

THE BENEFIT COMPANY



BENEFIT TRUST SERVICES

PKI – POLICY DISCLOSURE STATEMENT

Approved by: BENEFIT Certificate Authority Governance Committee

PUBLIC



Version:1.0

Effective Date: 06/04/2021

Contents

Document Update Notice	3
1. Introduction	3
2. TSP Contact Information	3
3. Certificate type, validation procedures and usage	4
4. Reliance Limit	4
5. Obligation of Subscribers	4
6. Certificate status checking obligations of relying parties	5
7. Limited warranty and disclaimer/Limitation of liability.....	5
8. Applicable agreements, CPS, CP	6
9. Privacy Policy.....	6
10. Refund Policy	6
11. Applicable law, complaints and dispute resolution	7
12. TSP and repository licenses, trust marks, and audit	7
13. Final Signoff.....	8

Document Update Notice

Version Number	Revision Date	Nature of Change	Date Approved
1	01 March 2021	Initial Draft	06 April 2021

1. Introduction

The present document is the "The BENEFIT Company" public "PKI Disclosure statement" (PDS) for the "BENEFIT CA". Throughout this document, the use of the term "PDS" refers to the present document, unless otherwise specified. BENEFIT acts as a Trust Service Provider (TSP).

The purpose of the PDS is to:

- summaries the key points of the CP and CPS for the benefit of Subscribers and Relying Parties
- Provide additional detail and further provisions that apply to the CP/CPS.

2. TSP Contact Information

Governance " BENEFIT CA" 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
--

The Certificate Holder (Subscriber) has no direct access to the revocation service. For revoking a certificate, he or she shall either:

- Contact the support center for "BENEFIT CA" support by phone to the call center: 00973 17 506065 (schedule: 24/7). In this case, the support center will identify the Subscriber and guide the Subscriber through the revocation process.
- Contact his/her bank to deactivate BenefitPay or E-Cheque accounts.

3. Certificate type, validation procedures and usage

Certificates issued by “BENEFIT CA” are certificates aiming at Signature of natural person.

Certificate Family	Issued to the public	OID	Short Description
Natural Person Signing Certificate	yes	1.3.6.1.4.1.56818.1.1.2.1.1	<ul style="list-style-type: none"> 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+). 2048-bit key size and with maximal validity period of “2 years”, and with a key usage limited to the support of advanced electronic signature.

4. Reliance Limit

- Certificates issued by "BENEFIT CA" may only be used for the purposes of digital signature within the E-Cheque platform.
- Certificates are issued for a maximum period of "2 years".
- These Certificates are not usable beyond their period of validity;
- The "The BENEFIT Company" CA keeps registration data and event logs for at least 10 years

5. Obligation of Subscribers

Certificate subscribers are responsible for the accuracy of the information they provide during their relationship with The BENEFIT CA. They especially must:

- Use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement “Terms and Conditions”. The Natural signing Certificate is for use in electronic signatures with non-repudiation within E-Cheque platform,
- Provide accurate and up-to-date information upon Certificate request and at all times,
- Meet customer registration requirements at customer Bank with the Registration Authority to verify their ID information,

- Protect the Private Key by taking all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key included in the issued Certificate,
- Securely manage the secrets and elements which are created at the end of certificate generating procedures, in particular the Subscriber shall keep its activation code (PIN) under its sole control,
- Acceptance of Certificate by reviewing and verifying the Certificate contents for accuracy
- Accept terms and conditions of usage of the key and corresponding certificate,
- Inform the BENEFIT Company of any changes concerning the information contained in their Certificate,
- Submit, without delay, certificate revocation request BENEFIT CA support call center or contact Subscriber Bank in the event of loss, or suspected compromise or misuse of their private key (or activation data), or if any information in the Certificate is or becomes incorrect or inaccurate, and
- Terminate the use of Certificate Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate.

6. Certificate status checking obligations of relying parties

Relying Party Applications withing BENEFIT E-Cheque platform when using the certificates shall:

- Verify that the key usage for which the Certificate was issued is appropriate for its certificate usage,.
- Verify the applicable limitations on the usage of Certificates and agrees to BENEFIT limitations on liability related to the use of Certificates,
- Read, understand, and agree to the CP/CPS of BENEFIT CA,
- Not use BENEFIT CA Certificates if the Certificate has expired or been revoked,
- Verify that the used Certificate has been issued by "BENEFIT CA" ,
- Verify the download access to the list of revoked certificates (CRL) of "BENEFIT CA" or ability to access Online Certificate Status Protocol, and
- Verify the Certificate signature, and the Certification chain, up to the "ALMERY'S ROOT CA" Certificate and check the validity of each certificate with respect to the CRL or OCSP (if possible) of each involved CA.

The CA certificate of "BENEFIT CA" is available at the following address :

<https://pki.almerys.com/befinitca.cer>

7. Limited warranty and disclaimer/Limitation of liability

Subject to the provisions of applicable law and Regulations, “BENEFIT CA” is not responsible for any unauthorized use of certificate or misuse of Certificates. This limit of responsibility is also applicable for the activation data, CRL and any software or hardware provided by the CA.

“BENEFIT CA” is, particularly, not responsible for any damage resulting of:

- The use of a key pair for another usage than the one agreed;
- The use of expired certificates;
- « Force majeure » as defined in the local Laws of Kingdom of Bahrain.
- Use of the certificate outside E-Cheque platform

“BENEFIT CA” 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.

8. Applicable agreements, CPS, CP

The BENEFIT CA CP/CPS, the Subscriber Agreement “Terms and Conditions” can be found on:

- CP/CPS

<https://www.benefit.bh/MediaHandler/GenericHandler/documents/CertificationAuthorityforDigitalCertificates/CertificatePracticeStatement.pdf>

- Subscriber Agreement (Terms & Conditions)

<https://www.benefit.bh/MediaHandler/GenericHandler/documents/CertificationAuthorityforDigitalCertificates/SubscriberAgreement.pdf>

- PKI Policy Disclosure Statement

<https://www.benefit.bh/MediaHandler/GenericHandler/documents/CertificationAuthorityforDigitalCertificates/PolicyDisclosureStatement.pdf>

9. Privacy Policy

Any collection and processing of personal data relating to the Subscriber is carried out in strict compliance with the applicable laws and regulations in the Kingdom of Bahrain

10. Refund Policy

No refund will be made.

11. Applicable law, complaints and dispute resolution

These Terms & Conditions are governed by Kingdom of Bahrain laws.

The parties shall endeavor to amicably settle any dispute concerning the interpretation or execution of the contract 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".

12. TSP and repository licenses, trust marks, and audit

About the provision of Advanced Signature Certificate, "The BENEFIT Company" is acting as TSP through its CA, operates:

- Following the terms of the Local Regulation,
- According to the ETSI EN 319 411-1, under Extended Normalized Certificate Policy (NCP+)
- According to its Certificate Policy/Certificate Practice Statement identified by the OID "1.3.6.1.4.1.56818.1.1.1.1"

A conformity assessment "BENEFIT CA" to the applicable CP and CPS may be carried out at the request of "The BENEFIT Company" PKI Governance Authority (GA).

The GA ensures that such conformity assessment is performed at least once a Year. On the other hand, from the date of certification, as part of the ETSI EN 319 401 and ETSI 319 411-1 certification, an assurance and compliance audit will be carried out annually by an accredited conformity assessment body.

13. Final Signoff

Title	PKI – POLICY DISCLOSURE STATEMENT
Doc	: BENEFIT-PKICA-DS
Version	: 1.0
Revision Date	: 1 March 2021

Prepared/Modified By:

Approved By:

Shafaq Al Kooheji

Riyad Al Maraj

Member of CAGC

Chairman of CAGC

Date: 06 April 2021

Date: 06 April 2021