



Politique de Signature

Application

« Dématérialisation de Contrats et Actes de Gestion »

**Profil « Clients, Mandataires ou Prospects du Groupe
BPCE »**

Référence du document	
1.3.6.1.4.1.40559.1.0.3.3.0.1.0	1 décembre 2013

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 467 226 960 €.

Siège social : 50 avenue Pierre Mendès France

75201 Paris Cedex 13. RCS n° 493 455 042.

Ce document est la propriété exclusive de BPCE SA.

Son usage est réservé à l'ensemble des personnes habilitées selon leur niveau de confidentialité.

Sa reproduction est régie par le Code de la propriété intellectuelle qui ne l'autorise qu'à l'usage privé du copiste.

SOMMAIRE

1	CONTEXTE & OBJECTIF	5
2	POLITIQUE DE SIGNATURE.....	7
2.1	CHAMP D'APPLICATION	7
2.2	IDENTIFICATION	8
2.3	PUBLICATION DU DOCUMENT.....	8
2.4	POINT DE CONTACT ET PRISE EN COMPTE DES REMARQUES	8
2.4.1	<i>Prise en compte des remarques.....</i>	<i>8</i>
2.5	PROCESSUS DE MISE A JOUR	9
2.5.1	<i>Circonstances rendant une mise à jour nécessaire</i>	<i>9</i>
2.5.2	<i>Information des acteurs.....</i>	<i>9</i>
2.6	ENTREE EN VIGUEUR DE LA NOUVELLE VERSION ET PERIODE DE VALIDITE	9
3	ACTEURS & ROLES.....	10
3.1	LES ACTEURS	10
3.1.1	<i>Signataires disposant du profil « Client » d'une des banques du Groupe BPCE, au sein de l'application « Dématisation des contrats et actes de gestion».....</i>	<i>10</i>
3.1.2	<i>Signataires disposant du profil « Prospect » d'une des banques du Groupe BPCE, au sein de l'application « Dématisation des contrats ».....</i>	<i>10</i>
3.1.3	<i>Réseau bancaire du Groupe BPCE.....</i>	<i>10</i>
3.1.4	<i>Destinataires des contrats et ou actes de Gestion signés électroniquement</i>	<i>11</i>
3.2	ROLES ET OBLIGATIONS DU SIGNATAIRE	11
3.2.1	<i>Equipement informatique</i>	<i>11</i>
3.2.2	<i>Environnement de l'application de signature.....</i>	<i>11</i>
3.2.3	<i>Outil de signature utilisé.....</i>	<i>12</i>
3.2.4	<i>Type de certificat utilisé</i>	<i>12</i>
3.2.5	<i>Protection du certificat Client.....</i>	<i>12</i>
3.2.6	<i>Révocation du certificat</i>	<i>13</i>
3.3	ROLES ET OBLIGATIONS DU GROUPE BPCE	13

3.3.1	<i>Données de Vérification</i>	13
3.3.2	<i>Protection des moyens</i>	14
3.3.3	<i>Journalisation</i>	14
3.3.4	<i>Reprise en cas d'interruption de service</i>	14
3.3.5	<i>Assistance aux utilisateurs</i>	14
3.3.6	<i>Audit technique et juridique</i>	14
3.4	ROLES ET OBLIGATIONS DES DESTINATAIRES	15
3.4.1	<i>Limitations des responsabilités de BPCE SA</i>	15
4	SIGNATURE ÉLECTRONIQUE ET VALIDATION	16
4.1	CARACTERISTIQUES DE L'ÉQUIPEMENT DU SIGNATAIRE.....	16
4.2	DONNEES SIGNEES	16
4.3	OPERATION DE SIGNATURE ELECTRONIQUE	16
4.4	CARACTERISTIQUES DES SIGNATURES.....	17
4.4.1	<i>Type de signature</i>	17
4.4.2	<i>Norme de signature</i>	17
4.5	ALGORITHMES UTILISABLES POUR LA SIGNATURE	17
4.5.1	<i>Algorithme de condensation</i>	17
4.5.2	<i>Algorithme de chiffrement</i>	17
4.5.3	<i>Canonicalisation</i>	17
4.6	CONDITIONS POUR DECLARER VALIDE LE FICHER SIGNE	17
4.6.1	<i>Vérification de la signature</i>	17
4.6.2	<i>Vérification des droits du signataire en fonction de données transmises</i>	18
4.7	GESTION DE LA PREUVE	18
5	POLITIQUE DE CONFIDENTIALITE	20
5.1	CLASSIFICATION DES INFORMATIONS.....	20
5.2	COMMUNICATION DES INFORMATIONS A UN TIERS.....	20
6	DISPOSITIONS JURIDIQUES	21
6.1	DROIT APPLICABLE	21
6.2	REGLEMENT DES DIFFERENDS	21
6.3	PROPRIETE INTELLECTUELLE DE L'INFRASTRUCTURE DE CREATION ET DE VALIDATION DES SIGNATURES	

6.4	DONNEES NOMINATIVES	21
7	DEFINITIONS	22

1 CONTEXTE & OBJECTIF

Dans le cadre de ses projets de dématérialisation de contrats et actes de Gestion, **BPCE SA** déploie des outils de signature électronique dans ses différents réseaux bancaires.

Lorsque les fonctions de signature électronique sont mises à disposition des signataires, il est important qu'ils aient connaissance du contexte dans lequel cette signature électronique est produite, des rôles, obligations que chaque acteur endosse, et des conditions dans lesquelles cette signature sera ultérieurement traitée, conservée, disponible pour vérification.

L'application « Dématérialisation de contrats et actes de Gestion » permet au signataire Clients, Mandataires habilité par les clients ou Prospects du Groupe BPCE de signer électroniquement : des contrats, des opérations de Guichet, des ordres et toutes opérations de Gestion en agence ou en ligne qui sont ensuite transmis aux signataires et aux back-offices des banques du Groupe BPCE. Ces documents sont ensuite vérifiables et lisibles par les signataires via des outils de lecture de fichiers PDF.

La liste des opérations éligibles à la signature sont appelées à évoluer au fil du temps.

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 ou Prospects du Groupe BPCE ;
- Les conditions et contexte dans lesquels ces signatures électroniques seront ultérieurement consultables, utilisables, vérifiables.

Ce document est destiné aux :

- Signataires Clients, Mandataires habilité par les clients ou Prospects 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

Cette « Politique de Signature », sous forme de document bureautique et lisible, est complétée par une « Politique de Signature technique », présentant les mêmes informations sous la forme d'un fichier technique de configuration, exploitable par les

infrastructures techniques des signataires et de ses destinataires, pour en automatiser la production et les vérifications ultérieures.

2 POLITIQUE DE SIGNATURE

2.1 Champ d'application

La présente politique de signature, s'applique aux transactions électroniques produites au sein de l'application « Dématisation des contrats et des actes de gestion », mise à disposition des Banques du Groupe BPCE. Ces contrats, avenants et ou actes de gestion sont contractualisés en agence, en face à face avec un chargé de clientèle, ou bien en ligne.

Dans le cadre de cette application « Dématisation des contrats et actes de gestion », les personnes qui ont la capacité de signer électroniquement ces contrats sont soit des Clients du Groupe BPCE soit des Prospects d'un des réseaux du Groupe BPCE.

Cette faculté de signature électronique permet de répondre à plusieurs contextes :

- Contexte bancaire :
 - Sous le terme « Infrastructure de Confiance Groupe » (appelée ICG dans la suite du document), BPCE SA définit l'ensemble des briques fonctionnelles et techniques qui permettent de donner une valeur contractuelle à une procédure électronique.
 - Cette infrastructure de confiance doit notamment répondre aux besoins métiers de vente en agence et en ligne et de non matérialisation des contrats et actes de gestion.
- Contexte fonctionnel :
 - La signature électronique reprend deux fonctions de la signature papier (authentification et consentement) et en demande une supplémentaire: la fiabilité (procédé fiable d'identification garantissant le lien entre la signature électronique et l'acte auquel elle s'attache).
 - Il faut donc apposer la signature du Client sur le contrat ou l'acte de gestion dans le délai le plus bref après son consentement. Cette signature est réalisée à partir d'un certificat Client
- Contexte réglementaire :
 - La solution doit s'inscrire dans le contexte réglementaire et juridique de l'ICG.
 - Pour cela BPCE SA s'est appuyée sur des études juridiques produites par un cabinet tiers, spécialiste du domaine de la signature électronique.
 - L'objectif est de diminuer le risque de fraude, en supprimant les ordres ou confirmation d'ordres sur support papier et en facilitant l'exécution et le traitement des ordres de façon électronique de bout en bout de manière sécurisée (volonté exprimée par la Banque de France)
- Contexte économique :
 - La mise en œuvre de la signature électronique a pour objectif de réduire les coûts d'impression en multi-exemplaire des contrats et réduire ainsi la

volumétrie nécessaire à l'archivage par les réseaux bancaires de BPCE SA pour conserver ces documents.

- La mise en œuvre de la signature électronique s'inscrit dans le projet global de « l'Infrastructure de Confiance Groupe ».

La présente Politique de signature a été portée à la connaissance du Client ou du Prospect lors du processus de signature électronique et avant l'opération de signature électronique. De cette façon, le signataire est en capacité de prendre connaissance de ces conditions de signature au moment de la réalisation de cette action. Respectivement, cette Politique de Signature est mise à disposition des destinataires de la signature électronique, pour leur permettre de prendre connaissance des conditions dans lesquelles le signataire a produit la signature électronique.

2.2 Identification

La présente politique de signature est identifiée par l'OID **1.3.6.1.4.1.40559.1.0.3.3.0.1.0.**

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 toute publication officielle, la politique de signature est validée par le Comité Sécurité Groupe.

Ce comité est placé sous la responsabilité du RSSI du Groupe BPCE, qui valide la nouvelle politique de signature.

La présente Politique de signature est publiée :

- Au sein de l'application « Dématisation des contrats et actes de gestion », et accessible par le signataire au moment de la réalisation de la signature électronique ;
- Sur l'URL : <http://pro.d00.pki01.bpce.fr/docs/pc/>

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 le Comité Sécurité Groupe, 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 **BPCE SA**, 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

Lorsqu'une mise à jour a été planifiée, les informations relatives à cette évolution sont mises en ligne sur les lieux de publication. Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du Comité Sécurité Groupe pour obtenir plus d'informations.

La publication d'une nouvelle version de la politique de signature est réalisée sous la responsabilité du RSSI de IT-CE 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

Lorsqu'une nouvelle version de la politique de signature est mise en ligne, un message électronique est diffusé sur le site <http://pro.d00.pki01.bpce.fr/docs/pc/>, accessible de tous les signataires pour les informer de la nature et de la date et heure du changement.

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 Signataires disposant du profil « Client » d'une des banques du Groupe BPCE, au sein de l'application « Dématisation des contrats et actes de gestion »

Les signataires des documents sont des personnes physiques, au sein de l'application « Dématisation 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 Signataires disposant du profil « Prospect » d'une des banques du Groupe BPCE, au sein de l'application « Dématisation des contrats »

Les signataires ayant le profil « Prospects », à l'instar des « Clients » du Groupe BPCE, ne sont pas connus nécessairement du Groupe BPCE et sont authentifiés via des moyens d'authentification forte basé sur des informations déclarées par le « Prospect ».

Le processus de signature est ensuite identique à celui d'un « Client » et les signataires ayant le profil « Prospect » 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.

3.1.3 Réseau 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 biparties avec le « Client » ou le « Prospect ».

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

BPCE SA 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 d'IT-CE.

IT-CE est l'opérateur technique de l'infrastructure ICG des signataires et exploite la plate-forme de confiance permettant d'horodater ces transactions à l'issue de leur signature, puis de valider et d'archiver ces informations signées.

BPCE SA 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.

3.1.4 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 ou les Prospects 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, Mandataires ou les Prospects 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 Prospects, 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.

Les certificats X509 sur support matériel : Le certificat est émis par une Autorité de Certification reconnue par le Groupe BPCE, il a généralement une durée de validité de trois ans.

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 ou du Prospect est généré dans le boîtier cryptographique associé au serveur de signature. Aucun support n'est remis au Client, Mandataire ou Prospect.

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, Mandataire ou Prospect
- Protéger cette bi-clé dans le boîtier cryptographique qualifié du serveur
- Réaliser les opérations de signature
- Détruire la bi-clé à la fin de l'opération du processus de signature.

Le certificat X509 référencé sur support « matériel » du Client professionnel équipé, est généré par une autorité de certification référencée selon des principes de sécurité stricts (de type PRIS, RGS,..) (Certificat personnel, enrôlement, remise en face à face, code confidentiel..).

Le Groupe BPCE autorise l'utilisation de certificats personnels référencés pour la signature d'un client

- Le client est enrôlé par une autorité d'enregistrement rattachée à l'autorité de certification
- La bi-clé est générée par une Autorité de Certification référencée
- Cette bi-clé est stockée dans un support matériel « qualifié » contrôlé par un code d'accès confidentiel
- Le certificat est remis en face à face au client, le code confidentiel est envoyé directement au client
- Le certificat est enregistré dans le système d'information de la banque et associé à un client
- Les opérations de signature sont effectuées sur l'équipement du client avec le certificat personnel « déclaré »
- Le serveur de signature consulte la liste de révocation émise par l'Autorité de certification qui a émis le certificat afin de s'assurer de sa validité

3.2.6 Révocation du certificat

Le signataire Client a la possibilité de demander la révocation du certificat électronique utilisé pour signer soit auprès du chargé de clientèle, soit auprès de l'autorité de certification qui l'a délivré.

Il est à préciser que les certificats éphémères ayant une durée de validité de quelques minutes, le cas de révocation d'un tel certificat ne pourra être qu'extrêmement ponctuel.

En tout état de cause, l'Autorité de Certification qui a émis le certificat de signature assure un service de révocation et publie la Liste des Certificats Révoqués.

Le signataire Client professionnel a la possibilité de demander la révocation du certificat électronique à l'autorité de certification qui l'a émis. Il peut aussi demander au chargé de clientèle ou chargé d'affaires de le supprimer de la liste des habilitations déclarées pour sa société.

3.3 Rôles et obligations du Groupe BPCE

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

BPCE SA, via l'opérateur IT-CE, 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

BPCE SA, via l'opérateur IT-CE, 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.

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

3.3.4 Reprise en cas d'interruption de service

BPCE SA, via l'opérateur IT-CE, 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 à BPCE SA 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 réglementaires sont conformes.

3.4 Rôles et obligations des destinataires

Les Clients, Mandataires et Prospects 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 chaînes 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 de BPCE SA

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, Mandataires et les Prospects 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

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 ou du Prospect 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 ou le Prospect 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 ou au Prospect 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 ou le Prospect signe le document. Les Conditions Générales d'Utilisation du Service de signature sont présentées au Client ou au Prospect 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 ou les Prospect 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 BPCE SA 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 ou du Prospect 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 ou du Prospect 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 ou du Prospect contenue dans le certificat transmis ;
- la vérification des données d'horodatage apposées sur la signature électronique du Client ou du Prospect ;
- 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 ou des Prospect 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.

4.6.2 Vérification des droits du signataire en fonction de données transmises

Suivant qu'il s'agisse d'un Client ou d'un Prospect, les produits « Contrats » qui peuvent être signés électroniquement ne sont pas les mêmes.

Cette séparation vient du niveau d'authentification qui a pu être mis en œuvre pour identifier un Client (déjà connu par l'établissement du Groupe BPCE) ou un Prospect (identification basée sur des données déclarées par le Prospect).

4.7 Gestion de la preuve

Pour conserver une trace de chaque validation de signature, BPCE SA 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 ou Prospect d'un côté et établissement du Groupe BPCE de l'autre),
- Certificat de signature utilisé par le Client ou le Prospect,
- 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 Classification des informations

Les informations suivantes sont considérées comme confidentielles :

- les données secrètes associées au certificat (clé privée),
- les journaux de l'application « Dématérialisation des contrats »,
- les procédures internes à IT-CE permettant d'assurer la disponibilité de l'application « Dématérialisation des contrats » mise à disposition des établissements du Groupe BPCE,
- les rapports d'audit sur cette application et sur les différents composants de l'infrastructure.

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 Droit applicable

Le présent document est régi par la loi française.

6.2 Règlement des différends

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux de Paris.

6.3 Propriété intellectuelle de l'infrastructure de création et de validation des signatures

Tous les logiciels participants à la constitution et à la validation du document signé sont mis à disposition des Clients ou des Prospects via une demande auprès de l'établissement du Groupe BPCE concerné.

Les Clients ou les Prospects ne disposent d'aucun droit de propriété intellectuelle sur ces différents éléments.

Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent, par quelque procédé que ce soit, est strictement interdite et constitue une contrefaçon sanctionnée par le Code de la propriété intellectuelle, sauf accord préalable et écrit du Groupe BPCE.

6.4 Données nominatives

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 nominatives réalisé par BPCE SA ont fait l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Le Client ou le Prospect est informé qu'il dispose d'un droit d'accès, de rectification et d'opposition portant sur les données le concernant en écrivant à BPCE SA.

Les Clients ou les Prospects sont tenus de respecter les dispositions de la loi relative à l'informatique, aux fichiers et aux libertés, dont la violation est passible de sanctions pénales.

Ils doivent notamment s'abstenir, s'agissant des informations nominatives auxquelles ils accèdent, de toute collecte, de toute utilisation détournée et, d'une manière générale, de tout acte susceptible de porter atteinte à la vie privée ou à la réputation des personnes.

7 DEFINITIONS

Les définitions et acronymes sont référencées dans le document annexe suivant : « Mesures communes, définitions et acronymes applicables à l'ICG ». Cette annexe est publiée au sein du même espace que la présente politique.