Politique d'Archivage (PA)

BPCE SA

Référence du document	
1.3.6.1.4.1.40559.1.0.6.6.0.1.0 _	1 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 d'Archivage (P.A.) du Groupe BPCE, mise en œuvre dans le cadre de son application de dématérialisation des contrats. Une telle politique décrit les règles applicables à la constitution et la mise en archive des éléments liés au processus de signature dématérialisée des contrats. Les éléments archivés constituent en partie les éléments nécessaires à l'établissement des preuves. Le présent document ne traite que des questions relatives au droit privé.

La présente PA définit les exigences minimales, en termes juridiques, fonctionnels, opérationnels, techniques et de sécurité, que BPCE SA respecte afin que l'archivage électronique mis en place puisse être regardé comme fiable. Cette fiabilité a pour objectif de conserver aux Archives leur force juridique originelle tant en termes de preuve que de légalité. En conséquence, un acte électronique n'ayant aucune valeur juridique lors de son établissement ne pourra se voir conférer une telle valeur au seul motif qu'il a été archivé conformément à la présente PA. En outre, à défaut de texte juridique venant préciser les modalités pour qu'un archivage électronique soit regardé comme fiable, le juge reste seul compétent pour se prononcer sur ce point.

1.1 Principe de l'archivage

Ceci étant précisé, cette PA repose sur des contraintes « standards » à mettre en place. Il en est ainsi :

- des contraintes en matière d'identification/authentification de l'origine de l'archive;
- de l'intégrité des éléments d'archives ;
- de l'intelligibilité / lisibilité des archives ;
- de la durée / pérennité de l'archives ;
- de la traçabilité des différentes opérations (notamment versement, consultation, élimination) ;
- de la disponibilité et de l'accessibilité des archives.

La présente PA définit alors :

- Les prestations fournies aux services versant / producteur et aux usagers / utilisateurs en matière d'archivage électronique : périmètre des prestations, niveaux de service, type d'archivage (courant / intermédiaire / définitif),…
- Les obligations pesant sur les intervenants, à commencer par l'Autorité d'Archivage (AA), mais également les autres intervenants (Services producteurs / versants, Usagers / utilisateurs, Contrôleurs). Les obligations concernant les autres intervenants constituent les obligations minimales qu'ils doivent respecter afin que l'AA puisse fournir les prestations d'archivage conformément à sa PA.
- Les fonctionnalités mises en œuvre au sein du service d'archivage, sous la responsabilité de l'AA, afin de fournir ces prestations (fonction de versement, fonction de stockage,…) et l'organisation fonctionnelle correspondante (liens entre fonctions, flux d'information,…).

- Les principes de sécurité à respecter au niveau de l'AA et par les différentes fonctions, basés sur les trois catégories suivantes : principes organisationnels, principes de mise en œuvre, principes techniques.

1.2 Champ d'application de la politique d'archivage

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

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

1.3 Identification de la P.A

La présente P.A. est identifiée par l'OID **1.3.6.1.4.1.40559.1.0.6.6.0.1.0.**

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

1.4 Entités intervenant dans le service d'Archivage

1.4.1 Autorité d'Archivage (A.A.)

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

L'A.A. est garante du niveau de confiance des archives qu'elle constitue. Ce niveau de confiance repose sur des mesures techniques et organisationnelles et sur une gouvernance, qui sont décrits dans la présente Politique d'Archivage. L'A.A. veille à l'application de la présente P.A.

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

- Mise en application de la P.A.
- Gestion des archives.
- Journalisation et archivage des événements et informations relatifs au fonctionnement de l'A.A.
- Réception et traitement des demandes de mise en archive.
- Réception et traitement des demandes de restitution d'archives.

Elle peut déléguer opérationnellement une partie de ses responsabilités.

1.4.1 Services Producteur

Il s'agit dans le cadre de la présente P.A. du processus de signature dématérialisée mise en œuvre par le Groupe BPCE auprès des clients et/ou des prospects des établissements du Groupe.

Le service producteur est donc représenté dans ce cadre par un processus automatisé déclenché à la fin du processus de signature.

1.4.2 Services Versant

Dans le cadre de la présente P.A. le Service Versant est équivalent au Service Producteur.

1.4.3 Demandeurs

Dans le cadre de la présente P.A., les demandeurs ne sont pas directement les signataires clients et/ou prospects des établissements du Groupe BPCE.

Le service de Gestion des Preuves est le module en capacité de faire les demandes de récupération d'archives pour constituer les éléments de preuves nécessaires.

1.4.4 Opérateur de Service de l'Archivage Electronique (O.S.A.E.)

L'Opérateur de Service de l'Archivage Electronique est chargé de la délivrance du service technique correspondant aux fonctions de l'A.A.

- 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'A.A.

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

1.5 Définition et Acronymes

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

2 GESTION DE LA P.A.

2.1 Entité gérant la P.A.

BPCE SA gère la P.A. via ses instances de pilotage et de décision de l'A.A. 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 d'Archivage doivent être adressées à :

Directeur de la Sécurité des Systèmes d'informations Groupe (RSSI Goupe)

50 Avenue 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 d'Archivage (voir le paragraphe 2.5)

2.3 Déclaration de conformité de la P.A.

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

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

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

L'approbation de la conformité de la P.A. 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.A. 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.A. 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.A. 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.A. entre en vigueur dès qu'elle est publiée sur le site cité précédemment.

2.7 Publication de la P.A.

2.7.1 Informations publiées

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

2.7.2 Points de publication

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

3 GESTION DU CYCLE DE VIE DE L'ARCHIVE

3.1 Contexte et éléments d'archive

3.1.1 Contexte

La P.A. 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, des éléments sont déposés dans un conteneur d'archive dédié à l'établissement concerné. Un plan de classement est mis en œuvre pour cloisonner fonctionnellement le système d'archive.

3.1.2 Éléments d'archives

La solution mise en œuvre consiste à archiver le dossier de preuve transmis par l'application de signature à l'issue du processus.

3.1.3 Données exclues du système d'archivage

En dehors du dossier de preuve, aucun autre élément n'est archivé au niveau du processus de signature. Un duplicata du contrat signé par les deux parties est néanmoins réalisés avant la mise en archive et ce duplicata est déposé dans les outils de gestion documentaire des établissements concernés.

3.2 Cycle de vie de l'archive

Cette section décrit le processus de mise en archive.

3.2.1 Processus de constitution de l'archive

Cette section décrit précisément les modalités de constitution de l'archive :

3.2.1.1 Fourniture des éléments par le Service Producteur

Les éléments constituants de l'archive sont fournis par le serveur de signature opéré par IT-CE.

Ce serveur de signature fournit à l'archivage le dossier de preuve sous une forme compressée.

3.2.1.2 Processus de génération de l'archive

L'archive est générée au terme du processus de signature et est transmise via une API au service d'archivage qui signe les données au moment du dépôt. La signature se fait au moment du dépôt dans le coffre-fort numérique correspondant et est réalisée via un certificat cachet technique propre à l'O.S.A.E.

3.2.2 Versement des archives

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 entre les établissements.

3.2.3 Etablissement d'un plan de classement des archives

Le plan de classement mis en œuvre est celui décrit de la manière suivante :

- 1 coffre dédié par réseau du Groupe BPCE
- 1 armoire dédiée par établissement

3.2.4 Procédure de vérification des archives

L'O.S.A.E. dispose d'interface permettant de vérifier la présence d'une archive. Il s'agit nécessairement d'un processus manuel qui doit faire l'objet d'une demande tracée.

3.2.5 Conservation de l'archive

Les archives sont conservées durant la durée légale et dépendent du type de contrat signé.

3.2.6 Recherche d'une archive

L'O.S.A.E. dispose d'interface permettant de rechercher la présence d'une archive. Il s'agit nécessairement d'un processus manuel qui doit faire l'objet d'une demande tracée.

3.2.7 Restitution de l'archive

L'archive ne peut pas être restituée directement. Le contenu de l'archive, lorsu'il s'agit d'un dossier de preuve, n'est restitué que dans le cadre d'une procédure judiciaire à des personnes habilitées.

Néanmoins le chargé de clientèle peut consulter une copie (duplicata-GED) du contrat signé via ces outils de consultation. A savoir que dans ce cadre l'archive dite à valeur probatoire reste stockée au niveau du service d'archivage de BPCE SA et ne peut être consultée directement par le chargé de clientèle.

3.2.8 Suppression de l'archive

Les archives ne peuvent pas être supprimées.

3.2.9 Pérennisation de l'archive

3.2.9.1 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.

3.2.9.2 Moyens organisationnels

La pérennisation des archives ne nécessitent pas actuellement de moyens organisationnels spécifiques. Néanmoins l'A.A. s'assurera que les moyens nécessaires seront mis en œuvre dans le cadre de l'ouverture de son service d'archivage pour d'autres éléments que les dossiers de preuve.

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 archive (dépôt, accès aux interfaces de recherche ou de vérification) sont tracées par le service d'archivage.

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.A.E.

3.3.4 Protection des journaux d'événements

L'accès aux journaux d'événement est réalisé par des personnes habilités de l'O.S.A.E. 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.A. 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.A.

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

L'A.A. 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.A.E., figurent dans le contrat entre l'A.A. et l'O.S.A.E.

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

La cessation d'activité est définie comme la fin d'activité d'une composante de l'A.A. 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.A.

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

L'A.A. 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'A.A.

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

L'A.A. 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 L'ARCHIVE

4.1 Obligations des acteurs en matière d'archivage

4.1.1 Obligations de l'A.A.

- L'A.A. est responsable vis-à-vis de ses utilisateurs des opérations relatives à la gestion des archives réalisées par les composantes de son infrastructure. Elle garantit le contenu de l'archive et son intégrité.

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

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

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

- L'A.A. doit documenter 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.A. et les exploitants mandatés à qui sont assignés des rôles relatifs à la gestion des archives doivent être 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 une action.

- L'A.A. doit être auditable et être 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.A. doit utiliser des ressources cryptographiques d'un niveau de sécurité suffisant pour le service d'archivage.

- L'A.A. doit mettre à jour et préserver l'intégrité des documents qu'il publie.

- L'A.A. doit assurer 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.A.

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 sont décrites dans la présente Politique d'Archivage.

4.1.5 Obligations des Services Versants

L'accès au système d'archivage est lié à la souscription de l'offre de signature dématérialisée des contrats avec les établissements du Groupe BPCE.

4.2 Limites de responsabilités de l'A.A.

Non applicable

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'Infrastructure de Confiance Groupe ». 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 d'archivage

Le service d'archivage mis en œuvre par le Groupe BPCE est 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 archives ;
- Réaliser les opérations de signature de l'archive au moment du dépôt.

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.A.E. IT-CE.

Dans ce cadre, les systèmes informatiques supportant les fonctions de l'A.A. et mis à disposition par l'O.S.A.E. 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.A.E.

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.A. 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.A.

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.A. 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.A. 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 archives

Les archives sont constituées d'un dossier compressé et du fichier de signature au format XML.

7.2 Format de signature

Le format de signature mis en œuvre dans le cadre de la constitution de l'archive 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.

7.4 Certificats

7.4.1 Certificats de signature

Paramètre	**Valeur**
AC émettrice	AC SIGNATURE ICG D01-01
DN du certificat	CN = SCEL <*enseigne du réseau du Groupe BPCE*> OU = 0002 552028839 O = BPCE C = FR
Taille de la clé	2048
Durée de validité	**1096** (3 ans)
Usage de la clé	Signature numérique, Non répudiation (critique)
Usage avancé de la clé	Ø
CRL DP	Oui

7.4.2 Certificats d'horodatage

Paramètre	**Valeur**
AC émettrice	AC SIGNATURE ICG XXX

DN du certificat	CN = **HPRE** <*enseigne du réseau du Groupe*> OU = 0002 552028839 O = BPCE C = fr
Taille de la clé	2048
Durée de validité	**1827** (5 ans)
Usage de la clé	Signature numérique, Non répudiation (critique)
Usage avancé de la clé	Horodatage (critique) Enregistrement des informations de date (1.3.6.1.5.5.7.3.8)
CRL DP	Oui

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.