



Les présentes Conditions Générales d'Utilisation des certificats cachets émis par SIGNEL, service de signature électronique de la fonction Informatique et Technologie Groupe (ITG) BNP Paribas, définissent les modalités d'utilisation entre SIGNEL et les entités ou filiales du groupe BNP Paribas clients du service.

## 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** : fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale. Le Certificat est valide pendant une durée de 3 ans.

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

**Client** : entité BNP Paribas ayant décidé de souscrire au Service, qu'elle utilise pour ses propres besoins de signature de documents.

**Gestionnaire de certificat** : est en charge de la gestion du certificat cachet et de la bi-clé pour le compte du Client.

**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.

**Signataire** : personne ayant le pouvoir d'autoriser une demande de certificat au nom du Client. Il Signataire s'engage sur ses conditions d'utilisation.

**Signature Electronique** : La signature électronique est un procédé technique qui consiste à l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte (le Document) auquel elle s'attache. La signature électronique a la même valeur qu'une signature manuscrite.

**SIGNEL** : désigne le service de Signature Electronique de la fonction Informatique et Technologie Groupe (ITG) BNP Paribas par lequel est mis à disposition du Signataire un Certificat.

## 2. OBJET DU SERVICE

Le service SIGNEL a pour objet de délivrer au Client un Certificat de type cachet serveur pour lui permettre d'apposer une Signature Electronique avancée sur un document.

Le service est délivré par BNP Paribas, en qualité d'Autorité de Certification, conformément à la Politique de certification disponibles au public sur le site <https://bnpp.digitaltrust.morpho.com/pc.html> et identifiée par l'OID (Object Identifier) suivant :

- **BNP Paribas Group Sealing and Timestamping CA: 1.2.250.1.62.10.5.1.1.2**

Le service a été certifié conforme ETSI EN 319 411-1 qui définit les exigences de politique et de sécurité applicables aux prestataires de service de confiance délivrant des Certificats de Signature Electronique avancée, en application du règlement européen eIDAS n°910/2014 du 23 juillet 2014.

Chaque année un audit de contrôle et de surveillance est mené sur le Service, par un cabinet accrédité par l'organisme d'accréditation français COFRAC, afin de renouveler cette certification.

## 3. LIMITATIONS D'USAGE DU SERVICE

L'usage des Certificats émis dans le cadre du service SIGNEL est strictement limité aux cas définis dans les Politiques de Certification.

Le Service est strictement réservé aux entités et filiales du groupe BNP Paribas pour les usages définis par BNP Paribas.

## 4. OBLIGATION DE SIGNEL

SIGNEL 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 Client.
- Notifier sans délai le Client et son Signataire si l'un des événements suivant se produit pendant la période de validité du Certificat :
  - La Clé privée du Client a été perdue, volée, ou est potentiellement compromise ;
  - Le contrôle sur la Clé privée du Client 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 SIGNEL.
- Interdire définitivement l'utilisation de la Clé privée immédiatement après sa compromission.
- S'assurer que le Client 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.
- 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 internes, 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 Client à des fins autres que celles pour lesquelles il a mandaté SIGNEL.
- Assurer le "contrôle exclusif" par le Client de la bi-clé générée pour le compte de celui-ci.
- 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 Conditions Générales d'Utilisation et la PC mise à disposition sur le site de publication à l'adresse <https://bnpp.digitaltrust.morpho.com/pc.html>
- Communiquer des informations exactes lors de la constitution de son enregistrement auprès du gestionnaire de certificat qui procédera à la demande de certificat auprès de l'AC, ainsi que toute modification de celles-ci.
- Notifier SIGNEL en cas d'arrêt ou de compromission du besoin pour que celui-ci procède ou fasse procéder 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 au gestionnaire de certificat :
  - Les opérations de génération de la bi-clé
  - Le pouvoir de transmettre à l'AC les demandes de génération et de révocation de certificat
- Le Signataire délègue à SIGNEL la responsabilité de l'utilisation des moyens cryptographiques générés pour le compte du Client dans le cadre du Service.
- Pour la gestion du cycle de vie du Certificat qu'il émet, SIGNEL est tenu à une obligation de moyens, en conformité avec la PC.

## **6. INFORMATION AUX 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

- **1.2.250.1.62.10.5.1.1.2 :**

<http://bnpp.digitaltrust.morpho.com/crl/bnpp-sealing-and-timestamping-ca.crl>

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 Conditions Générales d'Utilisation.

## **7. CONSERVATION DES INFORMATIONS PAR BNP PARIBAS**

Le Signataire reconnaît et accepte que :

- Les dossiers d'enregistrement sont conservés 7 ans.
- Les certificats et les informations sur le statut des Certificats

## **8. LIMITE DE RESPONSABILITE SIGNEL**

Cf. IX.H de la PC "BNP Paribas Group Sealing and Timestamping" : <https://bnpp.digitaltrust.morpho.com/cp/BNPP-FR-cp-bnpp-aatl-service.pdf>

## **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 Conditions Générales d'Utilisation 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 SIGNEL, 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.

## **11. POINTS DE CONTACT**

Pour toute demande concernant l'exécution des présentes Conditions Générales d'Utilisation ou du Service, le Client peut contacter l'adresse mail interne BNP Paribas : GLOBAL ITP SUPPORT3 SIGNEL.

## **12. TRAITEMENT DES PLAINTES ET LITIGES**

Dans le cadre de conflits provenant d'entités utilisant SIGNEL ou un des éléments de signature électronique fourni par SIGNE, cette entité pourra se tourner :

1. En premier lieu vers l'équipe SIGNEL pour traiter ce conflit et trouver une solution au problème,
2. En cas de non résolution de celui-ci contacter la hiérarchie qui gère l'équipe SIGNEL,
3. Enfin, en cas de non résolution, l'entité peut saisir la PMA afin de présenter son conflit et permettre la résolution de son litige.

## **13. LOI APPLICABLE ET ATTRIBUTION DE JURIDICTION**

Cf. IX.M de la PC "BNP Paribas Group Sealing and Timestamping" : <https://bnpp.digitaltrust.morpho.com/cp/BNPP-FR-cp-bnpp-aatl-service.pdf>

## **14. DATE D'EFFET DES CGU**

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

## **15. MODALITE D'ACCEPTATION**

Les présentes Conditions Générales d'Utilisation sont jointes au dossier d'enregistrement présenté au Signataire. Le Signataire accepte les présentes Conditions Générales d'Utilisation en apposant sa signature.