Mesures communes, définitions et acronymes applicables aux politiques de l'Infrastructure de Confiance Groupe (ICG)

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

1.1 Présentation générale

Le Groupe BPCE, pour ses Clients des réseaux Caisse d'Epargne, Banque Populaire et Filiales, met en œuvre pour un service de dématérialisation des contrats et des actes de gestion intégrant un processus de Signature électronique.

Le présent document constitue les mesures communes applicables aux documents de politiques de sécurité du Groupe BPCE.

1.2 Identification du document

Le présent document appelé : « Mesures communes, définitions et acronymes applicables aux documents de politiques de sécurité de l'Infrastructure de Confiance Groupe (ICG) » est la propriété du Groupe BPCE.

Il est identifié par un numéro d'identification unique, l'OID : **1.3.6.1.4.1.40559.000.2**

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 les Mesures Communes, on utilisera l'OID accompagné de l'empreinte de ce document et de la mention de l'algorithme utilisé pour produire cette empreinte.

1.3 Publication du document

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

Le présent document est publié 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 sur le site www.dossiers-securite.bpce.fr.

Les demandes d'information ou questions concernant le présent document 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.

2 DÉFINITIONS ET ACRONYMES

2.1 Acronymes

Les acronymes utilisés dans les Politiques des composants de l'Infrastructure de Confiance Groupe sont les suivants :

AC	Autorité de Certification
ADP	Attestation de Preuve
AE	Autorité d'Enregistrement
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AP	Autorité de Gestion des Politiques
API	Application Programming Interface
AS	Autorité de Signature
ASGP	Autorité de Signature et de Gestion de Preuve
CEN	Comité Européen de Normalisation
CERT	Computer Emergency Response Team
CESSIG	Comité Exécutif de la Sécurité des Systèmes d'Information
CISSI	Commission Interministérielle pour la SSI
CC	Critères Communs
CN	Common Name
CSR	Certificate Signing Request
CT	Contact Technique
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
EAL	Evaluation assurance level, norme ISO 15408 (Critères Communs) pour la certification des produits de sécurité
ETSI	European Telecommunications Standards Institute
HTTP	Hypertext Transport Protocol
HSM	Hardware Sécurity Module
ICG	Infrastructure de Confiance Groupe

IGC	Infrastructure de Gestion de Clés
IP	Internet Protocol
ISO	International Organization for Standardization
KC	Key Ceremony
LAR	Liste des certificats d'AC Révoqués
LCP	Lightweight Certificate Policy
LCR	Liste des Certificats Révoqués (ou CRL)
LDAP	Lightweight Directory Access Protocol
MC	Mandataire de Certification
NTP	Network Time Protocole
OCSP	Online Certificate Status Protocol
OF	Opérateur Fonctionnel
OID	Object Identifier
OSC	Opérateur de Service de Certification
OSGP	Opérateur de Service de Gestion des Preuves
OSH	Opérateur de Service d'Horodatage
OT	Opérateur Technique
PA	Politique d'Archivage
PC	Politique de Certification
PSGP	Politique de Signature et de Gestion des Preuves
PH	Politique d'Horodatage
PKCS	Public-Key Cryptography Standard
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Électronique
RFC	Request for comment
RSA	Rivest Shamir Adelman (algorithme cryptographique)
SHA	Secure Hash Algorithm (norme fédérale américaine)
SOC	Security Operation Center
SP	Service de Publication

SNMP Simple Network Management Protocol

SSI Sécurité des Systèmes d'Information

UC Utilisateur de certificat

UH Unité d'Horodatage

URL Uniform Resource Locator

2.2 Définitions

Abonné - Entité ayant besoin de faire horodater des données par une Autorité d'Horodatage et qui a accepté les conditions d'utilisation de ses services. La contremarque de temps est demandée directement à l'AH [ETSI].

Applications utilisatrices – Applications qui appellent les Services de l'ICG.

Attestation de preuve – Document émis et scellé par l'ICG, archivé par les réseaux. Il est conservé par l'Etablissement ou la Filiale et atteste qu'un document donné a bien été signé par le Client.

Audit - Contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures. [ISO/IEC POSIX Security].

Archivage - Désigne l'ensemble des actions, outils et méthodes mis en œuvre pour réunir, identifier, sélectionner, classer et conserver les documents, sur un support sécurisé, dans le but de les exploiter et de les rendre accessibles dans le temps, que ce soit à titre de preuve (notamment en cas d'obligation légale ou de litige) ou à titre informatif.

Authentification – Processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique [EIDAS].

Autorité d'Archivage (AA) - Autorité responsable de la gestion d'un Service d'archivage.

Autorité de Certification (AC) – Une Autorité de Certification a en charge, au sein de l'ICG, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre d'une politique de certification.

L'AC génère des Certificats et révoque des Certificats à partir des demandes que lui envoie l'Autorité d'Enregistrement. L'AC met en œuvre les services de génération de bi-clé d'AC, de génération de Certificats, de révocation de Certificats et de journalisation et d'audit.

Le Groupe BPCE s'appuie sur les capacités de l'Opérateur Technique (OT) afin de mettre en œuvre l'ensemble des opérations cryptographiques nécessaires à la création des Certificats et à la gestion de leur cycle de vie.

L'AC agit conformément à la PC et à la DPC associée. L'AC est identifiée par son Common Name (CN).

L'Autorité de Certification est le Groupe BPCE. Elle est représentée par le Directeur Sécurité Groupe. Elle est assurée en responsabilité par le représentant légal de l'AC lorsque celle-ci est externalisée.

Autorité d'Enregistrement (AE) – L'AE est responsable de la collecte auprès des AED des éléments de traçabilités des dossiers d'enregistrement des porteurs avant de les transmettre vers l'AC.

Autorité d'Enregistrement Déléguée (AED) – L'AED réalise, en délégation de l'AE, les opérations d'identification du client avant de valider la demande de signature électronique. Il y a une AED par réseau distributeur.

Autorité de Gestion des Politiques (AP) – Autorité responsable de la gestion (rédaction, validation, approbation et mise à jour) des politiques de confiance de l'ICG.

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

L'Autorité de Gestion des Politiques (AP) est responsable de la validation des Politiques.

Autorité de Signature et de Gestion des Preuves (ASGP) - Autorité responsable de la gestion d'un service de Signature Electronique et d'un service de gestion des preuves.

Autorité d'Horodatage (AH) – Autorité responsable de la gestion d'un Service d'horodatage.

Cachet électronique - Des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières [EIDAS]. Ces Cachets sont apposés par les Etablissements et Filiales.

Centre Opérationnel de Sécurité – voir Security Operation Center (SOC).

Certificat - Attestation électronique qui associe les données de validation d'une Signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne [EIDAS].

Certificat d'AC - Certificat pour une AC émis par une autre AC. [ISO/IEC 9594-8; ITU-T X.509].

Certificat auto signé - Certificat d'AC signé par la clé privée de cette même AC.

Chemin de certification - (ou chaîne de confiance, ou chaîne de certification) Chaîne constituée de multiples Certificats nécessaires pour valider un Certificat.

Clé privée - Clé de la bi-clé de chiffrement asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

Clé publique - Clé de la bi-clé de chiffrement asymétrique d'une entité qui peut être rendue publique [ISO/IEC 9798-1].

Client – Personne morale ou personne physique signataire d'un document, nécessairement connue d'un Etablissement ou d'une Filiale.

Composante – Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'ICG.

Compromission - Violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de la sécurité de cette clé privée.

Confidentialité - La propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus [ISO/IEC 13335-1:2004].

Conditions Générales d'Utilisation (CGU) - Récapitulatif de l'usage autorisé d'une Signature électronique et des obligations du Client, conformément aux Politiques applicables de l'ICG. Les CGU doivent être connues du Client.

Contremarque de temps - Des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant [EIDAS]. Dans le cadre de la documentation technique de l'ICG, elle peut également prendre de manière indifférente le terme de Jeton d'Horodatage.

Critères Communs - Ensemble d'exigences de sécurité qui sont décrites suivant un formalisme internationalement reconnu [ISO/IEC 15408]. Les produits et logiciels sont évalués par un laboratoire afin de s'assurer qu'ils possèdent des mécanismes qui permettent de mettre en œuvre les exigences de sécurité sélectionnées pour le produit ou le logiciel évalué.

Disponibilité - La propriété d'être accessible sur demande, à une entité autorisée [ISO/IEC 13335-1:2004].

Distance (à) - S'entend de toute procédure de contractualisation, sans la présence physique simultanée d'un représentant d'un Etablissement ou d'une Filiale d'une part et d'un Client d'autre part, par le recours exclusif à une ou plusieurs techniques de communication à distance jusqu'à la signature du document.

Document - ensemble composé d'un contenu, d'une structure logique, d'attributs de présentation permettant sa représentation, exploitable par une machine afin de restituer une version intelligible pour un homme. Il s'agit notamment les contrats et les actes de gestion.

Dossier de preuve - L'ensemble des éléments créés lors de la signature d'un ou plusieurs documents ainsi que l'historique des opérations réalisées, permettant d'assurer la pérennité de la validité dudit (desdits) document(s) signé(s).

Etablissement - Etablissement du réseau Banque Populaire ou du réseau Caisse d'Epargne.

Face à face (en) – S'entend de toute procédure de contractualisation nécessitant la présence physique simultanée d'un représentant d'un Etablissement ou d'une Filiale d'une part et d'un Client d'autre part.

Filiale - Entité majoritairement contrôlée par le Groupe BPCE, au sens de l'article L 233-3 du Code de Commerce.

Identification - Processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale [EIDAS].

Infrastructure de Confiance Groupe (ICG) - Plateforme de sécurité du Groupe BPCE regroupant tous les Composants fournissant les Services d'Authentification, de Signature électronique, d'Horodatage, d'Archivage à vocation probatoire et de Gestion de preuves.

Intégrité - Fait référence à l'exactitude de l'information, de la source de l'information, et au fonctionnement du système qui la traite.

Interopérabilité - Implique que le matériel et les procédures utilisés par deux entités ou plus sont compatibles; et qu'en conséquence il leur est possible d'entreprendre des activités communes ou associées.

Opérateur Fonctionnel (OF) – Le prestataire désigné pour prendre en charge toutes les évolutions applicatives et fonctionnelles conformément aux exigences métier.

Opérateur Technique (OT) – Le prestataire désigné pour exploiter la plateforme de l'ICG. L'OT assure des prestations techniques, en particulier cryptographiques, nécessaires au processus de certification, conformément à la PC et à la DPC. L'OT est techniquement dépositaire des clés privées et des moyens informatiques de l'AC, de l'AE et du SP. Sa responsabilité se limite au respect des procédures, référencées dans la DPC, définies afin de répondre aux exigences de la PC. La DPC précise quelles sont les entités qui sont OT pour les composantes et les opérations de l'Infrastructure de Gestion de Clés.

Opération – Un ou plusieurs Documents signés électroniquement entre le Client et l'Etablissement ou Filiale.

Plan de secours (après sinistre) - Plan défini par le PSCO pour remettre en place tout ou partie de ses services d'Infrastructure de Gestion de Clés après qu'ils aient été endommagés ou détruits à la suite d'un sinistre, ceci dans un délai défini dans l'ensemble PC/DPC.

Politique d'Archivage (PA) – Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une Autorité d'Archivage se conforme dans la mise en place et la fourniture de ses prestations d'archivage.

Politique de Certification (PC) – Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Politique de Signature et Gestion des Preuves (PSGP) – Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AGP se conforme dans la mise en place et la fourniture de ses prestations de Signature Electronique et de Gestion des Preuves.

Politique d'Horodatage (PH) – Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations d'Horodatage.

Politique de sécurité - Ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].

Prestataire de Services de Confiance (PSCO) - Personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de

confiance qualifié ou non qualifié [EIDAS]. Le PSCO comprend tous les acteurs de l'ICG, par exemple OT, OF, Autorités.

Produit de sécurité – Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Prospects – Personne morale ou personne physique signataire d'un Document, non connue d'un Etablissement ou d'une Filiale.

Qualification (procédure de) – Procédure suivie par l'ICG pour mettre à disposition des Etablissements et Filiales du Groupe BPCE des Services d'ICG qualifiés mais aussi pour être qualifié en qualité de PSCO [EIDAS].

Service d'Archivage à vocation probatoire – Ensemble des prestations nécessaires à l'Archivage électronique des documents.

Service d'Authentification - Ensemble des prestations nécessaires à l'Authentification des Clients.

Service d'Horodatage – Ensemble des prestations nécessaires à la génération et à la gestion de Contremarques de temps.

Service de Signature et de Gestion de Preuve – Ensemble des prestations nécessaires à la génération, la validation et la conservation des Signatures Electroniques mais aussi à la Gestion de Preuves.

Services de l'ICG - Ensemble des prestations mises en œuvre par l'ICG et relatives à l'Authentification, à la Signature électronique, à l'Horodatage, à l'Archivage à vocation probatoire et à la Gestion de Preuves.

Signataire – personne physique disposant par la loi ou par convention du pouvoir de signer en son nom ou au nom et pour le compte d'une personne physique ou morale un Document.

Signature électronique - Des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le Client utilise pour signer [EIDAS].

Signature électronique avancée (SEA) – Signature électronique qui :

a) est liée au Client de manière univoque ;

b) permet d'identifier le Client ;

c) a été créée à l'aide de données de création de Signature électronique que le Client peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ;

d) est liée aux données associées à cette Signature de telle sorte que toute modification ultérieure des données soit détectable [EIDAS].

Security Operation Center (SOC) – ou Centre Opérationnel de Sécurité. L'activité principale du SOC consiste à collecter les informations en provenance des éléments de sécurité, de les analyser et d'y détecter les potentielles anomalies. Pour le groupe, le SOC est le point d'entrée pour toute question ou problématique relative à la sécurité de l'activité bancaire.

Unité d'Horodatage (UH) - Ensemble de matériels et de logiciels en charge de la création de Contremarques de temps caractérisé par un identifiant de l'Unité d'Horodatage accordé par une Autorité de Certification (AC), et une clé unique de signature de contremarques de temps.

Validation de certificat électronique - Processus de vérification et de confirmation de la validité d'une Signature ou d'un Cachet électronique [EIDAS].

3 MESURES DE SÉCURITÉ NON TECHNIQUES

Ce chapitre présente un ensemble de mesures non techniques concernant la sécurité de l'infrastructure. Des précisions et des compléments sur la mise en œuvre de ces mesures sont donnés dans la documentation technique du PSCO.

Ces exigences s'appliquent à l'ensemble des acteurs de l'ICG.

3.1 Mesures de sécurité physiques

3.1.1 Situation géographique et construction des sites

La construction des sites respecte les règlements et normes en vigueur.

La localisation géographique des sites ne présente pas de risque concernant les tremblements de terre, les explosions ou les inondations.

Le site d'exploitation est protégé par des systèmes de détection d'intrusion, de caméra, de gardiennage permettant la protection contre les accès non autorisés aux équipements.

Les équipements de l'OT doivent toujours être protégés contre tout accès non autorisé. Les exigences relatives aux équipements sont les suivantes :

- S'assurer qu'aucun accès non autorisé au matériel ne soit autorisé.
- S'assurer que tous les supports amovibles et documents papier contenant des informations sensibles en texte brut sont stockés de manière sûre.
- S'assurer de l'existence d'une surveillance permanente via vidéo et gardiennage pour protéger les locaux contre les risques d'intrusions.
- S'assurer que les ressources cryptographiques et les composantes de l'AC sont accessibles uniquement sous double contrôle.
- Assurer qu'un journal des accès est entretenu et inspecté régulièrement.
- Fournir plusieurs niveaux de renforcement pour la sécurité périmétrique des accès physique.
- Assurer que seules les personnes physiques autorisées ont accès aux composantes de l'Infrastructure de Confiance Groupe.
- Assurer la désactivation des modules cryptographiques avant leur stockage.
- Assurer que les données d'activation utilisées pour accéder aux modules cryptographiques sont placées dans des coffres.
- Assurer que les données d'activation sont soit mémorisées soit enregistrées et stockées de manière compatible avec la sécurité offerte par le module cryptographique.

- Assurer que les données d'activation non nécessaire au fonctionnement quotidien de la ressource cryptographique « en ligne » ne sont pas stockées avec le module cryptographique associé.

Une personne ou un groupe de personnes doit être explicitement chargé d'effectuer ces contrôles.

3.1.2 Accès physique

L'accès physique aux fonctions sensibles de l'infrastructure est strictement limité aux seules personnes nominativement autorisées.

L'accès physique aux composantes supportant ces fonctions est limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique, permettant la séparation des rôles entre les différents intervenants.

La traçabilité des accès est assurée.

Des mesures de détection d'intrusion physique sont mises en œuvre, notamment via l'utilisation de caméras.

Des mesures de sécurité physique sont également mises en place pour limiter les accès aux supports sensibles (DPC, documents d'applications).

3.1.3 Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre par l'opérateur de manière à ce qu'une interruption de service d'alimentation électrique, ou une défaillance de climatisation ne portent pas atteinte aux engagements pris par l'OT en matière de disponibilité pour l'ensemble des fonctions sensibles de son infrastructure.

3.1.4 Vulnérabilité aux dégâts des eaux

La définition du périmètre de sécurité prend en considération les risques inhérents aux dégâts des eaux. Des moyens de protection sont mis en œuvre pour parer les risques résiduels (rupture de canalisation par exemple).

3.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre l'incendie permettent de respecter les engagements pris par l'OT en matière de disponibilité, et de pérennité de l'archivage pour l'ensemble des fonctions sensibles de son infrastructure.

3.1.6 Conservation des supports

Les moyens de conservation des supports permettent de respecter les engagements pris par l'OT en matière de restitution et de pérennité de l'archivage.

3.1.7 Mise hors service des supports

Les supports recensés comme sensibles en termes de confidentialité font l'objet de mesures de destruction, ou peuvent être réutilisés dans un contexte opérationnel identique à un même niveau de sensibilité.

3.1.8 Sauvegardes hors site

Afin de permettre une reprise après incident conforme aux engagements pris par l'AP, l'Opérateur Technique met en place 2 sites redondés permettant dans cette forme de garantir la reprise.

3.2 Mesures de sécurité procédurales

3.2.1 Rôles de confiance

Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

Les principaux rôles de confiance de l'ICG sont :

- Les personnels de l'OT, dont la responsabilité est d'exploiter les Services de l'Infrastructure de Confiance Groupe et de les maintenir en conditions opérationnelles de fonctionnement.
- Les personnels de l'OF, dont la responsabilité est d'administrer fonctionnellement les Services de l'Infrastructure de Confiance Groupe.
- Les personnels de « sécurité », dont la responsabilité est de définir et de réaliser les opérations de vérification de la bonne application des mesures et de la cohérence de fonctionnement de l'Infrastructure de Confiance Groupe.

3.2.2 Nombre de personnes requises par tâches

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

3.2.3 Identification et authentification pour chaque rôle

Le PSCO fait vérifier l'identité et les autorisations de tout membre de son personnel amené à définir et mettre en œuvre les Services de l'Infrastructure de Confiance Groupe avant de lui attribuer un rôle et les droits correspondants. L'attribution des accès et des rôles techniques donne lieu systématiquement à un enregistrement. Les accès sont nominatifs et permettent ainsi d'imputer les actions à une personne.

Les contrôles sont décrits dans la documentation technique et sont conformes à la politique de sécurité du PSCO. Chaque attribution d'un rôle à un membre du personnel de l'Infrastructure de Confiance Groupe lui est notifiée par écrit ou équivalent.

3.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous encadrant le cumul soient respectées :

- Les rôles Sécurité et Auditeur ne peuvent pas être cumulés avec administration et exploitation ;

- Le rôle Témoin peut être cumulé avec seulement Auditeur et détenteur de secret.

3.3 Mesures de sécurité vis-à-vis du personnel

3.3.1 Qualifications, compétences et habilitations requises

Chaque personne amenée à travailler au sein de l'Infrastructure de Confiance Groupe est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles.

Toute personne intervenant dans les procédures de l'Infrastructure de Confiance Groupe est informée de ses responsabilités relatives aux services de l'Infrastructure de Confiance Groupe et des procédures liées à la sécurité du système et au contrôle du personnel.

3.3.2 Procédures de vérification des antécédents

L'Infrastructure de Confiance Groupe met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification est basée sur un contrôle des antécédents de la personne, il est vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions.

Le choix des personnes pour exercer un rôle de confiance ne doit pas créer une situation de conflits d'intérêts susceptible de porter préjudice à l'impartialité de ces dernières.

3.3.3 Exigences en matière de formation initiale

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité, correspondants à la composante au sein de laquelle il opère.

Le personnel a eu connaissance et compris les implications des opérations dont il a la responsabilité.

3.3.4 Exigences et fréquence en matière de formation continue

En fonction de la nature des évolutions apportées, le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc.

3.3.5 Fréquence et séquence de rotation entre différentes attributions

Dès qu'une personne change de rôle de confiance, ses comptes dans l'Infrastructure de Confiance Groupe sont réinitialisés afin de ne pas porter atteinte à la sécurité du non cumul des rôles.

3.3.6 Sanctions en cas d'actions non autorisées

Les procédures internes de l'OT précisent ou font référence aux sanctions prévues en cas d'actions non autorisées. Elles sont communiquées au personnel avant la prise de fonction.

3.3.7 Exigences vis-à-vis du personnel des prestataires externes

Les exigences du paragraphe 2.3 sont applicables aux prestataires externes. Ces exigences sont explicitées dans les contrats avec les prestataires.

3.3.8 Documentation fournie au personnel

Le personnel a accès à la documentation concernant les procédures et les systèmes techniques qui le concernent dans le cadre de ses fonctions. Notamment il a accès à la politique de sécurité correspondante.

3.4 Procédures de constitution des données d'audit

La journalisation d'événements consiste à enregistrer les évènements manuellement ou électroniquement par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier et/ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.

3.4.1 Type d'événements à enregistrer

L'Infrastructure de Confiance Groupe journalise les évènements concernant les systèmes liés aux fonctions qu'elles mettent en œuvre dans le cadre de l'Infrastructure de Confiance Groupe :

- Création / modification / suppression de comptes utilisateur (droits d'accès)
- Selon le type de l'évènement concerné, les champs suivants peuvent être enregistrés :
  - Destinataire de l'opération.
  - Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande.
  - Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes).
  - Cause de l'évènement.
  - Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

3.4.2 Fréquence de traitement des journaux d'événements

Les opérations de journalisation sont effectuées au cours du processus considéré. En cas de saisie manuelle, l'écriture se fera, sauf exception, le même jour ouvré que l'évènement.

3.4.3 Période de conservation des journaux d'événements

Les journaux d'évènements sont conservés sur site pendant au moins 1 an.

Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous 15 jours (recouvrement possible entre la période de conservation sur site et la période

d'archivage). L'auditeur a la responsabilité des données d'audit qu'il consulte ou génère lors de toutes les phases de son travail (collecte, diffusion et archivage).

3.4.4 Procédures de sauvegarde des journaux d'événements

L'OT met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences des présents documents.

3.4.5 Système de collecte des journaux d'événements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non) et datés de manière fiable sur la base d'une même source de temps pour permettre le rapprochement des journaux entre les différentes composantes concernées. Les journaux sont conservés y compris une fois mis sur le site de secours.

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

Les journaux ne sont accessibles que par les personnes autorisées.

3.4.6 Evaluation des vulnérabilités

L'OT est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée. Les journaux d'évènements sont analysés suite à la détection d'une anomalie. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

3.5 Archivage des journaux

L'archivage des journaux permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'Infrastructure de Confiance Groupe.

3.5.1 Type de données à archiver

Les données archivées au niveau de chaque composante, sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques.
- Les politiques et déclarations adaptées
- Les Services de confiance objets de la composante
- Les Journaux d'évènements

3.5.2 Période de conservation des archives

Les données archivées sont conservées au minimum 10 ans.

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes :

- Seront protégées en intégrité.
- seront accessibles aux seules personnes autorisées.
- pourront être consultées et exploitées.

3.5.3 Exigences d'Horodatage des données

Si un service d'Horodatage est utilisé pour dater les enregistrements, il répond aux exigences répond aux exigences techniques de la norme 319421.

3.5.4 Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données.

3.5.5 Procédures de récupération et de vérification des archives

Les sauvegardes électroniques archivées sont récupérables dans les meilleurs délais.

4 AUDITS

Ce paragraphe concerne les audits commandités en interne afin de vérifier la conformité de l'implémentation au regard des différentes Politiques mises en œuvre au sein de l'ICG, et ce processus s'inscrit également dans une démarche de contrôle permanent.

4.1 Fréquences et circonstances des audits

L'Infrastructure fait l'objet d'audit périodique de conformité au moins une fois par an et permet de vérifier le respect des exigences des politiques.

A ce titre, des audits appelés « audit interne » quand ils sont réalisés par l'AP et « audit externe » quand ils sont réalisés par un auditeur externe sont réalisés de manière régulière.

Des contrôles peuvent également être déclenchés sur décision de l'AP.

4.2 Identité et qualifications des auditeurs

Les auditeurs démontrent leurs compétences dans le domaine des audits de conformité et doivent être familiers avec les exigences des politiques. L'AP apporte une attention particulière quant à l'audit de conformité, notamment vis-à-vis de ses exigences en matière d'audit. L'AP effectue elle-même le choix des auditeurs.

4.3 Relations entre auditeurs et entités auditées

Les auditeurs en charge de l'audit de conformité sont soit une entreprise privée indépendante du Groupe BPCE, soit une entité du Groupe BPCE suffisamment indépendante afin d'effectuer une évaluation juste et indépendante.

L'AP détermine si un auditeur remplit cette condition.

4.4 Sujets couverts par les audits

Les audits et les contrôles de conformité portent sur une composante de l'infrastructure (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'ICG (contrôles périodiques).

Ils visent à vérifier le respect des engagements et pratiques définies dans les Politiques et dans les autres documents (Politiques de Sécurité, procédures opérationnelles) cités.

Le sujet et le périmètre de l'évaluation seront préalablement définis dans un protocole d'audit qui sera validé par le Comité Sécurité Groupe.

4.5 Actions prises suite aux conclusions des audits

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'Autorité, un avis parmi les suivants : « réussite », « échec », « à confirmer ».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'Autorité qui peuvent être :
    - La cessation (temporaire ou définitive) d'activité.

- L'invalidation de tout ou partie des données déjà établies.

Le choix de la mesure à appliquer est effectué par l'Autorité et doit respecter ses politiques de sécurité interne :

- En cas de résultat « à confirmer », l'Autorité remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées.

- Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.

- En cas de réussite, l'Autorité confirme à la composante contrôlée la conformité aux exigences de la Politique visée.

5 GOUVERNANCE

Le comité de validation des Politiques détermine la conformité des documents techniques en fonction du cadre réglementaire, technique et organisationnel de l'ICG.

Le comité de validation des Politiques est intégré dans le Comité exécutif Sécurité des Systèmes d'Information du Groupe BPCE [CESSIG].

5.1 Composition du comité de validation des Politiques

Le comité de validation des Politiques est présidé par un membre du comité de direction générale.

Il est composé du directeur Conformité, Sécurité et Risques Opérationnels, des principaux RSSI et des responsables des principaux opérateurs informatiques du Groupe, dont l'Opérateur Fonctionnel et l'Opérateur Technique.

5.2 Fréquence des comités de validation des Politiques

Le comité de validation des Politiques se réunit en cas de besoin d'approbation d'une ou plusieurs Politiques, et avant leur publication.

La validation des Politiques est inscrite à l'ordre du jour du [CESSIG], préalablement au comité, sur demande de l'Opérateur Fonctionnel.

5.3 Attributs du comité de validation des Politiques

Le [CESSIG] décide et suit les projets et plans d'actions SSI majeurs du Groupe, et s'assure d'une mise en œuvre opérationnelle homogène entre les opérateurs.

Dans ce cadre, le comité de validation des Politiques approuve les évolutions et modifications majeures apportées aux Politiques, ainsi que leur cohérence vis-à-vis du référentiel documentaire, du cadre réglementaire et technique ainsi que de l'organisation de l'ICG.

6 AUTRES DISPOSITIONS

6.1 Tarification

Non applicable.

6.2 Responsabilité financière

Le Groupe BPCE assume en fonds propres le règlement des litiges éventuels liés au service d'archivage.

L'AA dispose de ressources financières suffisantes à son bon fonctionnement et à l'accomplissement de sa mission de service d'archivage.

En cas de dommage subi par une entité utilisatrice du fait d'un manquement par le service d'Archivage, l'AA pourra être amenée à dédommager l'entité utilisatrice dans la limite de sa responsabilité définie dans les conditions générales d'utilisation.

6.3 Confidentialité des données à caractère personnel

Dans le cadre du service de dématérialisation des contrats et des actes de gestion intégrant un processus de Signature électronique, et plus généralement de la relation Clients, les établissements des réseaux Caisses d'Epargne, Banques Populaires et Filiales recueillent et traitent des données à caractère personnel concernant les Clients et Signataires.

Les informations expliquant pourquoi et comment ces données sont utilisées, combien de temps elles sont conservées, ainsi que les droits dont disposent les personnes sur leurs données figurent dans la Notice d'information sur le traitement des données à caractère personnel de l'établissement concerné.

Cette notice est portée à la connaissance de la personne lors de la première collecte de ses données. Elle est accessible à tout moment sur le site internet de l'établissement. Il est également possible d'en obtenir un exemplaire auprès de l'agence bancaire concernée.

Pour les Caisses d'Epargne : www.caisse-epargne.fr/protection-donnees-personnelles.

Pour les Banques Populaires : www.banque-populaire.fr > Accueil > Mentions légales > Réglementation > Protection des données personnelles.

Pour les autres Filiales : site internet de la filiale, rubrique protection des données personnelles.

6.4 Droit applicable

Les dispositions de la politique d'archivage sont régies par le droit français.

6.5 Tribunaux compétents

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique, et faute d'être parvenues à un accord amiable ou à une transaction, les parties donnent compétence expresse et exclusive aux tribunaux compétents de Paris, nonobstant pluralité de défendeurs ou d'action en référé ou d'appel en garantie ou de mesure conservatoire.