UTILISATION DES CERTIFICATS BNP PARIBAS INSTANT CA

CONDITIONS GENERALES

Edition janvier 2018

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 et d'informer les destinataires des documents signés sur les limites d'usage et les conditions de vérification des signatures.

DESIGNATION DES POLITIQUES DE CERTIFICATION - USAGE DU SERVICE

Les présentes CGU s'appliquent aux certificats émis dans le cadre des politiques de certification identifiées par les OID (Object Identifier) 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 correspond aux exigences "Lightweight Certificate Policy" définies par la norme ETSI EN 319 411-1. Il est réservé aux clients de BNP Paribas pour la signature de documents dans le cadre d'applications métiers.

LIMITATIONS D'USAGE DU SERVICE

L'usage des Certificats émis dans le cadre du Service est strictement limité aux cas définis dans la PC.

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.

Certificat : fichier électronique délivré par une Autorité de Certification attestant l'identité d'un Signataire.

Le Certificat est valide pendant une durée précise de 50 minutes.
Le Certificat contient la clé publique attribuée au Signataire.

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

Client : désigne toute personne morale qui propose à un Signataire de signer un Document via le Service.

Politique de Certification ou PC : désigne l'ensemble de règles et d'exigences auxquelles est soumise 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 personnelle de documents par le Signataire.

Signataire : désigne tout utilisateur du Service se voyant délivrer un Certificat en rapport avec son état civil.

OBLIGATION DE BNP PARIBAS

BNP Paribas s'engage à :
1. Transmettre au Signataire des informations exactes et complètes conformément à la PC, en particulier pour ce qui concerne l'enregistrement.

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

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

4. Notifier sans délai le 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 (par ex. un code PIN) ou toute autre raison ;
   c) Inexactitudes ou modification du contenu du Certificat porté à la connaissance de BNP Paribas.

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

6. 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.

7. S'assurer que le Signataire accepte la publication de son Certificat.

8. Mettre en place tous les moyens nécessaires à la bonne exécution des prestations et 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.).

9. 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.

10. Assurer la mise en oeuvre 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.

11. 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.

12. Assurer le "contrôle exclusif" par le Signataire de la bi-clé générée pour le compte de celui-ci.

13. 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.

14. Révoquer immédiatement le Certificat en cas de demande par le Signataire, directement ou indirectement à travers le Service.

OBLIGATION DU SIGNATAIRE

Le Signataire s'engage à :
1. Utiliser le Service conformément aux limites d'usage définies dans la PC.

2. Prévenir toute utilisation non autorisée de la Clé privée du Signataire.

3. Notifier sans délai BNP Paribas 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 la donnée d'activation (par ex. un code PIN) ou toute autre raison ;
   b) Inexactitude ou modification du contenu du Certificat porté à la connaissance du Signataire.

4. Consulter les Conditions Générales d'Utilisation de l'infrastructure de gestion de BNP Paribas décrites dans la PC

que BNP Paribas met à disposition sur le portail aux URL suivantes :
https://bnpp.digitaltrust.morpho.com/cgu.html
https://bnpp.digitaltrust.morpho.com/cp

5. 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.

6. Notifier le Service en cas d'incohérence dans son état civil pour que celui-ci procède ou fasse procéder à la révocation du certificat généré.

7. Il est convenu que dans le strict cadre de l'utilisation de l'IGC inscrite au programme Adobe AATL, 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 signifiée par celui-ci, et présente dans les certificats que BNP Paribas émet dans le cadre du Service.

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.

CONSERVATION DES INFORMATIONS PAR BNP PARIBAS

Le Client/Signataire reconnaît et accepte que :
1. Les dossiers d'enregistrement sont conservés 7 ans après expiration du certificat associé.
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. Les traces techniques assurant l'imputabilité des actions sont conservées 7 ans après leur génération.
4. Ces informations pourront être transmises à un autre prestataire de services de confiances en cas d'arrêt des Services.

LIMITE DE RESPONSABILITE DE BNP PARIBAS

BNP Paribas, prestataire du Client agissant au nom et pour le compte de ce dernier, 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 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.

AUDIT DE L'AC

L'AC BNP Paribas a été certifié, selon le schéma européen, ETSI TS 102 042 et est en cours de certification 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 de BNP Paribas pour renouveler cette certification.

PROTECTION DES DONNEES A CARACTERE PERSONNEL

Les données à caractère personnel des Signataires sont traitées par BNP Paribas, responsable de traitement, dans le cadre de l'accès au Service et plus particulièrement aux fins de gestion de la signature électronique et du respect des obligations légales et réglementaires incombant à BNP Paribas.
Pour des besoins de gestion inhérents au Service, ces données pourront être communiquées à des sous-traitants et/ou des prestataires intervenants dans ce contexte.
Le respect et la protection des données à caractère personnel des Signataires sont assurés conformément à la PC.
Ces données pourront donner lieu à exercice du droit d'accès, de rectification et d'opposition dans les conditions prévues par la loi n°78-17 du 6 janvier 1978 modifiée relative à l'Informatique, aux Fichiers et aux Libertés par courrier adressé à :
BNP Paribas, APAC TDC Val de Marne TSA 30233
94729 FONTENAY SOUS BOIS CEDEX

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 loi française et aux tribunaux français, et ce conformément aux dispositions de l'Article 42 du Code de Procédure Civile.

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 Conditions Générales, le Client doit contacter son conseiller habituel ou le Directeur d'agence (niveau 1) : l'adresse postale est donc celle de son agence, qui peut se retrouver facilement sur Internet, notamment à partir de son espace sécurisé.
En cas d'indisponibilité de son conseiller, le Client peut également joindre le Centre de Relation Client (CRC) au 0 820 820 001 (0,12 €/min + prix d'un appel).
Si le conseiller (agence ou CRC) et/ou le Directeur de l'agence ne peuvent pas répondre, ou si le Client n'obtient pas satisfaction, la réclamation est transmise au Pôle Réclamations de la Direction Régionale concernée qui la traitera (niveau 2).
Si le Client estime que la réponse / le traitement ne sont toujours pas satisfaisants, il peut alors demander l'intervention de la Médiation Bancaire (niveau 3).