CONDITIONS OF USE OF BNP PARIBAS FORTIS SIGNATURE SERVICE CERTIFICATES

April 2023 Edition

SUBJECT

The purpose of these General Terms and Conditions (GTC) is to define the rights and obligations of the parties in connection with the provision of the Service. These are supplemented by the General Conditions of Services (GCS) of Mediacert OTU acting as Certification Authority that the Signatory accepts jointly with these GTC. These GTC are available at: https://www.mediacert.com/

DESIGNATION OF CERTIFICATE POLICIES

These GTC apply to certificates issued under the Certificate Policy (CP) and the BNP Paribas Fortis Registration Policy (RP) attached to the CP, documents identified by the following Object Identifier (OID):

- **CP CA « OTU CA n° 1 »: 1.2.250.1.111.20.5.6.1**
- **CP CA « OTU CA n° 2 »: 1.2.250.1.111.20.5.6.5**
- **RP RA BNP Paribas Fortis: 1.2.250.1.62.10.202.6.5.1**

The Service meets the "Lightweight Certificate Policy" requirements of the ETSI EN 319 411-1 standard.
The RP and CP are available online on the site https://www.mediacert.com/

RESTRICTIONS ON THE USE OF THE SERVICE

The Service is reserved to BNP PARIBAS FORTIS (BNP Paribas Fortis, Hello Bank! and Fintro) Clients for the electronic signature of documents in connection with the services distributed by BNP PARIBAS FORTIS (operating under the Fintro brand, hereinafter “BNP PARIBAS FORTIS”).

Where BNP PARIBAS FORTIS so requires, a Certificate may be issued by BNP PARIBAS FORTIS in the name of the Signatory. In order to do so, the Signatory authorises BNP Paribas Fortis, for the electronic data that it provides on the screen (for example, the file containing data related to an instruction or to the subscription of a service by the Client or on its behalf), to create or have created an Electronic Signature Certificate identifying the Signatory and to create its electronic signature by means of the Certificate.

The use of Certificates issued under the Service is strictly limited to the cases described in the applicable RP.

DEFINITIONS

Certificate Authority (CA): department responsible for signing, issuing and maintaining Certificates of a Public Key Infrastructure in accordance with the Certification Policy.

Registration Authority (RA): designates the authority responsible for identifying the Signatory to validate or reject requests for the issuance of a Certificate, in accordance with its Registration Policy. The RA ensuring this role within the framework of the execution of the Service is BNP Paribas Fortis.

Certificate: electronic file issued by a Certificate Authority attesting the identity of a Signatory. The certificate is valid for 50 minutes. The Certificate contains the public key assigned to the Signatory.

Private key: cryptographic key assigned to the Signatory to sign, generated at the same time as the public key (private key and public key together forming the "bi-key").

Client: any natural or legal person contractually bound with BNP PARIBAS FORTIS.

Certificate Policy or CP: refers to the set of rules, procedures and requirements to which stakeholders around the Service are subject, as well as the specifications of certificates.

Registration Policy or RP: refers to the set of rules identified by an OID (Unique Identifier) and published by the Registration Authority. The purpose of the Registration Policy is to describe the registration process implemented by the Registration Authority, the set of rules and requirements to which the Registration Authority complies in setting up and the provision of the Service as well as the conditions of use of the certificates issued by the “OTU CA” CA issued on behalf of BNP PARIBAS FORTIS.

Service: refers to the key management infrastructure service through which BNP PARIBAS FORTIS makes available to the Client an ephemeral Electronic Signature Certificate for the purpose of personal electronic signature of documents by the Signatory.

Signatory: any user of the Service who is issued a Certificate (in the RP called "holder") in relation to his or her identity, either as an individual Client signing a document via such Certificate, or as a person authorized by a Client to sign on his or her behalf a document via such a Certificate.

OBLIGATIONS OF BNP PARIBAS FORTIS

BNP PARIBAS FORTIS commits to:

1. Provide the Signatory with accurate and complete information in accordance with the applicable CP and RP.

2. Use the Service in accordance with the limits of use defined in the applicable CP and RP.

3. Prevent any unauthorized use of the Signatory's private key.

4. Notify the Signatory without delay if any of the following events occur during the period of validity of the Certificate:
   a) The Signatory's Private Key has been lost, stolen, or is potentially compromised;
   b) Control over the Signatory's Private Key has been lost due to a compromise of the activation data or for any other reason;
   c) Inaccuracies in the Certificate brought to the attention of BNP PARIBAS FORTIS.

5. Definitely prohibit the use of the Private Key immediately after its compromise.

6. Ensure that no unauthorized use is made of the Private Key after being informed of the revocation of the Certificate or the compromise of the issuing Certification Authority.

7. To set up all the means necessary for the good execution of services: it determines for this purpose the composition of its team which must meet the requirements of the Service(s) (adapted profiles and qualifications, professional experience, etc.).

8. Maintain its team at the required level by ensuring the information and training necessary for its performance through the organization of internships, regular meetings within the company, communication of any internal documents or circulars, etc.

9. Ensure the implementation of the Service, with availability compatible with the needs of the user application and structured documents complying with recognized quality standards in the profession.

10. Not to use the cryptographic means generated on behalf of the Signatory for purposes other than those for which BNP PARIBAS FORTIS has been mandated by it.

11. Ensure "exclusive control" by the Signatory of the Private Key generated on its behalf.

12. Immediately generate the Certificate when requested by the Service using ETSI TS 119 312 compliant key sizes and parameters.

13. Immediately revoke the Certificate if requested by the Signatory directly through the Service.

OBLIGATIONS OF THE SIGNATORY

The Signatory is committed to:

1. Use the Service within the limits of use defined in the CP and RP.

2. Prevent any unauthorized use of the Service.

3. Notify BNP PARIBAS FORTIS without delay if any of the following events occur during the period of validity of the Certificate:

a) Control over the Signatory's Private Key has been lost due to a compromise in its means of authentication (e. g. PIN) or for any other reason;
b) Incorrectness of the Certificate brought to the attention of the Signatory.

4. Ensure that control over the means of authentication is maintained.
The bearer shall notify BNP PARIBAS FORTIS without delay of any event related to the loss of control or the security of its means of authentication.

5. Accept the consultation of its Certificate for the purpose of validating its electronic signature in connection with the services distributed by BNP PARIBAS FORTIS.

6. Verify his or her identity as posted before any electronic signature transaction, and interrupt the electronic signature process if he or she notices an error in it so that the Service can revoke the generated Certificate.

7. Accept the Certificate generated on the basis of the identity as displayed by completing the document signature process.

8. Notify the Service of any inconsistency in its identity so that it may revoke or have revoked the Signatory's means of authentication, if necessary.

9. It is agreed that in the strict context of the use of the PKI (Public Key Infrastructure) registered in the Adobe AATL program, the following provisions shall apply:

- The Signatory delegates to BNP Paribas FORTIS the responsibility for the use of cryptographic means (bi-keys) generated on its behalf in connection with the Service.
- In order to manage the life cycle of the Certificate that it issues, BNP PARIBAS FORTIS is bound by an obligation of means, in accordance with the CP.

INFORMATION FOR CERTIFICATE VALIDATION

The BNP PARIBAS FORTIS CA provides a mechanism for the free consultation of information services on the status of the signatories' certificates.
Certificate Revocation List (CRL):

- **1.2.250.1.111.20.5.6.1:** **http://pki.mediacert.com/OTU2021S1/crl**
- **1.2.250.1.111.20.5.6.5:** **http://pki-s2.mediacert.com/OTU2021S2/crl**

Online Certificate Status Protocol (OCSP)

- **1.2.250.1.111.20.5.6.1:** **http://pki.mediacert.com/OTU2021S1/ocsp**
- **1.2.250.1.111.20.5.6.5:** **http://pki-s2.mediacert.com/OTU2021S2/ocsp**

In addition, information on certificates issued by the CA Mediacert OTU is available in the form of CRLs
at the distribution point:
https://mediacert.com/trustCA2021/trustCA2021.crl

INFORMATION STORAGE BY BNP PARIBAS FORTIS

The Signatory acknowledges and agrees that BNP PARIBAS FORTIS will keep the following information :
1. Registration files and personal data relating to the identity of the Signatory will be kept until 10 years after the end of relation between the Client and BNP PARIBAS FORTIS.
2. The signed document will be kept depending on the document type for a period of minimum 10 and maximum 30 years from:
(i) the end of the contract
(ii) the expiration date of the document (if a validity period is applicable)
(iii) the document date if (i) and (ii) are not applicable.
3. The technical traces ensuring the accountability of the actions will be kept depending on the document type for a period of minimum 10 and maximum 30 years from:
(i) the end of the contract
(ii) the expiration date of the document (if a validity period is applicable)
(iii) the document date if (i) and (ii) are not applicable.
4. The archiving period of elements specific to the CA (CRL, technical traces of the CA ...) is specified in the CP "OTU CA".
5. In accordance with the regulations, the information relating to the Service and the certificates issued, including the registration files, may be transmitted to another provider of trust services in the event of the Services being terminated, and this for the purposes of Service continuity.

LIMITATION OF BNP PARIBAS FORTIS'S LIABILITY

BNP PARIBAS FORTIS, provider of the Service, is not liable for any damages arising out of or in connection with the use of the Service. Any liability in connection with the use of the Service is the sole responsibility of the Customer.
BNP PARIBAS FORTIS shall not be held liable for any damage resulting from an error in the identity of the Signatory not reported by the Signatory and presented in the Certificates that BNP PARIBAS FORTIS issues as part of the Service.

AUDIT

The CA Mediacert OTU and the RA BNP PARIBAS FORTIS have been certified according to the European scheme ETSI EN 319 411-1 LCP by an audit firm accredited by COFRAC (Comité Français d'Accréditation). Each year, a control and surveillance audit is carried out by this firm on the Service to renew this certification.

PROTECTION OF PERSONAL DATA

BNP PARIBAS FORTIS processes your personal data in accordance with the terms of the Privacy Notice available on https://www.bnpparibasfortis.com/footer-pages/privacy-policy and also at your disposal in all branches.

APPLICABLE LAW AND JURISDICTION

In the event of any dispute relating to the interpretation, validity or performance of these GTC, the parties give express and exclusive jurisdiction to the laws and regulations in force on Belgian territory and to the Belgian courts.

COMPLAINTS AND DISPUTES

In the event of a complaint or a dispute, the Signatory must follow the process described in article 21 of the BNP Paribas Fintro General Banking Terms and Conditions if certificates are used in the context of Fintro Easy Banking Web or Fintro Easy Banking Business.

EFFECTIVE DATE OF THE GTC

The General Terms and Conditions shall take effect as of their acceptance by the Signatory and shall apply for the entire duration of the storage of registration files.

POINT OF CONTACT

For any inquiries regarding these GTC, the Signatory may contact Fintro at 02 433 45 20 (FR) or 02 433 45 10 (NL) if certificates are used in the context of Fintro Easy Banking Web, Fintro Easy Banking App or Fintro Easy Banking Business.