorized use of certificate or misusage of certificates. This limit of responsibility is also applicable for the activation data, CRL and any software or hardware provided by the TSP.
    - The TSP is, particularly, not responsible for any damage resulting of:
        - The use of a key pair for another usage than the one agreed;
        - Force majeure as defined in the “local Law”.
    - TSP is also not responsible for any damage resulting from errors or inaccuracies in the information contained in Certificates, where these errors or inaccuracies result directly from the erroneous nature of the information provided.
- This Subscriber Agreement is governed by Kingdom of Bahrain law.
- The Subscriber and TSP shall endeavor to amicably settle any dispute concerning the interpretation or execution of the service as soon as possible.
- 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” .
- On the other hand, from the date of certification, as part of the above mentioned ETSI standards compliance and certification, an assurance and compliance audit will be carried out annually by the accredited conformity assessment.