CONDITIONS D'UTILISATION DES CERTIFICATS DE SERVICE DE SIGNATURE BNP PARIBAS FORTIS

Edition Avril 2023

OBJET

Les présentes Conditions Générales d'Utilisation (CGU) ont pour objet de définir les droits et obligations des parties dans le cadre de la fourniture du Service. Celles-ci sont complétées par les conditions générales des services (CGS) de Mediacert OTU agissant comme autorité de certification que le Signataire accepte conjointement aux présentes CGU. Ces CGS sont disponibles à l'adresse : https://www.mediacert.com/

DESIGNATION DES POLITIQUES DE CERTIFICATION

Les présentes CGU s'appliquent aux certificats émis dans le cadre de la Politique de certification (PC) et de la politique d'enregistrement (PE) de BNP Paribas Fortis rattachée à la PC, documents identifiés par les OID (Object Identifier) suivants :

- **PC AC « OTU CA n° 1 » : 1.2.250.1.111.20.5.6.1**
- **PC AC « OTU CA n° 2 » : 1.2.250.1.111.20.5.6.5**
- **PE AE BNP Paribas Fortis : 1.2.250.1.62.10.202.6.5.1**

Le Service correspond aux exigences « Lightweight Certificate Policy » définie par la norme ETSI EN 319 411-1.

Les PE et PC sont disponibles en ligne sur le site https://www.mediacert.com/

LIMITATIONS D'USAGE DU SERVICE

Le Service est réservé aux Clients de BNP PARIBAS FORTIS (BNP Paribas Fortis, Hello Bank! and Fintro) pour la signature électronique de documents dans le cadre des services distribués par BNP PARIBAS FORTIS (agissant sous la marque Fintro, ci-après "BNP PARIBAS FORTIS").

Lorsque BNP PARIBAS FORTIS le requiert, un Certificat peut être émis au nom du Signataire par BNP PARIBAS FORTIS. Pour ce faire, le Signataire autorise BNP PARIBAS FORTIS, pour les données électroniques qu'elle lui propose à l'écran (par exemple le fichier contenant les données liées à une instruction ou à la souscription d'un service par le Client ou pour son compte), à créer ou faire créer un Certificat de signature électronique identifiant le Signataire et à créer sa signature électronique au moyen du Certificat.

L'usage des Certificats émis dans le cadre du Service est strictement limité aux cas décrits dans la PE applicable.

DEFINITIONS

Autorité de certification (AC) : service chargé de signer, émettre et maintenir les Certificats d'une infrastructure à clés publiques, conformément à la Politique de Certification.

Autorité d'enregistrement (AE) : désigne l'autorité chargée d'identifier le Signataire pour valider ou rejeter les demandes d'émission d'un Certificat, et ce conformément à sa Politique d'Enregistrement. L'AE assurant ce rôle dans le cadre de l'exécution du Service est BNP Paribas Fortis.

Certificat : fichier électronique délivré par une Autorité de Certification attestant l'identité d'un Signataire. Le certificat est valide pendant une durée de 50 minutes. Le Certificat contient la clé publique attribuée au Signataire.

Clé privée : clé cryptographique attribuée au Signataire pour signer, générée en même temps que la clé publique (la clé privée et la clé publique formant ensemble la « bi-clé »).

Client : désigne toute personne physique ou morale liée contractuellement avec BNP PARIBAS FORTIS.

Politique de Certification ou PC : désigne l'ensemble de règles, procédures et exigences auxquelles sont soumises les parties prenantes autour du Service ainsi que les spécifications des certificats.

Politique d'enregistrement ou PE : désigne l'ensemble de règles identifiées par un OID (identificateur unique) et publiées par l'Autorité de d'enregistrement. La Politique d'enregistrement a pour objet de décrire le processus d'enregistrement mis en œuvre par l'Autorité d'enregistrement, l'ensemble de règles et d'exigences auxquelles se conforme l'Autorité d'enregistrement dans la mise en place et la fourniture du Service ainsi que les conditions d'utilisation des certificats émis par l'AC « OTU CA » émis pour le compte de BNP PARIBAS FORTIS.

Service : désigne le service d'infrastructure de gestion des clés par lequel BNP PARIBAS FORTIS met à disposition du Client un Certificat de signature électronique éphémère à des fins de signature électronique personnelle de documents par le Signataire.

Signataire : désigne tout utilisateur du Service se voyant délivrer un Certificat (appelé « porteur » dans la PE) en rapport avec son identité, soit qu'il s'agisse d'un Client personne physique signant un document via un tel Certificat, soit d'une personne autorisée par un Client à signer pour son compte un document via un tel Certificat.

OBLIGATIONS DE BNP PARIBAS FORTIS

BNP PARIBAS FORTIS s'engage à :

1. Transmettre au Signataire des informations exactes et complètes conformément à la PC et à la PE applicables.

2. Utiliser le Service conformément aux limites d'usage définies dans la PC et la PE applicables.

3. Prévenir toute utilisation non autorisée de la clé privée du Signataire.

4. Notifier sans délai au Signataire si l'un des évènements suivants se produit pendant la période de validité du Certificat :
   a) La Clé privée du Signataire a été perdue, volée, ou est potentiellement compromise ;
   b) Le contrôle sur la Clé privée du Signataire a été perdu du fait d'une compromission de la donnée d'activation ou pour toute autre raison ;
   c) Inexactitudes du Certificat portées à la connaissance de BNP PARIBAS FORTIS.

5. Interdire définitivement l'utilisation de la Clé privée immédiatement après sa compromission.

6. S'assurer qu'aucune utilisation non autorisée n'est faite de la Clé privée après avoir été informé de la révocation du Certificat ou de la compromission de l'Autorité de Certification émettrice.

7. Mettre en place tous les moyens nécessaires à la bonne exécution des prestations : elle détermine à cet effet la composition de son équipe qui doit répondre aux exigences du ou des Service(s) (profils et qualifications adaptés, expériences professionnelles, etc.).

8. Maintenir son équipe au niveau requis en lui assurant les informations et la formation nécessaires à sa prestation par l'organisation de stages, de réunions régulières au sein de

l'entreprise, de communication de tout document ou circulaire internes, etc.

9. Assurer la mise en œuvre du Service, avec une disponibilité compatible avec le besoin de l'application utilisatrice et des documents structurés répondant à des normes de qualité reconnues dans la profession.

10. Ne pas utiliser les moyens cryptographiques générés pour le compte du Signataire à des fins autres que celles pour lesquelles il a mandaté BNP PARIBAS FORTIS.

11. Assurer le "contrôle exclusif" par le Signataire de la Clé privée générée pour le compte de celui-ci.

12. Générer immédiatement le Certificat lors de la demande de ce dernier par le Service en utilisant des tailles et paramètres de clés conformes à la norme ETSI TS 119 312.

13. Révoquer immédiatement le Certificat en cas de demande par le Signataire directement à travers le Service.

OBLIGATIONS DU SIGNATAIRE

Le Signataire s'engage à :

1. Utiliser le Service conformément aux limites d'usage définies dans la PC et la PE.

2. Prévenir toute utilisation non autorisée du Service.

3. Notifier sans délai à BNP PARIBAS FORTIS si l'un des évènements suivants se produit pendant la période de validité du Certificat :

a) Le contrôle sur la Clé privée du Signataire a été perdu du fait d'une compromission de ses moyens d'authentification (par ex. un code PIN) ou pour toute autre raison ;
b) Inexactitudes du Certificat portées à la connaissance du Signataire.

4. Veiller à garder le contrôle sur ses moyens d'authentification. Le porteur notifiera sans délais à BNP PARIBAS FORTIS tout événement lié à la perte de contrôle ou à la sécurité de ses moyens d'authentification.

5. Accepter la consultation de son Certificat aux fins notamment de validation de sa signature électronique dans le cadre des services distribués par BNP PARIBAS FORTIS.

6. Vérifier son identité telle qu'affichée avant toute opération de signature électronique, et interrompre le processus de signature électronique s'il remarque une erreur dans celle-ci afin que le Service révoque le Certificat généré.

7. Accepter le Certificat généré sur base de l'identité telle qu'affichée en finalisant le processus de signature des documents.

8. Notifier au Service toute incohérence dans son identité pour que celui-ci procède ou fasse procéder à la révocation du moyen d'authentification du Signataire le cas échéant.

9. Il est convenu que dans le strict cadre de l'utilisation de l'IGC (Infrastructure de Gestion de Clés) inscrite au programme Adobe AATL, les dispositions suivantes s'appliquent :

- Le Signataire délègue à BNP Paribas FORTIS la responsabilité de l'utilisation des moyens cryptographiques (bi-clés) générés pour son compte dans le cadre du Service.
- Pour la gestion du cycle de vie du Certificat qu'il émet, BNP PARIBAS FORTIS est tenue à une obligation de moyens, en conformité avec la PC.

INFORMATION POUR LA VALIDATION DES CERTIFICATS

L'AC Mediacert OTU met à disposition un mécanisme de consultation libre des services d'information sur le statut des certificats des signataires.
Liste des certificats révoqués (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

Protocole de vérification en ligne de certificats (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

Par ailleurs, l'information quant aux certificats de l'autorité de certification Mediacert OTU est disponible sous forme de CRL au point de distribution:
https://mediacert.com/trustCA2021/trustCA2021.crl

CONSERVATION DES INFORMATIONS PAR BNP PARIBAS FORTIS

Le Signataire reconnaît et accepte que BNP PARIBAS FORTIS conserve les informations suivantes :

1. Les dossiers d'enregistrement et les données liées à l'identité du Signataire seront conservés pour une durée de 10 ans à compter de la fin de la relation entre le Client et BNP PARIBAS FORTIS.

2. Le document signé sera conservé en fonction du type de document pour une durée de minimum 10 et maximum 30 ans à compter :
(i) de la fin du contrat
(ii) de l'expiration du document si une période de validité s'applique
(iii) de la date du document si (i) et (ii) ne s'appliquent pas.

3. Les traces techniques assurant l'imputabilité des actions seront conservées en fonction du type de document pour une durée de minimum 10 et maximum 30 ans à compter :
(i) de la fin du contrat
(ii) de l'expiration du document si une période de validité s'applique
(iii) de la date du document si (i) et (ii) ne s'appliquent pas.

- La durée de conservation des éléments spécifiques à l'AC (CRL, traces techniques de l'AC…) est précisée dans la PC « OTU CA »

5. Conformément à la réglementation les informations relatives au Service et aux certificats émis, y compris les dossiers

d'enregistrement, pourront être transmises à un autre prestataire de services de confiances en cas d'arrêt des Services et ce à des fins d'assurer le suivi du Service.

LIMITE DE RESPONSABILITE DE BNP PARIBAS FORTIS

BNP PARIBAS FORTIS, prestataire du Service, n'est pas responsable des dommages découlant ou liés à l'utilisation du Service. Toute responsabilité liée à l'utilisation du Service incombe au seul Client.

BNP PARIBAS FORTIS ne saurait être tenue responsable de tout dommage résultant d'une erreur dans l'identité du Signataire non rapportée par celui-ci et présente dans les Certificats que BNP PARIBAS FORTIS émet dans le cadre du Service.

AUDIT

L'AC Mediacert OTU et l'AE BNP PARIBAS FORTIS ont été certifiées, selon le schéma européen, ETSI EN 319 411-1 LCP par un cabinet d'audit accrédité par le COFRAC (Comité Français d'Accréditation). Chaque année un audit de contrôle et de surveillance est mené par ce cabinet sur le Service pour renouveler cette certification.

PROTECTION DES DONNEES A CARACTERE PERSONNEL

BNP PARIBAS FORTIS traite vos données à caractère personnel conformément à la Déclaration Vie Privée disponible sur https://www.fintro.be/fr/Public/Vie-privee ainsi que dans toutes les agences.

LOI APPLICABLE ET ATTRIBUTION DE JURIDICTION

En cas de litige relatif à l'interprétation, la validité ou l'exécution des présentes CGU, les parties donnent compétence expresse et exclusive à la législation et à la réglementation en vigueur sur le territoire belge et aux juridictions belges.

PLAINTES ET LITIGES

En cas de plainte ou litige, le Signataire doit suivre le processus décrit à l'article 21 des conditions générales bancaires de BNP Paribas Fintro en cas d'utilisation de Certificats dans le cadre de Fintro Easy Banking Web ou de Fintro Easy Banking Business.

DATE D'EFFET DES CGU

Les CGU prennent effet à compter de leur acceptation par le Signataire et sont applicables pendant toute la durée de conservation des dossiers d'enregistrement.

POINT DE CONTACT

Pour toute demande concernant les présentes CGU, le Signataire peut contacter Fintro au 02 433 45 20 (FR) ou au 02 433 45 10 (NL) en cas d'utilisation de Certificats dans le cadre de Fintro Easy Banking Web, Fintro Easy Banking App ou Fintro Easy Banking Business.