Politique d'Archivage

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 INTRODUCTION

Le Groupe BPCE, pour ses réseaux Caisse d'Epargne, Banque Populaire et Filiales, met en œuvre pour ses Clients un service de dématérialisation des Documents intégrant un processus d'Archivage électronique. Ce service d'Archivage électronique est composé de la constitution et de la mise en Archive des Documents.

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.

Le présent document constitue la Politique d'Archivage (PA) du Groupe BPCE. Il a pour objet de décrire la gestion des Archives et leur cycle de vie.

La présente PA définit les exigences minimales, en termes juridiques, fonctionnels, opérationnels, techniques et de sécurité, que le Groupe BPCE 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 document 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, l'article 1366 du code civil met en exergue la nécessité de conserver de manière intègre dans le temps le Document électronique.

La présente PA est élaborée conformément au document : « Electronic Signatures and Infrastructures (ESI), Data preservation Systems Security », Part 1: Requirements for Implementation and Management ETSI TS 101 533-1 v 1.2.1.

1.1 Principe de l'archivage

La présente PA détaille les exigences à respecter :

- 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 des 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 des intervenants : Autorité d'Archivage (AA), Services producteurs / versants, Usagers / utilisateurs, Contrôleurs.
- Les fonctionnalités mises en œuvre au sein du Service d'Archivage, 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.

1.2 Champ d'application de la Politique d'Archivage

La présente PA décrit les exigences respectées par le Groupe BPCE pour son service d'Archivage électronique dans le cadre de la dématérialisation des Documents de ses réseaux Caisse d'Epargne, Banque Populaire et Filiales, et mis en œuvre pour ses Clients.

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

1.3 Identification du document

La présente PA appelée : « Politique d'Archivage du Groupe BPCE » est la propriété du Groupe BPCE.

Elle est identifiée un numéro d'identification unique, l'OID : **1.3.6.1.4.1.40559.1.0.6.6.0.1.2**

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

Lors de toute communication ultérieure, pour référencer la présente PA, 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 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 d'Archivage.

L'AP agit conformément à la présente PA et à la DPA associée.

1.5 Publication du document

Avant toute publication officielle, la Politique d'Archivage est validée par le comité de validation des Politiques [CESSIG].

La publication d'une nouvelle version de la Politique d'Archivage 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 PA.

La présente Politique d'Archivage 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.

1.6 Processus de mise à jour

1.6.1 Circonstances rendant une mise à jour nécessaire

La mise à jour de la Politique d'Archivage 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 Politique d'Archivage est réexaminée *a minima* tous les ans.

1.6.2 Prise en compte des mises à jour

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

- Groupe BPCE
- Responsable de la Sécurité des Systèmes d'informations Groupe
- 50 Avenue 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.

1.6.3 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.

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

La nouvelle version de la Politique d'Archivage 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.

1.8 Déclaration de conformité de la PA

1.8.1 Entité déterminant la conformité d'une DPA avec cette PA

L'AP détermine la conformité de la DPA à la présente PA.

1.8.2 Procédures d'approbation de la conformité de la DPA

L'AP possède ses propres méthodes pour approuver le présent document. L'AP procède à des analyses/contrôles de conformité et/ou des audits. L'AP approuve les résultats de la revue de conformité effectuée par les experts qu'elle nomme à cet effet et détermine en fonction des résultats la conformité de la DPA.

1.9 Cohérence de la documentation

Cette Politique d'Archivage 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 d'Archivage avec les autres documents.

1.10 Entités intervenant dans le service d'Archivage

1.10.1 Autorité d'Archivage (AA)

L'AA 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 décrites dans la présente Politique d'Archivage. L'AA veille à l'application de la présente PA

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

- Mise en application de la PA ;
- Gestion des Archives ;
- Journalisation et archivage des événements et informations relatifs au fonctionnement de l'AA ;
- 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.

1.10.2 Services Producteur

Il s'agit dans le cadre de la présente PA du processus de signature dématérialisée mise en œuvre par le Groupe BPCE auprès des Clients 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. Ce processus automatisé est en charge de constituer les différents documents à déposer dans le système d'archivage.

1.10.3 Services Versant

Dans le cadre de la présente PA, il s'agit d'un service automatisé qui est en charge de déposer les documents dans le système d'archivage.

1.10.4 Demandeurs

Dans le cadre de la présente PA, les demandeurs sont identifiés au sein des établissements du Groupe BPCE. Les Clients ne peuvent pas demander directement de restitution de Dossier de preuve.

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

Le Service d'Archivage est mis en œuvre par l'opérateur de Service de l'Archivage Electronique pour le compte du Groupe BPCE. Il est chargé de la délivrance du service technique correspondant aux fonctions de l'AA :

- 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'AA

Il s'agit de l'Opérateur Technique.

1.11 Définition et Acronymes

Les définitions et acronymes sont référencés dans le document: « Mesures communes », publié au même endroit que la présente politique.

2 GESTION DU CYCLE DE VIE DE L'ARCHIVE

2.1 Contexte et éléments d'Archive

2.1.1 Contexte

La PA s'applique au service de dématérialisation de Documents mis en œuvre par le Groupe BPCE. Ce service de dématérialisation fait intervenir des fonctions de Signature électronique.

A l'issue du processus de Signature électronique, 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'archivage.

2.1.2 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 de Signature électronique.

2.1.3 Données exclues du Service d'archivage

En dehors du Dossier de preuve, aucun autre élément n'est archivé.

Un duplicata des documents signés par les deux parties peut être réalisé avant la mise en Archive et déposé dans les outils de gestion documentaire des établissements concernés.

2.2 Cycle de vie de l'Archive

Cette section décrit le processus de mise en Archive.

2.2.1 Processus de constitution de l'Archive

Cette section décrit précisément les modalités de constitution de l'Archive.

2.2.1.1 Fourniture des éléments par le Service Producteur

Les éléments constituants de l'Archive sont fournis par le processus de Signature électronique. Il fournit à l'archivage le dossier de preuve sous une forme compressée.

2.2.1.2 Processus de génération de l'Archive

L'Archive est générée au terme du processus de signature et est transmise par le service versant au Service d'Archivage. Le Service d'Archivage chiffre et scelle les données au moment du dépôt dans le coffre-fort numérique correspondant de l'Etablissement bancaire ou filiale.

2.2.2 Versement des Archives

Les données sont chiffrées et scellées par le serveur d'archivage au moment de la réception des données au moyen de Certificats propres au Service d'Archivage.

Chaque Etablissement du Groupe BPCE dispose d'un espace cloisonné sur le Service d'Archivage qui garantit la confidentialité des données entre les établissements.

2.2.3 Etablissement d'un plan de classement des Archives

Le plan de classement mis en œuvre est le suivant :

- 1 coffre électronique dédié par Réseau du Groupe BPCE
- 1 armoire électronique dédiée par établissement

2.2.4 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.

2.2.5 Conservation de l'Archive

Les Archives sont conservées et ne sont pas purgées durant la validité du Document.

2.2.6 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.

2.2.7 Restitution de l'Archive

L'Archive (Dossier de preuve à valeur probatoire) est restituée dans le cadre d'une procédure judiciaire à des personnes habilitées. Elle n'est pas accessible au chargé de clientèle et ne peut pas être restituée directement au Client.

Néanmoins le chargé de clientèle peut consulter une copie (duplicata-GED) du Document signé via ses outils de consultation de GED.

L'extraction d'une copie de l'Archive fait l'objet d'une procédure applicable selon l'organisation interne des Etablissements bancaires. (Service Juridique ou Service Contentieux).

2.2.8 Suppression de l'Archive

Les Archives ne peuvent pas être supprimées.

2.2.9 Pérennisation de l'Archive

2.2.9.1 Moyens physiques

Les services assurant le stockage et l'archivage des preuves sont assurés sur deux sites distants avec une réplication synchrone des données.
Le Service d'Archivage dispose de moyens pour garantir que les Archives ne sont pas corrompues.
La lisibilité des Archives dans le temps est assurée du fait des mises à jour matérielles.
Ces services font l'objet de sauvegardes quotidiennes.

2.2.9.2 Moyens organisationnels

La pérennisation des preuves de dépôts des Archives est effectuée par l'OSAE selon ses procédures au moment du renouvellement des Certificats de chiffrements.

2.3 Traçabilité du cycle de vie de la preuve

2.3.1 Types d'événements enregistrés

Toutes actions liées à la gestion d'une Archive (dépôt, accès aux interfaces de recherche ou de vérification) sont tracées.

2.3.2 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.

2.3.3 Durée de conservation des journaux d'événements

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

2.3.4 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.

2.3.5 Copies de sauvegarde des journaux d'événements

Les sauvegardes sont réalisées conformément à la politique de sauvegardes des serveurs de l'O.S.A.E.

2.3.6 Système de collecte des journaux d'événements

Une collecte de logs liés à l'ICG est réalisée et des analyses sont effectuées au niveau du SOC.

2.3.7 Imputabilité

Chaque trace de l'AA 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.

2.4 Fin de vie de l'AA

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

L'AA 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.

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

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

2.4.1 Transfert d'activité ou cessation d'activité affectant une composante de l'AA

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AA 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 utilisateurs du Service d'Archivage, l'AA les en avise aussitôt que nécessaire.

L'AA 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 utilisateurs du Service d'Archivage.

2.4.2 Cessation d'activité affectant l'AA

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des Utilisateurs du Service d'Archivage, l'AA s'engage à les informer de cette cessation aussitôt que possible et, au moins, 1 mois avant la cessation effective. L'AA s'engage à ce que Les Archives constituées ne soient transmises en aucun cas, hormis dans le cadre d'une procédure judiciaire.

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

3 OBLIGATIONS ET RESPONSABILITÉS DANS LE CYCLE DE VIE DE L'ARCHIVE

3.1 Obligations des acteurs en matière d'archivage

3.1.1 Obligations de l'AA

- L'AA est responsable vis-à-vis des Etablissements et Filiales, 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'AA veille à ce que l'ensemble des prestataires intervenant dans la gestion des Archives se conforme aux exigences de la présente politique.
- L'AA et son responsable doivent se conformer aux exigences de la présente Politique.
- L'AA et son personnel doivent respecter les droits des utilisateurs eu égard aux lois et règlements en vigueur.
- L'AA doit documenter les relations avec les autres composants techniques de l'infrastructure de Confiance Groupe.
- Les membres du personnel de l'AA 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'AA 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'AA doit utiliser des ressources cryptographiques d'un niveau de sécurité suffisant pour le Service d'Archivage.
- L'AA doit mettre à jour et préserver l'intégrité des documents qu'il publie.
- L'AA doit assurer le contrôle de conformité de ses propres pratiques par rapport à la présente politique.

3.1.2 Exigences relatives à l'AH fournissant les contremarques de temps

L'AA s'appuie sur le service d'horodatage respectant les exigences décrites dans la politique d'horodatage consultable depuis le lien suivant : www.dossiers-securite.bpce.fr .

3.1.3 Exigences relatives à l'AC fournissant les Certificats de l'AA

Les Certificats utilisés par le Service d'Archivage sont des Certificats techniques émis par une AC technique interne au Groupe BPCE.

3.1.4 Exigences relatives à l'Archiveur

Le tiers Archiveur est l'opérateur technique des services de confiance du Groupe BPCE. Les règles liées à l'archivage sont décrites dans la présente Politique d'Archivage.

3.1.5 Obligations des Services Versants

L'accès au système d'archivage est lié à la souscription de l'offre de signature dématérialisée des Documents mise à disposition des établissements du Groupe BPCE.

3.2 Limites de responsabilités de l'AA

L'AA est responsable des exigences et des principes édictés dans la présente PA, ainsi que de tout dommage causé à une application / utilisateur du Service d'Archivage suite à un manquement aux procédures définies dans la PA et la DPA associée.

L'AA décline toute responsabilité à l'égard de l'usage des Archives émises par elle dans des conditions et à des fins autres que celles prévues dans la PA ainsi que dans tout autre document contractuel applicable associé.

L'AA décline toute responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, et quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication.

L'AA ne saurait être tenue responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1218 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des cours et tribunaux français, les conflits sociaux, la défaillance des installations ou des réseaux de télécommunications externes.

L'AA n'est en aucun cas responsable des préjudices indirects subis par les entités utilisatrices, celles-ci n'étant pas pré-qualifiées par les présentes.

En cas de prononcé d'une quelconque responsabilité de l'AA, les dommages, intérêts et indemnités à sa charge toutes causes confondues, et quel que soit le fondement de sa responsabilité, sont limités à la somme prévue au titre de limite de responsabilité dans les conditions générales d'utilisation applicables.

4 MESURES DE SÉCURITÉ NON TECHNIQUES

Les exigences de ce chapitre sont référencées dans le document suivant : « Mesures communes » publié au même endroit que la présente politique.

5 MESURES DE SÉCURITÉ TECHNIQUES

5.1 Objectifs de sécurité propres au Service d'Archivage

Le Service d'Archivage mis en œuvre par le Groupe BPCE est en mode « serveur ». Dans ce cadre, le serveur mis en œuvre est utilisé pour :

- Générer et protéger les clés privées correspondant aux Certificats de chiffrement mis en œuvre pour le Service d'Archivage ;
- Réaliser les opérations de protection 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.

Les systèmes informatiques supportant les fonctions de l'AA 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.

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.

5.2 Niveau de qualification des systèmes informatiques

Les composants du Service d'Archivage ont été conçus en suivant les recommandations des normes ETSI comme décrit en introduction de la présente PA.

5.3 Mesures de sécurité des systèmes durant leur cycle de vie

5.3.1 Mesures de sécurité liées au développement des systèmes

Le contrôle des développements des systèmes s'effectue comme suit :

- Des matériels et des logiciels achetés de manière à réduire les possibilités qu'un composant particulier soit altéré.
- Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce.
- Tous les matériels et logiciels sont expédiés ou livrés de manière contrôlée permettant un suivi continu depuis le lieu de l'achat jusqu'au lieu d'utilisation.
- Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de l'AA. Seules les applications nécessaires à l'exécution des activités sont acquises auprès de sources autorisées par politique applicable de l'AA. Les matériels et logiciels de l'AA font l'objet d'une recherche de codes malveillants dès leur première utilisation et périodiquement par la suite.
- Les mises à jour des matériels et logiciels sont achetées ou mises au point de la même manière que les originaux, et seront installés par des personnels de confiance et formés selon les procédures en vigueur.

5.3.2 Mesures liées à la gestion de la sécurité

La configuration du système de l'AA, ainsi que toute modification ou évolution, est documentée et contrôlée. Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration. Une méthode de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système. Lors de son premier chargement, on vérifie que le logiciel de l'AA bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

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

En ce qui concerne les logiciels et matériels évalués, l'AA poursuit sa surveillance des exigences du processus de maintenance pour maintenir le niveau de confiance.

5.4 Mesures de sécurité réseau

L'AA est en ligne accessible par des postes informatiques sous contrôle et uniquement d'un réseau interne à l'OSAE. L'AA n'est pas hébergée sur le même réseau que le service de Publication. Le principe de défense en profondeur est appliqué.

Les composantes accessibles de l'AA sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu.

Les autres composantes de l'AA utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion provenant d'Internet.

Dans tous les cas, les mesures comprennent l'utilisation de pare-feu et de routeurs filtrants. Les ports et services réseau non utilisés sont coupés. Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système AA est hébergé refuse tout service, hormis ceux qui sont nécessaires au système AA, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.

Le réseau est protégé contre toute intrusion d'une personne ou d'un système non autorisé et assure la confidentialité et l'intégrité des données qui y transitent.

L'interconnexion de l'AA à des applications ou des utilisateurs ne remet pas en cause les règles de sécurité réseau prévues par l'AP.

5.5 Horodatage / Système de datation

L'AA utilise une datation sûre, régulièrement synchronisée avec des serveurs de temps Network Time Protocol (NTP).

Des procédures automatiques ou manuelles peuvent être utilisées pour maintenir l'heure du système.

La précision est inférieure à 1 seconde.

6 FORMAT DES DOSSIERS DE PREUVE

6.1 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.

6.2 Format de signature

Le format de signature mis en œuvre dans le cadre de la constitution de l'Archive est le format XAdES-T (signature) puis XAdES-A (conservation).

6.3 Algorithmes cryptographiques

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

6.4 Certificats

6.4.1 Certificats de chiffrement

Paramètre	**Valeur**
AC émettrice	BPCE UCG ACE MATERIELS CAISSE D EPARGNE
DN du certificat	CN = icguce.d3s.chif ou CN = icguce.d3s.sequestre OU = SSLCE OU = 0002 493455042 O = BPCE C = FR
Taille de la clé	RSA 2048
Durée de validité	**1096** (3 ans)
Usage de la clé	Signature numérique (digitalSignature) (critique), Chiffrement de clé (keyEncipherment) (critique)
Usage avancé de la clé	Authentification SSL/TLS client (clientAuth), Authentification SSL/TLS serveur (serverAuth)

6.4.2 Certificat d'horodatage

Le gabarit « Certificat Horodatage » décrit dans la politique de certification de l'AC publiée sous www.dossiers-securite.bpce.fr.

7 AUDITS

Les exigences de ce chapitre sont référencées dans le document suivant : « Mesures communes » publié au même endroit que la présente politique.

8 AUTRES DISPOSITIONS

Se référer au document « Mesures communes ».