Politique de Signature

Dématérialisation des contrats et actes de gestion du Groupe BPCE

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 155 742 320 €.

Siège social : 50 avenue Pierre Mendes France

75201 Paris Cedex 13.

RCS n° 493 455 042.

SOMMAIRE

1 CONTEXTE & OBJECTIF

Le Groupe BPCE, pour ses réseaux Caisse d'Epargne, Banque Populaire et Filiales, met en œuvre pour ses Clients un service de dématérialisation des contrats et des actes de gestion intégrant un processus de signature électronique. Ce service de signature peut avoir lieu à distance ou en face à face dans une agence du réseau.

L'objet de ce document « Politique de Signature » est de décrire :

- Les conditions dans lesquelles sont réalisées, traitées, conservées ces signatures électroniques, dans le cadre de l'application « Dématérialisation des contrats et actes de Gestion », pour le profil de signataire Clients du Groupe BPCE ;

- Les conditions et contexte dans lesquels ces signatures électroniques seront ultérieurement consultables, utilisables, vérifiables.

Ce document est destiné aux :

- Signataires Clients ou Mandataires habilités par les clients du Groupe BPCE au sein de l'application « Dématérialisation des contrats et actes de Gestion» ;

- Destinataires de ces contrats et ou actes ;

- Eventuels prestataires participant à ces échanges pour le compte des destinataires ;

- Eventuels destinataires ultérieurs de ces documents signés, qui auront nécessairement besoin d'avoir connaissance des conditions dans lesquelles ces signatures électroniques auront été réalisées.

La structure de ce document est conforme aux documents normatifs suivants :

- ETSI TR 102 041 V1.1.1 (2002-02) : Signature Policies Report

- RFC 3125 - Electronic Signature Policies

2 POLITIQUE DE SIGNATURE

2.1 Champ d'application

La présente politique de signature, s'applique aux contrats et ou actes de gestion signés dans le cadre du processus de signature électronique inclus dans le service de dématérialisation mis à disposition par le Groupe BPCE pour ses réseaux Caisse d'Epargne, Banque Populaire et Filiales. Les contrats et ou actes de gestion sont contractualisés en agence, en face à face avec un chargé de clientèle, ou bien en ligne avec les clients ou mandataires désignés par les clients d'un des réseaux du Groupe BPCE.

2.2 Identification

La présente politique de signature est identifiée par l'OID **1.3.6.1.4.1.40559.1.0.3.3.0.1.1.**

Cette référence, ainsi que le numéro de version de la Politique de Signature utilisée, doit obligatoirement figurer dans les données signées, afin d'attester du régime sous lequel le signataire adresse ses informations métiers.

Lors de toute communication ultérieure, pour référencer la présente politique de signature, on utilisera l'OID accompagné de l'empreinte de ce document et de la mention de l'algorithme utilisé pour produire cette empreinte.

2.3 Publication du document

Avant publication, la politique de signature est validée par l'Autorité de Gestion des politiques (AP) sous la responsabilité du RSSI-Groupe au sein de la Direction de la Sécurité des Systèmes d'Information (DSSI-G).

La présente Politique de signature est publiée à l'adresse www.dossiers-securite.bpce.fr

2.4 Point de contact et prise en compte des remarques

2.4.1 Prise en compte des remarques

Les demandes d'information ou questions concernant la présente politique sont à adresser par courriel à l'adresse suivante:

BPCE

Directeur de la Sécurité des Systèmes d'informations Groupe

50 Rue Pierre Mendes France

75201 Paris Cedex 13

rssi-pssi-icg@bpce.fr

Ces remarques et souhaits d'évolution sont examinés par l'AP, qui engage si nécessaire le processus de mise à jour de la présente politique de signature.

Une signature électronique est toujours valide, au regard de la Politique de Signature qui s'appliquait au moment de la signature électronique. Toutes les versions des Politiques de Signature, et leur durée respective de validité sont donc conservées par **le Groupe BPCE**, et accessibles sur demande.

2.5 Processus de mise à jour

2.5.1 Circonstances rendant une mise à jour nécessaire

La mise à jour d'une politique de signature est un processus impliquant tous les acteurs et faisant l'objet d'une démarche rigoureuse. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique ou combler des lacunes.

La présente politique est réexaminée lors de toute modification majeure de l'application.

2.5.2 Information des acteurs

Les informations relatives à la version courante de cette politique et aux versions antérieures sont disponibles sur les lieux de publication. La publication d'une nouvelle version de la politique de signature est réalisée sous la responsabilité de l'AP et consiste à archiver la version précédente et mettre en ligne dans le répertoire prévu à cet effet, les éléments suivants :

- Document au format PDF,
- OID du document,

2.6 Entrée en vigueur de la nouvelle version et période de validité

La nouvelle version de la politique de signature entre en vigueur dès sa publication sur le site identifié au paragraphe 2.3. La nouvelle version reste valide jusqu'à la publication de la version suivante.

3 ACTEURS & ROLES

3.1 Les acteurs

3.1.1 Clients

Les signataires des documents sont des personnes physiques, au sein de l'application « Dématérialisation des contrats et actes de gestion ». Il s'agit nécessairement de clients ou de Mandataires représentant ou intervenant pour compte de clients, préalablement identifiés et connus des agences ou centres d'affaires du réseau du Groupe BPCE. Le Client a déjà souscrit à un moyen d'authentification forte qui permet de l'authentifier avant d'entamer le processus de signature.

Dans le cadre de ce processus de signature, les signataires signent électroniquement l'ensemble des pièces du dossier, intégrant notamment les conditions d'usage de ce service, reprenant les rôles et obligations contenues dans la présente politique.

3.1.2 Etablissement bancaire du Groupe BPCE

Le Groupe BPCE dispose de plusieurs établissements bancaires. Chaque établissement dispose d'un certificat cachet qui lui permet de signer, au nom de la personne morale que représente l'établissement, le contrat biparti avec le « Client ».

3.1.3 Destinataires des contrats et ou actes de Gestion signés électroniquement

Les destinataires des contrats et ou actes de gestion signés électroniquement sont :

- D'une part les Clients eux-mêmes qui conservent ce document, dont la signature électronique matérialise leur consentement par rapport aux clauses du contrat ou actes de gestion;
- Les établissements du Groupe BPCE qui ont apporté leur signature cachet sur le document ;
- Eventuellement aux distributeurs du Groupe BPCE selon le type de documents signés.

3.2 Rôles et obligations du signataire

3.2.1 Equipement informatique

L'équipement utilisé pour réaliser l'opération de signature doit permettre de s'authentifier et de se connecter sur le portail de la Banque.

Avec un certificat généré à la volée, le processus de signature ne dépend pas du poste client, que l'opération se déroule en agence ou en ligne. Dans ce cas, aucun outil lié aux opérations de signature n'est à installer sur l'équipement informatique des signataires.

Avec un certificat sur support matériel X509, des drivers ou logiciels tiers (ex. JAVA) peuvent être requis et installés sur l'équipement informatique des signataires.

Si l'opération est réalisée par un chargé de clientèle ou chargé d'affaires, l'environnement mis en œuvre est conforme aux règles de sécurité mises en œuvre par chaque entreprise du Groupe BPCE.

3.2.2 Environnement de l'application de signature

L'application « Dématérialisation des contrats et actes de gestion» utilisée par le signataire est l'élément sensible du processus de signature. L'application est installée dans des Datacenters du Groupe BPCE.

En particulier, il est mis en œuvre :

- La surveillance de l'accès physique et logique au système et de le protéger contre les intrusions,
- Une limitation d'accès et d'administration de l'application métier à un minimum de personnes de confiance, ayant les compétences préconisées par le fournisseur en matière de sécurité des systèmes informatiques,
- Le suivi des recommandations du fournisseur relatives à la sécurité du système.

3.2.3 Outil de signature utilisé

Les Clients doivent contrôler les données qu'ils vont signer avant d'y apposer leur signature électronique. Ils utilisent pour cela l'application de signature du portail de signature ou celle installée sur leur poste de travail et mise à disposition par le Groupe BPCE et dont les différentes étapes du processus de signature les amènent à :

- Contrôler les éléments du contrat ou de l'acte de gestion,
- Valider leur compréhension des Conditions Générales du Service,
- Accepter formellement l'opération de signature.

La signature cachet, réalisée par l'établissement avec lequel le contrat est signé, est appelée par le même processus de signature.

La configuration du processus de signature n'est pas modifiable ni par les Clients, ni par les établissements du Groupe BPCE.

3.2.4 Type de certificat utilisé

Les certificats éphémères : Le certificat est généré par l'application de l'autorité de certification de l'ICG au moment de l'opération de signature du document. Ce certificat a une durée de validité limitée au processus de signature.

L'établissement du Groupe BPCE avec qui le document est signé dispose également d'un certificat de signature de type cachet serveur qui engage dans la signature la personne morale correspondante. Il existe un certificat cachet par établissement et ces derniers sont émis par une Autorité de Certification du Groupe BPCE.

Dans le processus de signature, des certificats techniques d'horodatage et de mise en archive sont également utilisés. Ces certificats sont émis par des Autorités de Certification du Groupe BPCE.

3.2.5 Protection du certificat Client

Le certificat « éphémère » de signature du Client est généré dans le boitier cryptographique associé au serveur de signature. Aucun support n'est remis au Client.

Le Groupe BPCE utilise un serveur de signature qui est en charge de :

- Générer une nouvelle bi-clé (clé publique et clé privée) pour créer le certificat Client
- Protéger cette bi-clé dans le boitier cryptographique qualifié du serveur
- Réaliser les opérations de signature
- Détruire la bi-clé à la fin de l'opération du processus de signature.

3.2.6 Révocation du certificat client

Sans objet.

3.3 Rôles et obligations du Groupe BPCE

Le Groupe BPCE est le promoteur de l'application utilisé par les signataires.

Le Groupe BPCE maintient l'application pour l'ensemble des établissements du Groupe BPCE et met à disposition des signataires des outils de signature de contrat en agence ou en ligne.

L'application est réalisée au niveau Groupe BPCE qui fait héberger et exploiter les services nécessaires à l'application auprès de son opérateur technique.

Le Groupe BPCE met en œuvre auprès des différents établissements les moyens permettant de garantir la validité dans le temps des signatures électroniques produites par les signataires. Ces moyens se traduisent par un service d'archivage électronique garantissant la pérennité des contrats et actes de gestion signés.

3.3.1 Données de Vérification

Pour effectuer les vérifications, le Groupe BPCE utilise les données présentes dans le système d'archivage mis en œuvre, notamment :

- les données publiques relatives aux certificats des signataires, telles que les listes de révocations.
- les habilitations des signataires à signer ces informations métier ;

Toutes les informations signées font l'objet d'un horodatage permettant :

- de s'assurer de la traçabilité des informations de date et heure de signature de ces transactions ;
- de déterminer la liste de révocation à utiliser pour valider cette transaction.

3.3.2 Protection des moyens

Le Groupe BPCE, via l'opérateur technique, s'assure de la mise en œuvre des moyens nécessaires à la protection des équipements fournissant les services de signature et de validation.

Les mesures prises concernent à la fois :

- la protection des accès physiques et logiques aux équipements aux seules personnes habilitées;
- la disponibilité du service ;
- la surveillance et le suivi du service.

3.3.3 Journalisation

Le Groupe BPCE, via l'opérateur technique, s'assure de la conservation des traces relatives :

- à la circulation des échanges au sein des réseaux et des équipements informatiques ;
- au traitement des données échangées.

Le Groupe BPCE s'assure que les preuves de traitement relatives à la vérification des signatures électroniques sont conservées pendant toute la durée règlementaire.

3.3.4 Reprise en cas d'interruption de service

Le Groupe BPCE, via l'opérateur technique, s'assure de la mise en œuvre des moyens nécessaires à la reprise d'activité en cas d'interruption de service d'un des composants nécessaire aux tâches dont il a la responsabilité.

Il s'assure en particulier que ces moyens font l'objet de tests à intervalles réguliers.

3.3.5 Assistance aux utilisateurs

Les signataires peuvent s'adresser au Groupe BPCE pour toute information complémentaire ou pour signaler tout dysfonctionnement à l'adresse indiquée au paragraphe 2.4.

3.3.6 Audit technique et juridique

Le Groupe BPCE fait réaliser sur son infrastructure de confiance :

- Un audit technique pour s'assurer que les mises en œuvre techniques correspondent bien aux exigences prévues dans les documents de politique,
- Un audit juridique pour s'assurer que les contextes règlementaires sont conformes.

3.4 Rôles et obligations des destinataires

Les Clients et les établissements du Groupe BPCE doivent mettre en œuvre les moyens leur permettant de s'assurer de l'origine du message reçu, et de l'identité de l'émetteur.

Pour se faire, les destinataires peuvent :

- Mettre en œuvre par eux-mêmes des moyens de vérification des signatures électroniques des informations reçues;
- Demander à l'établissement du Groupe BPCE de leur mettre à disposition des outils de vérification de ces signatures électroniques chaines de certification, fichier de preuves auto portant;
- Demander à l'établissement du Groupe BPCE de façon ponctuelle, de vérifier la signature électronique des informations reçues, pour leur compte.

3.4.1 Limitations des responsabilités du Groupe BPCE

3.4.1.1 Mise à jour des informations utilisées

Certaines données, notamment les listes de révocations, ne peuvent être mises à jour en temps réel et il s'écoule plusieurs heures (24 au maximum) avant la publication de ces données par l'Autorité de Certification.

Dans ces conditions, il se peut qu'une signature soit déclarée valide si elle est réalisée entre le moment où le certificat a été révoqué et le moment où sa révocation a été publiée par l'Autorité de Certification et prise en compte par l'établissement du Groupe BPCE.

Le Groupe BPCE et l'établissement concerné ne peuvent être alors tenus responsables de cet état de fait.

Le Groupe BPCE recommande donc au signataire de vérifier les opérations dans l'intervalle de temps autour de la révocation, à l'occasion d'une demande de révocation (cf. 3.2.6).

3.4.1.2 Contenu des données signées

Les Clients sont responsables du contenu des informations présentes dans le document signé, et de la bonne utilisation des certificats de signature dans ce cadre.

4 SIGNATURE ÉLECTRONIQUE ET VALIDATION

Au préalable du processus de signature électronique, le client accède à un ou plusieurs moyens d'authentification suivant le processus d'enrôlement en vigueur.

Les moyens d'authentification proposés sont :

- La reconnaissance visuelle sur présentation d'un justificatif d'identité, uniquement en face-à-face

- L'authentification non rejouable par SMS basée sur le numéro de téléphone mobile ayant été vérifié en face-à-face après authentification ou en ligne par 2 canaux différents, par exemple internet et courrier postal,

- L'authentification non rejouable par CAP, le lecteur CAP ayant été remis au client lors d'un rendez-vous en face-à-face ou par envoi postal,

- L'authentification par certificat matériel, le certificat ayant été remis au client lors d'un rendez-vous en face-à-face. Les certificats sur support matériel sont des certificats qualifiés émis par une autorité de certification reconnue par le Groupe BPCE et conforme aux exigences RGS et ou équivalent PAC.

Le processus de signature électronique se déroule en 3 étapes :

a. Lecture et consentement des documents.

Les documents à lire sont présentés à l'écran en séquence. Pour chaque document, il est invité à confirmer qu'il en a pris connaissance en cliquant sur « j'ai lu et j'accepte ».

b. Authentification

Le client va être authentifié fortement via reconnaissance visuelle, via une authentification non rejouable par SMS ou par lecteur CAP ou via certificat sur support matériel. Dans le cas d'une authentification par SMS ou lecteur CAP, le client reçoit un code sur son mobile ou sur le lecteur CAP qu'il est invité à saisir à l'écran pour s'authentifier puis passer à l'étape de signature.

c. Signature

La liste des documents à signer est présentée au client. Il est invité à confirmer qu'il a été informé du moyen de mise à disposition, puis à signer l'ensemble des documents.

Une fois signés, les documents sont mis à disposition du client et archivés.

4.1 Caractéristiques de l'équipement du signataire

L'équipement du signataire fonctionne dans un environnement sous le contrôle :

- Du chargé de clientèle lorsque la signature se fait en agence ;
- Du Client lorsque la signature se fait en ligne.

Les certificats utilisés pour la signature suite à une authentification forte (Ex : SOL) sont des certificats éphémères, valables le temps de l'opération de signature et conformes aux exigences portées par l'ETSI 102042 niveau LCP.

Ce certificat est produit par une Autorité de Certification du Groupe BPCE.

Les certificats sur support matériel sont des certificats qualifiés émis par une autorité de certification reconnue par le Groupe BPCE et conforme aux exigences RGS et ou équivalent PAC. L'utilisation de ces certificats en signature électronique nécessite la présence d'une application sur le poste client.

4.2 Données signées

Au moment de la signature électronique, le Client signe électroniquement les informations suivantes :

- l'ensemble des documents,
- de pièces jointes, le cas échéant
- les propriétés de la Signature Electronique (Certificat du Client ou du Prospect, Certificat Cachet de l'établissement, identifiant de la politique de signature utilisée).

4.3 Opération de signature électronique

Les fonctionnalités minimales suivantes sont assurées, pour permettre au Client d'avoir connaissance et conscience de l'action qu'il est sur le point d'effectuer :

- **Présentation du document à signer :**

Le signataire a la possibilité de visualiser les informations du document que l'application de signature lui propose de signer.

- **Présentation des attributs de la signature au signataire**

La fonction de signature est intégrée au Portail de l'établissement du Groupe BPCE avec lequel le Client signe le document. Les Conditions Générales d'Utilisation du Service de signature sont présentées au Client et précisent notamment les conditions dans lesquelles sa signature électronique sera réalisée et traitée :

- **Interaction avec le signataire : consentement explicite et possibilité d'arrêt du processus de signature**

Le signataire a les moyens d'exprimer explicitement (c'est-à-dire, de manière volontaire et non ambiguë) son consentement pour sélectionner un document ou plusieurs documents et déclencher le processus de signature des documents sélectionnés.

4.4 Caractéristiques des signatures

4.4.1 Type de signature

Les signatures électroniques apposées par les Clients sont des signatures PDF

4.4.2 Norme de signature

La signature mise en œuvre est basée sur la norme PaDES.

4.5 Algorithmes utilisables pour la signature

4.5.1 Algorithme de condensation

Les algorithmes de condensation supportés sont SHA-1 et SHA-2.

4.5.2 Algorithme de chiffrement

L'algorithme de chiffrement à utiliser est RSA Encryption

4.5.3 Canonicalisation

L'algorithme de forme canonique exclusive xml-exc-c14n identifié par l'URI http://www.w3.org/2001/10/xml-excc14n# est mis en œuvre.

4.6 Conditions pour déclarer valide le fichier signé

Un fichier signé est considéré comme valide par le Groupe BPCE lorsque les conditions suivantes sont remplies :

- vérification positive de la signature électronique du signataire ;
- vérification positive des droits du signataire en fonction des données transmises ;
- validation du dossier signé par le service de validation interne à l'ICG.

4.6.1 Vérification de la signature

La vérification de la signature porte sur :

- la vérification du respect de la norme de signature ;
- la vérification de l'appartenance du certificat du Client à la famille de certificat émis par une des AC du Groupe BPCE ou d'une AC reconnue et acceptée par le Groupe BPCE;
- la vérification du certificat du Client et de tous les certificats de la chaîne de certification:
  - validité temporelle,
  - statut,
  - signature cryptographique ;

- la vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue ;

- la vérification de la signature électronique apposée sur le fichier en utilisant la clé publique du Client contenue dans le certificat transmis ;

- la vérification des données d'horodatage apposées sur la signature électronique du Client;

- la vérification que le certificat utilisé au moment de la signature n'était pas dans une Liste de Certificats Révoqués. Cela concerne les certificats des Clients et également les certificats cachet mis en œuvre par les établissements du Groupe BPCE. Cette vérification est basée sur la constitution d'une liste blanche lors de la génération ou la révocation d'un certificat de signature ;

- la vérification de l'identifiant de la politique de signature référencée.

4.7 Gestion de la preuve

Pour conserver une trace de chaque validation de signature, le Groupe BPCE constitue une preuve électronique signée et horodatée, qui recense les éléments associés à la validation de signature effectuée :

- Document signé par l'ensemble des Parties (Client d'un côté et établissement du Groupe BPCE de l'autre),

- Certificat de signature utilisé par le Client,

- Certificat cachet utilisé par l'établissement du Groupe BPCE,

- Résultat de la validation,

- Statut de contrôle de la Liste de Certificats Révoqués,

- L'ensemble des chaînes de certification mises en œuvre,

- Trace d'audit généré par le serveur de signature.

Cette preuve peut être rejouée (par la validation de la signature de la preuve) ultérieurement en cas de litige et restitue exactement les informations utilisées lors de la validation.

5 POLITIQUE DE CONFIDENTIALITÉ

5.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- Les procédures internes à l'opérateur technique du Groupe BPCE,
- Les clés privées de l'AC, des composantes et des porteurs (Client) de certificats,
- Les données d'activation associées aux clés privées d'AC et des porteurs (Client),
- Toutes les données d'activation (secrets) de l'Infrastructure,
- Les journaux d'évènements des composantes de l'Infrastructure,
- L'affectation des rôles de confiance
- Le dossier de demande de certificat pour les certificats cachet et horodatage,
- Les causes de révocations, sauf accord explicite du porteur,
- La PSSI du Groupe BPCE.

5.2 Communication des informations à un tiers

On entend par tiers, tout organisme n'étant pas dans la chaîne de traitement des informations du Groupe BPCE.

La diffusion des informations à un tiers ne peut intervenir qu'après acceptation du Groupe BPCE.

6 DISPOSITIONS JURIDIQUES

6.1 Juridictions compétentes

Les dispositions de la politique de signature sont régies par le droit français.

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique, et faute d'être parvenues à un accord amiable ou à une transaction, les parties donnent compétence expresse et exclusive aux tribunaux compétents de Paris, nonobstant pluralité de défendeurs ou d'action en référé ou d'appel en garantie ou de mesure conservatoire.

6.2 Droits sur la propriété intellectuelle et industrielle

Tous les logiciels participants à la constitution et à la validation du document signé sont la propriété du Groupe BPCE et au regard des droits de propriété intellectuelle, ils sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, …) est sanctionnée par le Code de la propriété intellectuelle et le Code pénal.

Le Groupe BPCE détient tous les droits de propriété intellectuelle : il est propriétaire de la Politique de signature.

Le porteur détient tous les droits de propriété intellectuelle sur les informations personnelles contenues dans les certificats porteurs émis par l'AC et dont il est propriétaire.

6.3 Données personnelles

En conformité avec les dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le traitement automatisé des données personnelles a fait l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Le Client est informé qu'il dispose d'un droit d'accès, de rectification et d'opposition portant sur les données le concernant en s'adressant à :

- Groupe BPCE
- Directeur de la Sécurité des Systèmes d'informations Groupe
- 50 Avenue Pierre Mendes France
- 75201 Paris Cedex 13
- rssi-pssi-icg@bpce.fr

7 DEFINITIONS

Les définitions et acronymes sont référencées dans le document« « Mesures communes » publié à la même adresse que la présente politique.