UTILISATION DES CERTIFICATS BNP PARIBAS INSTANT CA

CONDITIONS GENERALES

Edition septembre 2018

Les présentes Conditions Générales d'Utilisation (ci-après "CGU") ont pour objet de définir les modalités d'utilisation par le Signataire du service lui permettant d'apposer une signature électronique avancée sur un Document électronique présenté par BNP Paribas.

1. DEFINITIONS

Autorité de Certification ou AC : désigne l'entité chargée de signer, émettre et maintenir les Certificats d'une infrastructure à clés publiques, conformément à sa Politique de Certification.

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

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

Document : désigne le document nativement électronique signé par le Signataire.

Politique de Certification ou PC : désigne l'ensemble de règles identifiées par un OID (identificateur unique) et publiées par l'Autorité de Certification. La politique de Certification a pour objet de décrire les caractéristiques générales des Certificats délivrés par l'Autorité de Certification et l'ensemble de règles et d'exigences auxquelles se conforme l'Autorité de Certification dans la mise en place et la fourniture du Service.

Service : désigne le service d'infrastructure de gestion des clés par lequel BNP Paribas met à disposition du client un Certificat de signature électronique éphémère à des fins de signature électronique de Documents par le Signataire.

Signataire : désigne tout utilisateur du Service, client de BNP Paribas, se voyant délivrer un certificat en rapport avec son état civil.

2. OBJET DU SERVICE

Le Service a pour objet de délivrer au Signataire un Certificat pour lui permettre d'apposer une signature électronique avancée sur un Document.
Le Service est délivré par BNP Paribas, en qualité d'Autorité de Certification, conformément aux Politiques de Certification disponibles au public sur le site https://bnpp.digitaltrust.morpho.com/pc.html et identifiées par les OID (identificateurs uniques) suivants :

- **AC BNPP Instant n° 1 : 1.2.250.1.62.10.3.1.1.2**
- **AC BNPP Instant n° 2 : 1.2.250.1.62.10.4.1.1.2**

Le Service a été certifié conforme aux normes ETSI TS 102 042 et ETSI EN 319 411-1 V1.1.1 qui définissent les exigences de politique de sécurité applicables aux prestataires de service de confiance délivrant des Certificats, en application du règlement européen eIDAS n°910/2014 du 23 juillet 2014.
Chaque année un audit de contrôle et de surveillance est mené par un cabinet accrédité par l'organisme d'accréditation français COFRAC sur le Service pour renouveler cette Certification.

3. LIMITATIONS D'USAGE DU SERVICE

L'usage des Certificats émis dans le cadre du Service est strictement limité aux cas définis dans les Politiques de Certification.
Le Service est strictement réservé aux clients de BNP Paribas pour les usages définis par BNP Paribas.

4. OBLIGATION DE BNP PARIBAS

BNP Paribas s'engage à :

- Transmettre au Signataire des informations exactes et complètes conformément à la PC, en particulier pour ce qui concerne l'enregistrement.
- Délivrer le Service conformément aux limites d'usage définies dans la PC.
- Prévenir toute utilisation non autorisée de la Clé privée du Signataire.
- Notifier sans délai le Signataire si l'un des évènements suivants se produit pendant la période de validité du Certificat :
  - La Clé privée du Signataire a été perdue, volée, ou est potentiellement compromise ;
  - Le contrôle sur la Clé privée du Signataire a été perdu du fait d'une compromission de la donnée d'activation (par ex. un code PIN) ou toute autre raison ;
  - Inexactitudes ou modification du contenu du Certificat porté à la connaissance de BNP Paribas.
- Interdire définitivement l'utilisation de la Clé privée immédiatement après sa compromission.
- S'assurer que le Signataire n'utilise pas sa Clé Privée après qu'il ait été informé de la révocation du Certificat ou compromission de l'autorité de certification émettrice.
- S'assurer que le Signataire accepte la publication de son Certificat.
- 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.).
- 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 interne, etc.
- 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.
- 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.
- Assurer le "contrôle exclusif" par le Signataire de la bi-clé générée pour le compte de celui-ci.
- 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.
- Révoquer immédiatement le Certificat en cas de demande par le Signataire, directement ou indirectement à travers le Service.

5. OBLIGATION DU SIGNATAIRE

Le Signataire s'engage à :

- Utiliser le Service conformément aux présentes CGU.

- Vérifier son état civil tel qu'affiché avant toute opération de signature électronique réalisée par le Service, et interrompre le processus de signature électronique s'il remarque une erreur dans celui-ci.
- Notifier sans délai BNP Paribas si l'un des évènements suivants se produit pendant la période de validité du Certificat :
  - Le contrôle sur la Clé privée du Signataire a été perdu du fait d'une compromission de la donnée d'activation (par ex. un code PIN) ou toute autre raison ;
  - Inexactitudes ou modification du contenu du Certificat porté à la connaissance du Signataire ;
  - Présence d'incohérences dans son état civil pour que celui-ci procède ou fasse procéder à la révocation du Certificat généré.

L'infrastructure de gestion de clés de BNP Paribas est référencée au sein du programme de confiance d'Adobe (programme AATL) et dans ce cadre, les dispositions suivantes s'appliquent :

- Le Signataire délègue à BNP Paribas la responsabilité de l'utilisation des moyens cryptographiques générés pour son compte dans le cadre du Service ;
- Pour la gestion du cycle de vie du Certificat qu'il émet, BNP Paribas est tenu à une obligation de moyens, en conformité avec la PC ;
- BNP Paribas ne saurait être tenu responsable de tout dommage résultant d'une erreur dans l'état civil du Signataire n'ayant pas été reportée par celui-ci, et présente dans les Certificats que BNP Paribas émet dans le cadre du Service.

6. INFORMATION DES DESTINATAIRES DES DOCUMENTS SIGNES

Il est recommandé aux destinataires des documents signés de vérifier la validité de la signature électronique et du Certificat.
A cette fin, l'AC BNP Paribas tient à leur disposition les moyens suivants :

Points de distribution des CRL

- **1.2.250.1.62.10.3.1.1.2 :** http://bnpp.digitaltrust.morpho.com/crl/bnpp-customer- ephemeral1-ca.crl
- **1.2.250.1.62.10.4.1.1.2 :** http://bnpp.digitaltrust.morpho.com/crl/bnpp-customer- ephemeral2-ca.crl

Répondeurs OCSP

- **1.2.250.1.62.10.3.1.1.2 :** http://bnpp.digitaltrust.morpho.com/ocsp/bnpp- customer-ephemeral1-ca
- **1.2.250.1.62.10.4.1.1.2 :** http://bnpp.digitaltrust.morpho.com/ocsp/bnpp- customer-ephemeral2-ca

Par ailleurs, ces mêmes personnes doivent s'assurer que les documents signés sont conformes aux limitations d'utilisation du Service telles que mentionnées dans les présentes CGU.

7. CONSERVATION DES INFORMATIONS PAR BNP PARIBAS

Le Signataire reconnaît et accepte que :

1. Les dossiers d'enregistrement contenant les éléments relatifs à l'exécution du Service et les traces techniques assurant l'imputabilité des actions sont conservés 10 ans à compter de la fin du Document concerné, signé avec le Certificat.
2. Les Certificats et les informations sur le statut des Certificats (CRL, OCSP) sont conservés au moins 8 ans après leur date d'expiration.
3. 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 confiance en cas d'arrêt des Services et ce à des fins d'assurer le suivi du Service.

8. LIMITE DE RESPONSABILITE DE BNP PARIBAS

BNP Paribas ne saurait être tenu responsable de tout dommage résultant d'une erreur non reportée par le Signataire de son état civil présent dans les Certificats que BNP Paribas émet dans le cadre du Service.

9. FORCE MAJEURE

Aucune des parties ne sera tenue responsable de tout manquement ou retard dans l'exécution d'une ou de plusieurs obligations en vertu des présentes CGU en raison d'un cas de force majeure, tel que défini à l'Article 1218 du Code civil.

10. DONNEES PERSONNELLES

Les données personnelles recueillies dans le cadre de l'accès au Service sont traitées par BNP Paribas, responsable du traitement, aux fins de gestion des Certificats et du respect des obligations légales et réglementaires. Ces données pourront être communiquées aux prestataires de service et sous-traitants, qui exécutent pour le compte de BNP Paribas, certaines tâches matérielles et techniques indispensables à la réalisation du Service.
Les informations sur les traitements de données et sur l'exercice des droits du Signataire sur ces données figurent dans la Notice de protection des données personnelles qui lui a été fournie en tant que client de BNP Paribas.
Ce document est également disponible en agence et sur le site Internet mabanque.bnpparibas

11. LOI APPLICABLE ET ATTRIBUTION DE JURIDICTION

En cas de litige relatif à l'interprétation, la validité ou l'exécution des présente CGU, les parties donnent compétence expresse et exclusive à la loi française et aux tribunaux français, et ce conformément aux dispositions e l'Article 42 du Code de Procédure Civile.

12. 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.

13. MODALITE D'ACCEPTATION

Les présentes CGU sont jointes au Document présenté au Signataire pour qu'il appose sa signature électronique.
En signant le Document, le Signataire accepte les présentes CGU.