Politique de Gestion des Preuves

BPCE SA

Référence du document	
1.3.6.1.4.1.40559.1.0.5.5.0.1.0	01 JUILLET 2013

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 467 226 960 €.

Siège social : 50 avenue Pierre Mendes France

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

SOMMAIRE

1 INTRODUCTION

Le présent document est le document de *Politique de Gestion de Preuve* (P.G.P.) de BPCE SA, mise en œuvre notamment dans le cadre de son application de dématérialisation des contrats. Une telle politique décrit les règles applicables à l'établissement et à la conservation des fichiers de preuve dans le cadre de services dématérialisés. Le présent document ne traite que des questions relatives au droit privé.

1.1 Contexte juridique : l'écrit à valeur probante (principaux textes juridiques applicables)

Article 1316-1 *Code civil* :

> *« L'écrit sous forme électronique est admis en preuve au même titre 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 1316-1 et 1316-4 du *Code civil* constituent la base pour reconnaître la valeur juridique d'un écrit sous forme électronique. La signature électronique 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 la personne dont il émane »
2. 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 une P.G.P. s'appuiera de même sur une *Politique d'archivage*.

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

- Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (J.O.C.E., n° L.013 du 19 janvier 2000, p. 12 et s.)
- Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (J.O. du 14 mars 2000, p. 3968)
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (J.O. du 22 juin 2004, p. 11168 et s.)
- Ordonnance n°2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique (J.O. du 17 juin 2005, p.10342)
- Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du *Code civil* et relatif à la signature électronique (J.O. du 31 mars 2001, p. 5070)

1.2 Les politiques voisines

En pratique, la constitution de la preuve s'appuie sur plusieurs services de confiance. Ces services peuvent être opérés par différents acteurs, liés entre eux par différentes

conventions, lois ou contrats. Par conséquent, une P.G.P. est raisonnablement adossée aux politiques de ces services :

- Politique de certification (P.C.)
- Politique d'horodatage (P.H.)
- Politique de signature (P.S.)
- Politique d'archivage (P.A.)

1.3 Champ d'application de la politique de gestion de preuve

La présente P.G.P. décrit les règles respectées par le BPCE SA pour fournir l'ensemble des preuves liées à une transaction de signature électronique d'un contrat entre des clients et/ou des prospects des établissements du BPCE SA.

La présente P.G.P. est de la responsabilité de BPCE SA.

1.4 Identification du document

La présente P.G.P. est identifiée par l'OID **1.3.6.1.4.1.40559.1.0.5.5.0.1.0.**

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

1.5 Entités intervenant dans la gestion de la preuve

1.5.1 Autorité de Gestion des Preuves (A.G.P.)

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

L'A.G.P. 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 Politique de Gestion des Preuves. L'A.G.P. veille à l'application de la présente Politique de Gestion des Preuves.

En particulier, l'A.G.P. a la responsabilité des fonctions suivantes :

- Mise en application de la P.G.P.
- Gestion des preuves.
- Journalisation et archivage des événements et informations relatifs au fonctionnement de l'A.G.P.
- Réception et traitement des demandes de preuves.
- Archivage des dossiers de demande de preuves.

Elle peut déléguer opérationnellement une partie de ses responsabilités.

1.5.2 Demandeurs

Les Demandeurs sont les personnes habilitées à faire une demande de preuve auprès de BPCE SA. Dans le cadre de la présente P.G.P., les demandeurs sont les clients ou les prospects du Groupe BPCE ayant signé un contrat dématérialisé.

Opérationnellement la demande est faite par le demandeur auprès d'un chargé de clientèle qui transmet alors la demande auprès de l'Opérateur de Service de Gestion des Preuves.

1.5.3 Opérateur de Service de Gestion des Preuves (O.S.G.P.)

L'Opérateur de Service de Gestion des Preuves est chargé de la délivrance du service technique correspondant aux fonctions de l'Autorité de Gestion des Preuves.

- Il héberge, exploite et maintient en conditions opérationnelles les composants d'infrastructure et les interfaces de gestion.
- Il s'engage sur le niveau de service de l'Autorité de Gestion des Preuves.
- Il traite les demandes d'extraction des dossiers de preuve.

L'O.S.G.P. est IT-CE. Il est lié par une convention de service avec BPCE SA.

1.6 Définition et Acronymes

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.

2 GESTION DE LA P.G.P

2.1 Entité gérant la P.G.P.

BPCE SA gère la P.G.P. via ses instances de pilotage et de décision de l'A.G.P. Dans ce cadre :

- BPCE SA édicte des règles dans la PSSI-Groupe et contrôle leurs applications
- IT-CE opère et le RSSI d'IT-CE contrôle et édicte les règles spécifiques

2.2 Point de contact

Les demandes d'informations ou questions concernant l'Autorité de Gestion des Preuves doivent être adressées à :

Directeur de la Sécurité des Systèmes d'informations Groupe

50 Rue Pierre Mendes France

75201 Paris Cedex 13

rssi-pssi-icg@bpce.fr

Ce point de contact est disponible et à jour sur le site de publication de l'Autorité de Gestion des Preuves (voir le paragraphe 2.5)

2.3 Déclaration de conformité de la P.G.P.

2.3.1 Entité déterminant la conformité d'une P.G.P.

Le Comité Sécurité Groupe (COSSIG) sous la responsabilité du RSSI-Groupe détermine la conformité de la P.G.P.

2.3.2 Procédures d'approbation de la conformité de la P.G.P.

L'approbation de la conformité de la P.G.P. est mise à l'ordre du jour du COSSIG. Ce dernier se base sur des résultats d'audits menés par le contrôle RSSI IT-CE et sur les PV de mise en production. Deux niveaux de contrôles sont alors appliqués.

- Contrôle niveau 1 par les équipes opérationnelles d'IT-CE
- Contrôle niveau 2 par les équipes sécurité IT-CE

2.4 Circonstances rendant une mise à jour nécessaire

La mise à jour d'une P.G.P. 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.

2.5 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 P.G.P. 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 P.G.P. est mise en ligne, un message électronique est diffusé sur le site http://pro.d00.pki01.bpce.fr/, accessible de tous les acteurs pour les informer de la nature et de la date et heure du changement.

La nouvelle version de la P.G.P. entre en vigueur dès qu'elle est publiée sur le site cité précédemment.

2.7 Publication de la P.G.P.

2.7.1 Informations publiées

La P.G.P. est mise à disposition de l'ensemble des acteurs via un lien de publication sur Internet.

2.7.2 Points de publication

La P.G.P. est publiée sur le site http://pro.d00.pki01.bpce.fr/.

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

3.1 Contexte et éléments de preuve

3.1.1 Contexte

La Politique de Gestion des Preuves s'applique au service de dématérialisation de contrats mis en œuvre par le Groupe BPCE dans ses établissements. Ce processus de dématérialisation fait intervenir les fonctions de signatures électroniques. Ces signatures sont réalisées à l'aide de certificats électroniques éphémères, valables le temps de la transaction de signature. Les Clients ou les Prospects signataires de ces contrats disposent du document PDF intégrant les signatures électroniques horodatées de leur contrat, celle du signataire et celle de l'établissement concerné du Groupe BPCE.

A l'issue de la transaction de signature, une enveloppe de preuve est constituée et conservée dans le système d'Archivage du Groupe BPCE.

A la demande d'un Client ou d'un Prospect, une demande de consultation de cette enveloppe de preuve peut être demandée. Cette demande est transmise par un chargé de clientèle auprès de l'O.S.G.P.

3.1.2 Éléments de preuve concernés par la P.G.P.

La solution mis en œuvre consiste à collecter les éléments suivants pour constituer l'enveloppe de preuve :

- 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 enveloppe de preuve est signée par un certificat cachet.

3.1.3 Données exclues de la P.G.P.

Tous les autres éléments de la transaction de signature ne sont pas conservés dans l'enveloppe de preuve. Notamment toutes les traces liées à la gestion de la clé privée utilisée pour signer les contrats ne font pas partie de l'enveloppe de preuve.

3.2 Cycle de vie de la preuve

Cette section décrit le processus de création des attestations de preuves.

3.2.1 Processus de constitution de la preuve

Cette section décrit précisément les canaux de réception des éléments de preuve :

3.2.1.1 Acteurs fournissant les preuves

Les éléments de preuve sont générés par le serveur de signature à la fin de ce processus. Les éléments mis dans le dossier de preuve sont :

- Le contrat ;
- La Signature horodatée du Client ou du Prospect ;
- La Signature horodatée de l'établissement du Groupe BPCE ;
- La trace d'audit générée par le serveur de signature.

3.2.1.2 Processus de génération des preuves

Ces 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.

3.2.2 Versement des preuves

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 établissement du Groupe BPCE dispose d'un espace cloisonné sur le service d'archivage qui garantit la confidentialité des données de preuve entre les établissements.

3.2.3 Procédure de vérification des preuves au moment du dépôt

Une validation des différentes signatures est ajoutée au dossier de preuve. Cette validation se fait sur la base de la vérification de la signature au moment de l'horodatage de la donnée.

3.2.4 Conservation de la preuve

Le service d'archivage mis en œuvre pour conserver les preuves est opéré par IT-CE.

La Politique d'Archivage applicable est définie sur le site : http://pro.d00.pki01.bpce.fr.

Les éléments de preuve sont conservés durant la durée légale et dépendent du type de contrat signé.

3.2.5 Restitution de la 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 :

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

3.2.6 Pérennisation de la 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 ». Ces mesures peuvent être décrites dans la politique d'archivage.

3.2.6.1 Moyens physiques

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

Ces services font l'objet de sauvegardes quotidiennes.

3.2.6.2 Moyens organisationnels

Le système de génération du dossier de preuve est un système déclenché automatiquement à la fin du processus de signature.

Toutes transaction de signature fait donc l'objet d'une constitution d'un dossier de preuve sans intervention humaine nécessaire.

Le processus d'extraction d'un dossier de preuve fait l'objet des moyens décrits au paragraphe 3.2.5.

3.2.7 Vérification de la preuve

L'A.G.P. 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 valider les signatures des documents PDF.

- Visualisation de la signature des documents PDF dans le lecteur Adobe du Client. Pour permettre la vérification complète de la signature, l'A.G.P. fournit au Client les moyens d'intégrer la chaîne d'AC nécessaire dans le lecteur PDF.

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.

3.2.8 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 ou au Prospect à la fin du processus de génération du dossier de Preuve. Néanmoins le Prospect ou le Client repart avec son contrat signé électroniquement, la signature étant intégrée au document PDF.

La génération du dossier de preuve étant une étape obligatoire du processus globale de signature, l'attestation de génération est acquise automatiquement si le Client ou le Prospect a obtenu son contrat signé.

3.2.9 Modalités de délivrance d'une preuve

La preuve n'est pas mise à disposition du client. Elle sera transmise devant un tribunal. La demande d'extraction d'un dossier de preuve est tracée par l'O.S.G.P.

3.3 Traçabilité du cycle de vie de la preuve

3.3.1 Types d'événements enregistrés

Toutes actions liées à la gestion d'une preuve (dépôt, restitution) sont tracées par le service d'archivage et font partie intégrante du fichier de suivi établi dans le dossier de preuve.

Les actions liées à la génération de la preuve sont signées au moment du dépôt du dossier de preuve. 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'OS.G.P., ce processus de restitution étant organisationnel.

3.3.2 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.

3.3.3 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.

3.3.4 Protection des journaux d'événements

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

3.3.5 Copies de sauvegarde des journaux d'événements

Voir 3.3.3.

3.3.6 Système de collecte des journaux d'événements

Sans objet.

3.3.7 Imputabilité

Chaque trace de l'A.G.P. 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.

3.4 Fin de vie de l'A.G.P.

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

L'A.G.P. 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'A.G.P. et l'O.S.G.P.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'A.G.P. ne comportant pas d'incidence sur la validité des preuves émises antérieurement au transfert considéré et la reprise de cette activité organisée par l'A.G.P. en collaboration avec la nouvelle entité.

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

3.4.1 Transfert d'activité ou cessation d'activité affectant une composante de l'A.G.P.

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'A.G.P. 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'A.G.P. s'engage à les informer de ce transfert aussitôt que possible et, au moins, 1 mois avant.

L'A.G.P. 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.

3.4.2 Cessation d'activité affectant l'AC

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des Clients et des Prospects, l'A.G.P. 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 preuves constituées ne seront transmises en aucun cas, hormis dans le cadre d'une procédure judiciaire ;
- Le certificat cachet utilisé pour signer les preuves sera révoqué ;
- La clé privée du service de signature des A.D.P. sera détruite définitivement.

L'A.G.P. 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.

4 OBLIGATIONS ET RESPONSABILITÉS DANS LE CYCLE DE VIE DE LA PREUVE

4.1 Obligations des acteurs en matière de gestion de la preuve

4.1.1 Obligations de l'A.G.P

- L'A.G.P. est responsable vis-à-vis de ses utilisateurs des opérations relatives à la gestion de la preuve réalisées par les composantes de son infrastructure. Elle garantit le contenu du fichier de preuve et son intégrité.

- L'A.G.P. veille à ce que l'ensemble des prestataires intervenant dans la gestion de preuve se conforme aux exigences de la présente politique.

- L'A.G.P. et son responsable doivent se conformer aux exigences de la présente Politique.

- L'A.G.P. et son personnel doivent respecter les droits des utilisateurs eu égard aux lois et règlements en vigueur.

- L'A.G.P. documente les relations contractuelles, les versions des contrats avec ses utilisateurs, les conditions d'utilisation du service et la convention de service.

- Les membres du personnel de l'A.G.P 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'A.G.P est auditable et est en mesure de répondre aux contrôles techniques et audits de qualité des procédures qui pourraient lui être demandées dans le cadre des obligations légales et de ses engagements.

- L'A.G.P met à jour et préserve l'intégrité des documents qu'il publie.

- L'A.G.P assure le contrôle de conformité de ses propres pratiques par rapport à la présente politique.

4.1.2 Obligations relatives à l'A.H

Voir la Politique d'Horodatage consultable depuis le lien suivant : http://pro.d00.pki01.bpce.fr.

4.1.3 Exigences relatives à l'A.C fournissant les certificats de l'A.G.P.

Les certificats mis en œuvre dans ce cadre sont des certificats de signature cachet émis par IT-CE pour le compte du service d'archivage du Groupe BPCE. Il s'agit d'une AC technique interne à IT-CE.

4.1.4 Exigences relatives à l'archiveur

Le tiers archiveur est l'opérateur technique des services de confiance du Groupe BPCE, IT-CE. Les règles liées à l'archivage des enveloppes de preuve sont décrites dans la

Politique d'Archivage correspondante, disponible sur le lien suivant : http://pro.d00.pki01.bpce.fr.

4.1.5 Obligations des utilisateurs du service

L'accès au système de gestion des preuves est lié à la souscription de l'offre de signature dématérialisée des contrats avec les établissements du Groupe BPCE. Dans ce cadre, le Client ou le Prospect est amené à prendre connaissance et à accepter les Conditions Générales du Service de Signature et reconnait ne pas avoir accès directement à la preuve.

4.2 Limites de responsabilités de l'A.G.P.

Sans objet

5 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.

6 MESURES DE SÉCURITÉ TECHNIQUES

6.1 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 postes des utilisateurs 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 de signature cachet mis en œuvre pour la signature des dossiers de preuves ;
- Réaliser les opérations de signature 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. IT-CE.

Dans ce cadre, les systèmes informatiques supportant les fonctions de l'A.G.P. 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.

6.2 Niveau de qualification des systèmes informatiques

Sans objet.

6.3 Mesures de sécurité des systèmes durant leur cycle de vie

6.3.1 Mesures de sécurité liées au développement des systèmes

La conception et le développement des systèmes informatiques supportant les fonctions de l'A.G.P. 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.

6.3.2 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'A.G.P.

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

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

Sans objet.

6.4 Mesures de sécurité réseau

L'architecture réseau des systèmes informatiques supportant les fonctions de l'A.G.P. 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.

6.5 Horodatage / Système de datation

L'A.G.P. 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.

7 FORMAT DES PREUVES

7.1 Format des preuves

Les preuves sont contenues dans un dossier compressé qui contient :

- Le justificatif d'identité au format PDF ;
- Le contrat signé électroniquement par les deux parties au format PDF ;
- La preuve au format XML de la signature du contrat ;
- Le ou les avenants au contrat initial, signé électroniquement par les deux parties, au format PDF ;
- La preuve au format XML de la signature du ou des avenants ;
- Le fichier de suivi au format XML, traçant les actions du processus de signature ;
- Le fichier de scellement du dossier de preuve.

7.2 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.

7.3 Algorithmes cryptographiques

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

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

Non applicable.

9.3 Confidentialité des données à caractère personnel

La loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel s'applique à toutes les données détenues par l'A.G.P. Toutes les données collectées et détenues par l'A.G.P. sur une personne physique sont considérées comme confidentielles. Elles ne peuvent être divulguées que dans des conditions prévues par cette loi.

9.4 Droit applicable

Le présent document est régi par la loi française.

9.5 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.