Politique de Signature et de Gestion de Preuves

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 Signature Electronique de Documents et met en œuvre les règles applicables à l'établissement et à la conservation des Dossiers de preuve. Le service de signature peut, quant à lui, avoir lieu à Distance ou en Face à face dans une agence du réseau.

1.1 Contexte juridique

En ce qui concerne les écrits dématérialisés, les principaux textes juridiques applicables sont :

Article 1366 *Code civil* :

> *« L'écrit électronique a la même force probante que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».*

Les articles 1366 et 1367 du *Code civil* constituent la base pour reconnaître la valeur juridique d'un écrit sous forme électronique. La Signature Electronique est donc essentielle pour les écrits sous forme électronique, parce qu'elle apporte (sous réserve du respect d'un minimum d'exigences) précisément :

1. « l'identification de son auteur » ;
2. La manifestation du consentement de l'auteur de l'acte ;
3. l'intégrité de cet écrit, du moins lors de son établissement.

L'intégrité de l'écrit dans le temps est une question d'*archivage*, c'est pourquoi la présente PSGP s'appuie sur une *Politique d'archivage*.

Les autres textes juridiques pouvant s'appliquer sont les suivants :

- Règlement n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS) (JOUE L. 257 du 28 août 2014, p. 73 et s). [EIDAS] ;

- Code civil réformé par l'Ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations (JO du 11 février 2016).

1.2 Contexte autres politiques

En pratique, la constitution de la preuve s'appuie sur plusieurs services de confiance et est par nature liée à la PSGP

Ces services peuvent être opérés par différents acteurs, liés entre eux par différentes conventions ou lois. Par conséquent, une PSGP est raisonnablement adossée également aux politiques des services suivants :

- Politique de certification (PC) ;

- Politique d'horodatage (PH) ;

- Politique d'archivage (PA).

1.3 Objet du document

L'objet de ce document est de décrire :

- Les conditions dans lesquelles sont réalisées, traitées, vérifiées et conservées les signatures électroniques,
- Les conditions dans lesquelles sont établis, conservés et consultés les dossiers de preuves.

1.4 Conformité normative

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 ET GESTION DE PREUVES

2.1 Champ d'application

La présente PSGP décrit les règles respectées par le Groupe BPCE pour :

- établir, vérifier et conserver les signatures électroniques des Documents,
- fournir l'ensemble des preuves liées à une transaction de signature électronique d'un contrat entre des Clients et des Etablissements du Groupe BPCE.

La présente PSGP est de la responsabilité de l'Autorité de gestion des Politiques (AP).

2.2 Identification du document

La présente PSGP appelée « Politique de Signature et de Gestion de Preuve du Groupe BPCE » est la propriété du Groupe BPCE.

Elle est identifiée par un numéro d'identification unique, l'OID : **1.3.6.1.4.1.40559.1.0.3.3.0.1.2**

D'autres éléments plus explicites (nom, numéro de version, date de mise à jour) permettent également de l'identifier.

Cette référence, ainsi que le numéro de version de la PSGP utilisée, doit obligatoirement figurer dans les données signées.

Lors de toute communication ultérieure, pour référencer la présente PSGP, 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 Approbation du document.

Le [CESSIG] constitue l'Autorité de Gestion des Politiques (AP).

L'Autorité de Gestion des Politiques (AP) est responsable de la validation de la Politique de Signature et de Gestion de Preuve.

L'AP agit conformément à la présente PSGP.

2.4 Publication du document

Avant toute publication officielle, la Politique de Signature et de Gestion de Preuve est validée par le comité de validation des Politiques [CESSIG].

La publication d'une nouvelle version de la Politique de Signature et de Gestion de Preuve 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 ;
- Le hash de la PSGP ;

La présente Politique de Signature et de Gestion de Preuve est publiée à l'adresse www.dossiers-securite.bpce.fr

L'ensemble des informations associées notamment les versions antérieures de ces documents avec leur période de validité, sont également publiées à l'adresse www.dossiers-securite.bpce.fr.

2.5 Processus de mise à jour

2.5.1 Circonstances rendant une mise à jour nécessaire

La mise à jour de la Politique de Signature et de Gestion de Preuve 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 PSGP est réexaminée a minima tous les ans.

2.5.2 Prise en compte des mises à jour

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

- Groupe BPCE
- Responsable 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 Groupe BPCE, qui engage si nécessaire le processus de mise à jour de la présente politique et qui redirige les demandes vers les acteurs concernés.

2.5.3 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 Groupe BPCE pour obtenir plus d'informations, en envoyant un mail à rssi-pssi-icg@bpce.fr.

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

La nouvelle version de la Politique de Signature et de Gestion de Preuve entre en vigueur dès qu'elle est publiée

Elle sera valide jusqu'à publication d'une nouvelle version.

Les versions précédentes sont archivées sur le site dans des conditions de nature à garantir le maintien d'intégrité.

2.7 Cohérence de la documentation

Cette Politique de Signature et de Gestion de Preuve ne constitue qu'une brique du référentiel documentaire du Groupe BPCE.

L'AP s'assure de la cohérence de ce référentiel documentaire et de l'adéquation de la présente Politique de Signature et de Gestion de Preuve avec les autres documents.

2.8 Définition et Acronymes

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

3 ACTEURS & ROLES

3.1 Les acteurs pour la PSGP

3.1.1 Clients

Le Client dispose d'un moyen d'Authentification qui permet de confirmer son identité avant d'entamer le processus de Signature.

3.1.2 Etablissement bancaire du Groupe BPCE

Chaque Etablissement dispose d'un Cachet électronique qui lui permet de signer un Document.

3.1.3 Destinataires des Documents signés électroniquement

Les destinataires des Documents signés électroniquement sont :

- Les Clients ;
- Les Etablissements et Filiales du Groupe BPCE.

3.1.4 Autorité de Signature et de Gestion des Preuves (ASGP)

L'Autorité de Signature et Gestion de Preuve est le Groupe BPCE, dûment représentée par son responsable, le Directeur de la Sécurité des Systèmes d'informations Groupe.

L'ASGP est garante du niveau de confiance des preuves qu'elle émet. Ce niveau de confiance repose sur des mesures techniques et organisationnelles et sur une gouvernance, qui sont décrits dans la présente PSGP

En particulier, l'ASGP a la responsabilité des fonctions suivantes :

- Mise en application de la PSGP,
- Signature Electronique des Documents,
- Gestion des preuves,
- Journalisation et archivage des événements et informations relatifs au fonctionnement de l'ASGP,
- Réception et traitement des demandes de preuves,
- Archivage des dossiers de demande de preuves.

Elle peut déléguer opérationnellement une partie de ses responsabilités.

3.1.4.1 Exigences de l'ASGP

L'ASGP est responsable des opérations relatives à la gestion des Dossiers de preuve réalisées par les composantes de son infrastructure. Elle garantit le contenu du Dossier de preuve et son intégrité.

L'ASGP veille à ce que l'ensemble des prestataires intervenant dans la gestion du Dossier de preuve se conforment aux exigences de la présente politique.

L'ASGP et son responsable doivent se conformer aux exigences de la présente Politique.

L'ASGP documente les relations contractuelles, les versions des contrats avec les Etablissements et les Clients, les conditions d'utilisation du service et la convention de service.

Les membres du personnel de l'ASGP et les exploitants mandatés à qui sont assignés des rôles relatifs à la gestion de la preuve sont personnellement responsables de leurs actes. L'expression « personnellement responsable » signifie que l'on puisse apporter la preuve qu'une personne a bel et bien fait telle action.

L'ASGP est auditable et est en mesure de répondre aux contrôles techniques et audits de qualité des procédures qui pourraient lui être demandés dans le cadre des obligations légales et de ses engagements.

L'ASGP met à jour et préserve l'intégrité des documents qu'il publie.

L'ASGP assure le contrôle de conformité de ses propres pratiques par rapport à la présente politique.

3.1.4.2 Exigences relatives à l'AC fournissant les certificats de l'ASGP

Les Certificats mis en œuvre dans ce cadre sont des Certificats Cachet émis par l'OT pour le compte du Service d'Archivage du Groupe BPCE. Il s'agit d'une AC technique interne à l'OT.

3.1.4.3 Limites de responsabilités de l'ASGP

L'ASGP n'est responsable de l'inexécution ou de la mauvaise exécution d'une de ses obligations qu'autant que celle-ci est due à sa faute, sa négligence ou à un quelconque manquement à ses obligations.

La responsabilité de l'ASGP ne peut être engagée en cas d'apparition soudaine et inattendue de vulnérabilités avérées sur des algorithmes utilisés pour signer les Documents et pour sceller les Dossiers de preuve.

Les établissements bancaires et financiers des réseaux Banques Populaires et Caisses d'Epargne sont seuls responsables de l'identité des Clients qu'ils transmettent en qualité d'Autorité d'Enregistrement. L'ASGP reste responsable de la validation de la Signature électronique d'un Document ave une identité Client même si celle-ci est erronée du fait d'une erreur de saisie ou d'absence de vérification d'une autorité d'enregistrement.

Il est toutefois précisé que l'ASGP ne pourra en aucun cas être tenue pour responsable des préjudices indirects ou imprévisibles encourus par le Client, tels que notamment les pertes de chiffre d'affaires, de commandes, de bénéfices, de marge, de clientèle, de revenus réels ou anticipés, de réputation, préjudice d'exploitation, gain manqué ou économie attendue, absence d'atteinte de résultats escomptés, utilisation frauduleuse des données, inexactitude ou corruption de fichiers, de remise en cause des principes mathématiques de la cryptographie asymétrique en relation ou provenant de l'inexécution ou exécution fautive de la PSGP Sont également exclus de toute demande de réparation les dommages causés par un événement de force majeure ou cas fortuit.

Par ailleurs, l'ASGP ne pourra être tenue responsable de la qualité de la liaison Internet du Client, ni de la défaillance de l'opérateur de communications électroniques en charge de l'accès au réseau Internet ou de toute autre liaison mise en place afin de permettre la mise en ligne du Service.

De même, l'ASGP n'est pas non plus responsable des dommages résultant de la perte, de l'altération, de la destruction ou de toute utilisation frauduleuse de données, de la transmission accidentelle de virus ou autres éléments nuisibles via Internet.

Il est également convenu que l'ASGP ne peut être tenue responsable d'éventuels dysfonctionnements sur le poste du Client si ces dysfonctionnements font suite à une utilisation du Service ou à une manipulation du Client non conforme aux Conditions générales de signature électronique et/ou d'autres documents techniques.

3.1.5 Opérateur Fonctionnel

L'Opérateur Fonctionnel (OF) est chargé de la délivrance du service correspondant aux fonctions de l'ASGP :

- Il fait héberger, exploiter et maintenir par l'Opérateur Technique (OT), en conditions opérationnelles, les composants d'infrastructure et les interfaces de gestion ;
- Il s'engage sur le niveau de service de l'ASGP ;
- Il traite les demandes d'extraction des Dossiers de preuve.

3.2 Rôles et obligations du Signataire

3.2.1 Equipement informatique

L'équipement informatique du Client utilisé pour réaliser l'opération de signature doit lui permettre de se connecter sur le portail de l'Etablissement et de s'authentifier.

Des logiciels tiers ou drivers peuvent être requis et installés sur l'équipement informatique des Signataires.

L'environnement mis en œuvre par l'Etablissement est conforme aux règles de sécurité prévues par le Groupe BPCE.

3.2.2 Environnement du Service de signature électronique et de gestion de preuve

Le Service de signature électronique et de gestion de preuve constitue un élément essentiel de l'ICG.

En particulier, il est mis en œuvre :

- La surveillance de l'accès physique et logique au système et la protection contre les intrusions,
- Une limitation d'accès et d'administration du Service de signature électronique et de gestion de preuve à un minimum de personnes de confiance, ayant les compétences préconisées 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 Electronique.

Ils utilisent pour cela le Service de signature électronique et de gestion de preuve, mis à disposition par le Groupe BPCE.

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

3.2.4 Type de certificat utilisé

Les Certificats « éphémères », « à la volée » ou « à usage unique » : le Certificat est généré par l'application de l'Autorité de Certification de l'ICG au moment de l'opération de Signature du Document par le Client. Ce Certificat a une durée de validité limitée dans le temps.

L'Etablissement du Groupe BPCE avec qui le document est signé dispose également d'un certificat de signature de type Cachet serveur qui l'engage.

Dans le processus de signature, des Certificats d'Horodatage et d'Archivage 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 », « à la volée » ou « à usage unique » 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 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

La procédure de révocation d'un Certificat Client est écrite dans la PC qui est utilisée pour gérer les Certificats Client.

3.2.7 Obligations du Client

Le Client prend connaissance et accepte les Conditions Générales du Service de Signature.

3.2.8 Limitations des responsabilités du Groupe BPCE

3.2.8.1 Mise à jour des informations utilisées

Certaines données, notamment les listes de révocation, 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'Etablissement du Groupe BPCE.

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

La mise en œuvre d'un service OCSP permet la mise à jour en temps réel des listes de révocation.

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

3.2.8.2 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 Electronique, le Client accède à un ou plusieurs moyens d'Authentification.

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 de manière sécurisée,
- 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 référencés émis par une autorité de certification reconnue par le Groupe BPCE et conforme aux exigences RGS et/ou équivalent PAC,
- L'Authentification basée sur 2 moyens d'authentification sécurisés (exemple Sécur'pass): l'enrôlement d'un téléphone mobile et la détention de ce matériel lors de la Signature pour la saisie d'un mot de passe.

Le processus de Signature Electronique se déroule en 3 étapes :

1. Lecture et consentement des Documents,
2. Authentification ,
3. Signature des Documents.

Une fois signés, les Documents sont mis à disposition du Client et archivés.

4.1 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'Etablissement 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.

4.2 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 Face à face ;
- Du Client lorsque la signature se fait à Distance.

L'utilisation de Certificats sur support matériel nécessite la présence d'une application sur le poste client.

4.3 Caractéristiques des signatures

4.3.1 Type de signature

Les Signatures Electroniques sont des signatures « à la volée » apposées par les Clients sur des fichiers PDF.

4.3.2 Norme de signature

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

4.4 Algorithmes utilisables pour la signature

4.4.1 Algorithme de condensation

L'algorithme de condensation supporté est SHA-2.

4.4.2 Algorithme de chiffrement

L'algorithme de chiffrement utilisé est *RSA Encryption*.

4.4.3 Canonicalisation

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

4.5 Vérification de la Signature

Sous réserve du respect des critères d'éligibilité à la Signature Electronique, 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 Electronique 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 Cachets mis en œuvre par les Etablissements 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 PSGP référencée.

L'ASGP propose deux solutions pour mettre en œuvre la vérification des Signatures électroniques des documents PDF :

- Intégration dans les applications web des réseaux bancaires du Groupe BPCE d'un lecteur adapté permettant de visualiser les Signatures des documents PDF ;

- Visualisation de la Signature des documents PDF dans le lecteur PDF du Client lorsque le logiciel utilisé par le Client le permet.

5 GESTION DU CYCLE DE VIE DE LA TRANSACTION ET DE LA PREUVE

5.1 Contexte et éléments de preuve

5.1.1 Contexte

A l'issue de la transaction de signature, un Dossier de preuve est constitué et conservé dans l'ICG du Groupe BPCE si l'archivage de la transaction a été demandé par l'Application métier.

5.1.2 Éléments de preuve concernés par la PSGP

La solution mise en œuvre consiste à collecter les éléments suivants pour constituer le Dossier de preuve :

- Document signé par l'ensemble des Parties (Client d'un côté et Etablissement du Groupe BPCE de l'autre),
- Certificat de Signature utilisé par le Client,
- Certificat Cachet utilisé par l'Etablissement du Groupe BPCE,
- Résultat de la vérification,
- Statut de contrôle de la Liste de Certificats Révoqués,
- L'ensemble des chaînes de certification mises en œuvre (AC racine et AC intermédiaire),
- Trace d'audit générée par le serveur de signature.

Ce Dossier de preuve est signé par un Certificat Cachet.

5.1.3 Données exclues de la PSGP

Toutes les traces liées à la gestion de la clé privée utilisée pour signer les Documents ne font pas partie du Dossier de preuve.

5.2 Cycle de vie des Dossiers de preuve

5.2.1 Processus de constitution du Dossier de preuve

Les éléments de preuve sont générés au terme du processus de signature et sont transmis via une API au service d'Archivage qui signe les données au moment du dépôt.

5.2.2 Versement des Dossiers de preuve

Les données sont signées par le serveur d'archivage au moment de la réception des données par un Certificat Cachet propre au service d'archivage. Chaque Etablissement du Groupe BPCE dispose d'un espace cloisonné sur le service d'Archivage qui garantit la confidentialité des Dossiers de preuve entre les établissements.

5.2.3 Procédure de vérification des Dossiers de preuve au moment du dépôt

La validation s'effectue sur la base de la vérification du Cachet horodaté du Dossier de preuve au moment de son dépôt dans le Service d'Archivage.

5.2.4 Conservation des Dossiers de preuve

Les éléments de preuve sont conservés durant la durée légale et dépendent du type de Document signé conformément à la Politique d'Archivage.

5.2.5 Restitution des Dossiers de preuve

Les éléments de preuve peuvent être fournis dans le cadre d'une enquête légale et sur la réquisition d'un juge. La demande de restitution de la preuve est opérée manuellement par l'O.S.G.P. qui remet les éléments de preuves tels qu'ils sont contenus dans le Service d'Archivage sous la forme d'un dossier compressé contenant :

- Eventuellement la copie de la carte d'identité du Client ;
- Les documents PDF signés ;
- Les preuves de signatures au format XML.

5.2.6 Pérennisation des Dossiers de preuve

Cette section décrit les mesures mises en œuvre pour assurer la conservation à moyen ou long terme de la preuve, « *dans des conditions de nature à en garantir l'intégrité* ».

5.2.6.1 Moyens physiques

Les services assurant le stockage et l'archivage des Dossiers de preuve sont assurés sur deux sites distants avec une réplication synchrone des données.

Ces services font l'objet de sauvegardes quotidiennes.

5.2.6.2 Moyens organisationnels

Le système de génération du Dossier de preuve est un système déclenché automatiquement à la fin du processus de Signature.

Sous réserve de l'activation préalable pour une Application métier, toute transaction de Signature fait donc l'objet d'une constitution d'un Dossier de preuve sans intervention humaine nécessaire.

Le processus de restitution d'un Dossier de preuve fait l'objet des moyens organisationnels décrits au paragraphe « Restitution des Dossiers de preuve ».

5.2.7 Vérification du Dossier de preuve

La vérification du dossier de preuve dans son ensemble consiste à analyser le contenu du dossier compressé. Tous les éléments du dossier de preuve sont lisibles humainement au travers de la visionneuse.

5.2.8 Établissement de l'Attestation de preuve

La solution mise en œuvre ne fournit pas d'Attestation de preuve dans le sens où aucun fichier n'est retourné au Client à la fin du processus de génération du Dossier de preuve. Néanmoins le Client dispose de tous les documents signés électroniquement, dont son contrat, la signature étant intégrée aux documents PDF.

Toutefois, une Attestation de preuve pourra être fournie au Client par le Chargé de Clientèle en cas de besoin.

5.2.9 Modalités de délivrance d'un Dossier de preuve

Le Dossier de preuve n'est pas mis à disposition du Client. Il sera transmis en cas de contentieux à l'autorité concernée. La demande d'extraction d'un Dossier de preuve est tracée par l'OF.

5.3 Traçabilité du cycle de vie de la preuve

5.3.1 Types d'événements enregistrés

Toutes les actions liées à la gestion d'un Dossier de preuve (dépôt, extraction) sont tracées par l'OT.

Les actions liées à la génération d'un Dossier de preuve sont signées au moment du dépôt. Il s'agit du fichier de suivi qui contient toutes les actions horodatées réalisées durant le processus de signature.

Les actions liées à la restitution d'un Dossier de preuve font l'objet d'une trace d'exploitation qui peut être fournie par l'OF ce processus de restitution étant organisationnel.

5.3.2 Fréquence des traitements des journaux d'événements

Les journaux d'exploitation sont analysés suite à la détection d'une anomalie. En fonction de cette anomalie, un rapprochement des journaux de chacune des composantes est mis en œuvre par l'opérateur technique.

5.3.3 Durée de conservation des journaux d'événements

Les journaux sont conservés directement sur le serveur, et font l'objet d'une sauvegarde conformément à la politique de sauvegardes des serveurs de l'O.S.G.P.

5.3.4 Protection des journaux d'événements

L'accès aux journaux d'événements est réalisé par des personnes habilitées de l'O.S.G.P. et nécessite une authentification.

5.3.5 Copies de sauvegarde des journaux d'événements

Voir « Durée de conservation des journaux d'événements ».

5.3.6 Système de collecte des journaux d'événements

Sans objet.

5.3.7 Imputabilité

Chaque trace de l'ASGP identifie de manière explicite la personne ou le système à l'origine de l'action. Des informations de datation de l'action sont également associées à cette trace.

5.4 Format des Dossiers de preuve

5.4.1 Format des Archives

Les Archives sont constituées d'un dossier compressé incluant les documents signés au format pdf, le fichier de l'ensemble des étapes de la cinématique de signature (piste d'audit) au format XML et fichier de preuve de signature au format XML.

5.4.2 Format de signature

Le format de signature mis en œuvre dans le cadre de la constitution du dossier de preuve est le format XAdES-T (signature) puis XAdES-A (conservation).

5.4.3 Algorithmes cryptographiques

Les signatures mises en œuvre utilisent les algorithmes RSA et la fonction de hachage SHA-256.

5.5 Fin de vie de l'ASGP

Une ou plusieurs composantes de l'ASGP peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'ASGP a pris les dispositions nécessaires pour couvrir les coûts permettant de respecter un certain nombre d'exigences minimales dans le cas où elle serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Les dispositions présentées ci-dessous, quand elles concernent l'O.S.G.P., figurent dans le contrat entre l'ASGP et l'O.S.G.P.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'ASGP ne comportant pas d'incidence sur la validité des Dossiers de preuve émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'ASGP en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'ASGP comportant une incidence sur la validité des preuves émises antérieurement à la cessation concernée.

5.5.1 Transfert d'activité ou cessation d'activité affectant une composante de l'ASGP

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'ASGP prend la mesure d'assurer la continuité du service d'archivage.

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des Clients ou des Prospects, l'ASGP s'engage à les informer de ce transfert aussitôt que possible et, au moins, 1 mois avant.

L'ASGP mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, la gêne pour les Clients et les Prospects.

5.5.2 Cessation d'activité affectant l'ASGP

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des Clients, l'ASGP s'engage à les informer de cette cessation aussitôt que possible et, au moins, 1 mois avant la cessation effective et s'engage à respecter les principes suivants :

- Les Dossiers de preuve constitués ne seront transmis- en aucun cas, hormis dans le cadre d'une procédure judiciaire ;
- Le Certificat cachet utilisé pour signer les Dossiers de preuve sera révoqué ;
- La clé privée du service de signature des A.D.P. sera détruite définitivement.

L'ASGP mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, la gêne pour les Clients.

6 MESURES DE SÉCURITÉ NON TECHNIQUES

Les exigences de ce chapitre 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.

7 MESURES DE SÉCURITÉ TECHNIQUES

7.1 Objectifs de sécurité propres au service de gestion de la preuve

Les services de gestion de la preuve mis en œuvre par le Groupe BPCE sont en mode « serveur ». Cela signifie que les équipements des Clients n'impliquent pas de critères de sécurité particuliers.

Dans ce cadre le serveur mis en œuvre est utilisé pour :

- Générer et protéger la clé privée correspondante au Certificat Cachet mis en œuvre pour la signature des Dossiers de preuve ;
- Réaliser les opérations de scellement du Dossier de preuve.

Le serveur bénéficie donc des mesures de sécurité nécessaires à la protection d'un tel système et ces mesures sont assurées directement par l'O.S.G.P.

Dans ce cadre, les systèmes informatiques supportant les fonctions de l'ASGP et mis à disposition par l'O.S.G.P. sont encadrés par les mesures de sécurité suivantes :

- Identification et authentification pour l'accès au système,
- Gestion des droits des utilisateurs, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles,
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels,
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- Protection du réseau contre toute intrusion d'une personne non autorisée,
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- Fonctions d'audits (non-répudiation et nature des actions effectuées),
- Gestion des reprises sur erreur.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont mis en place.

Ces mesures de sécurité sont explicitées dans des règles opérationnelles de sécurité et dans des documents d'exploitation utilisés par l'O.S.G.P.

7.2 Niveau de qualification des systèmes informatiques

Sans objet.

7.3 Mesures de sécurité des systèmes durant leur cycle de vie

7.3.1 Mesures de sécurité liées au développement des systèmes

La conception et le développement des systèmes informatiques, supportant les fonctions de l'ASGP, ont été réalisés dans le respect des normes et standards applicables.

Les aspects sécurité ont notamment été pris en compte.

La documentation existe et évolue en fonction des mises à jour.

Les systèmes informatiques sont testés dans un environnement de test dédié avant mise en production.

7.3.2 Mesures liées à la gestion de la sécurité

Le Comité Sécurité Groupe valide les évolutions à apporter aux systèmes afin de maintenir le niveau de sécurité de l'ASGP

Ces évolutions donnent lieu à des tests et à une mise à jour de la documentation et des procédures d'exploitation.

7.3.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

7.4 Mesures de sécurité réseau

L'architecture réseau des systèmes informatiques supportant les fonctions de l'ASGP respecte les bonnes pratiques en matière de sécurité réseau : cloisonnement, séparation des environnements (test / production), règles de filtrage, robustesse des équipements réseau, gestion de la haute disponibilité…

Des audits périodiques suivis d'actions correctrices sont menés pour lutter contre les vulnérabilités.

7.5 Horodatage / Système de datation

L'ASGP date les journaux d'événements avant de les envoyer vers l'archivage.

Le mécanisme de synchronisation est basé sur des flux NTP. La précision est inférieure à 1 seconde.

8 AUDITS

Les exigences de ce chapitre 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.

9 AUTRES DISPOSITIONS

9.1 Tarification

Non applicable.

9.2 Responsabilité financière

Le Groupe BPCE assume en fonds propres le règlement des litiges éventuels liés à l'Autorité de gestion des Preuves.

9.3 Protection des données à caractère personnel

Cf. Mesures communes.

9.4 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 PSGP.

9.5 Droit applicable

Le présent document est régi par la loi française.

9.6 Tribunaux compétents

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.

10 POLITIQUE DE CONFIDENTIALITÉ

10.1 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.

10.2 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.