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

Mentions Légales

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 207 603 030 €.

Siège social : 7, promenade Germaine Sablon 75013 PARIS

RCS Paris n° 493 455 042.

Version du document	1.6	Nombre de pages	29
Statut du document	☐Projet	☒Version finale	

Historique du document

Date	Version	Commentaire
25/04/2013	1.0	
01/10/2014	1.1	
01/01/2019	1.2	
01/09/2021	1.3	
01/03/2022	1.4	
07/02/2023	1.4	
25/07/2023	1.4	
09/08/2024	1.4	Ajout d'un cartouche d'historique des versions Changement du montant de capital dans les mentions légales
06/12/2024	1.5	Modification de la notion Client – Utilisateur
03/02/2025	1.6	Changement de nom de l'Infrastructure
21/02/2025	1.6	Changement du montant de capital social
16/04/2025	1.6	Modification du paragraphe rôles de confiance

SOMMAIRE

1 INTRODUCTION

1.1 Présentation générale

Le Groupe BPCE met en œuvre un service de signature électronique de documents pour :

- ses réseaux Banque Populaire et Caisse d'Epargne ;
- ses Filiales Bancaires ;
- ses Filiales Métiers ;
- ses partenaires .

Il met aussi en œuvre les règles applicables à l'établissement et à la conservation des dossiers de preuves liés aux opérations de signature électronique.

Le service de signature peut être utilisé à distance ou dans une agence du réseau.

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 Signature Groupe (ISG)*, est la propriété du Groupe BPCE.

Il est identifié par un numéro d'identification unique, l'OID : **1.3.6.1.4.1.40559.000.4**

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 des documents

Les Autorités (AC, AH) délivrant les Services de l'ISG doivent mettre à la disposition des Utilisateurs [USSE] un certain nombre de documents (politiques, dont le présent document) et d'informations (certificats, CRL, etc.).

1.3.1 Entité gérant les documents

Les documents sont sous la responsabilité de l'AP.

1.3.2 Point de contact

Les demandes d'informations ou questions concernant l'Autorité de Certification sont adressées à :

Groupe BPCE

Responsable de la Sécurité des Systèmes d'informations Groupe

7, promenade Germaine Sablon 75013 PARIS

rssi-pssi-ICG@bpce.fr

Ce point de contact est disponible et à jour sur le site du SP.

1.3.3 Entité déterminant la conformité des documents avant publication

L'AP détermine la conformité des documents avant leur publication.

1.3.4 Procédure d'approbation de la conformité

L'AP possède ses propres méthodes pour approuver le présent document. L'AP procède à des analyses/contrôles de conformité et/ou des audits qui aboutissent à l'autorisation ou non pour l'AC/AH de fournir son service. L'AP approuve les résultats de la revue de conformité effectuée par les experts qu'elle nomme à cet effet.

1.4 Entrée en vigueur

Le présent document est publié au plus tard le 16/02/2026.

Le présent document entre en vigueur le 17/02/2026.

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*

CERTIC² Comité Exécutif des Risques Technologie de l'Information, Communication et Cyber

CISSI Commission Interministérielle pour la SSI

CC Critères Communs

CN *Common Name*

CRL *Certificates Revocation List*

CSR *Certificate Signing Request*

CT Contact Technique

DN *Distinguished Nam*e

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 Security Module*

ISG	Infrastructure de Signature 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
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

USSE Utilisateur du Service de Signature Electronique

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'ISG.

Attestation de preuve – Document émis et scellé par l'ISG, archivé par les réseaux. Il est conservé par l'Établissement ou la Filiale et atteste qu'un document donné a bien été signé par l'Utilisateur [USSE] .

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'ISG, 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)*.

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 de l'Utilisateur [USSE] 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'ISG (PA, PH, PE, en cohérence avec la PC/DPC de l'Autorité de Certification externalisée).

Le [CERTIC²] est 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 Électronique 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 Établissements 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].

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'ISG.

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 de l'Utilisateur [USSE], conformément aux Politiques applicables de l'ISG. Les CGU doivent être connues de l'Utilisateur [USSE].

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'ISG, 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 d'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 13335-1:02004].

Distance (à) - S'entend de toute procédure de contractualisation, sans la présence physique simultanée d'un représentant d'un Établissement ou d'une Filiale d'une part et d'un Utilisateur [USSE] 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).

Établissement - Établissement du réseau Banque Populaire ou du réseau Caisse d'Épargne et filiales du Groupe BPCE.

Face à face (en) – S'entend de toute procédure de contractualisation nécessitant la présence physique simultanée d'un représentant d'un Établissement ou d'une Filiale d'une part et d'un Utilisateur [USSE] 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 Signature Groupe (ISG) – 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'ISG. 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 l'Utilisateur [USSE] et l'Établissement 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 Électronique 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'ISG, par exemple OT, OF, Autorités.

Prestataire de Vérification d'Identité à Distance – Personne morale spécialisée dans la vérification d'identité en ligne des personnes physiques, certifié par l'ANSSI selon les critères du référentiel PVID.

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 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 Établissement ou d'une Filiale.

Qualification (procédure de) – Procédure suivie par l'ISG pour mettre à disposition des Établissements et Filiales du Groupe BPCE des Services d'ISG 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 Utilisateurs [USSE].

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

Service de publication (SP) – Le SP est en charge de la publication des données devant être publiées par le PSCO et du maintien du site de publication (voir section 3).

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

Services de l'ISG - Ensemble des prestations mises en œuvre par l'ISG 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 à l'Utilisateur [USSE] de manière univoque ;

b) permet d'identifier l'Utilisateur [USSE] ;

c) a été créée à l'aide de données de création de Signature électronique que l'Utilisateur [USSE] 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.

Utilisateur [USSE] – Utilisateur du Service de Signature Electronique. Personne physique (Utilisateur particulier) ou personne physique représentant une personne morale (Utilisateur professionnel) à qui il est délivré un certificat électronique de signature.

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

3 RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES

3.1 Entités chargées de la mise à disposition des informations

Le Service de Publication (SP) est en charge de la publication des données sur le site https://www.dossiers-securite.bpce.fr.

3.2 Informations devant être publiées

Les informations suivantes sont publiées sur le site https://www.dossiers-securite.bpce.fr :

- Les PC/DPC des AC ;
- Les certificats de la chaîne de confiance des AC ;
- La politique d'horodatage de BPCE ;
- Les conditions générales d'utilisation des services de confiance ;
- Les listes des autorités révoqués (LAR) ;
- Les listes des certificats révoqués (LCR).

3.3 Délais et fréquences de publication

Le site de publication est disponible 24h/24 et 7j/7 et son contenu mis à jour selon les besoins. Ces éléments sont publiés avant toute génération d'un certificat final correspondant, et toute version validée (déclarée conforme, cf. 1.3.3) d'un document (PC/DPC, PH/DPH, CGU) est publiée sans délai par le SP.

Les LCR sont disponibles 24h/24 et 7j/7, mises à jour toutes les 24 heures et après chaque révocation.

Les LAR sont disponibles 24h/24 et 7j/7, mises à jour annuellement et après chaque révocation.

3.4 Contrôle d'accès aux informations publiées

Le SP s'assure que les informations sont disponibles et protégées en intégrité contre les modifications non autorisées.

L'ensemble des informations publiques et publiées est libre d'accès en lecture et téléchargement sur Internet.

4 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'ISG.

4.1 Analyse de risques

Des analyses de risques sont réalisées pour déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble des services, ainsi que les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre.

Le Groupe BPCE réalise, sur le périmètre des services de confiance, des analyses de risques afin d'identifier, analyser et évaluer les risques portant sur les services de confiance. Ces analyses de risques prennent en compte les risques techniques, mais également les risques commerciaux et métiers.

En fonction des résultats de l'analyse de risques, Le Groupe BPCE sélectionne des mesures appropriées de traitement du risque. Ces mesures de traitement sont mises en place afin d'atteindre un niveau de sécurité proportionné par rapport au risque encouru.

Le Groupe BPCE détermine les exigences de sécurité et les procédures opérationnelles nécessaires pour mettre en place l'ensemble des mesures de traitement du risque sélectionnées. Ces exigences et procédures sont décrites dans le présent document, dans les PSSI, ainsi que dans les politiques et déclarations des pratiques de chacun des services de confiance.

L'analyse de risques est revue chaque année et après chaque modification majeure du SI.

Le comité de sécurité du Groupe BPCE approuve l'analyse des risques et accepte les risques résiduels identifiés. De plus, cette acceptation des risques est à nouveau formalisée à travers la procédure d'homologation de chacun des services qualifiés.

4.2 Mesures de sécurité physique

4.2.1 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.

4.2.2 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).

4.2.3 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.

4.2.4 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).

4.2.5 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.

4.2.6 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.

4.2.7 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.

4.2.8 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.

4.3 Mesures de sécurité procédurales

4.3.1 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'ISG sont :

- Le Responsable de Sécurité des Systèmes d'information, qui a la charge de la mise en place des procédures de sécurité applicables de l'OT et de la vérification de la bonne application de ces procédures ;
- Les Administrateurs, dont la responsabilité est de s'assurer du bon fonctionnement et de la sécurité des systèmes qui composent l'IGC dans le respect des procédures en vigueur ;
- Les Exploitants de l'IGC, dont la responsabilité est le du maintien en conditions opérationnelles des composants de l'IGC qui génèrent les certificats d'AC et les certificats clients ;

- Les Responsables du Contrôle de l'Infrastructure, dont la responsabilité est l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission ;

- Les Opérateurs d'AE, dont la responsabilité est de vérifier et d'accepter les demandes de Certificats Cachet ;

- Les Exploitants HSM, dont la responsabilité est de réaliser les opérations techniques sur les modules cryptographiques de l'IGC. ;

- Le Responsable Certifications, qui organise la mise et le maintien en conformité des composantes de l'IGC par rapport aux exigences de standards ou de référentiels.

4.3.2 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.

4.3.3 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.

4.3.4 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.

4.4 Mesures de sécurité vis-à-vis du personnel

4.4.1 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.

4.4.2 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.

4.4.3 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.

4.4.4 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.

4.4.5 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.

4.4.6 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.

4.4.7 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.

4.4.8 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.

4.5 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.

4.5.1 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).

4.5.2 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.

4.5.3 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).

4.5.4 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.

4.5.5 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.

4.5.6 Évaluation 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.

4.6 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.

4.6.1 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.

4.6.2 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 :

- Sont protégées en intégrité ;
- Sont accessibles aux seules personnes autorisées ;
- Peuvent être consultées et exploitées.

4.6.3 Exigences d'Horodatage des données

Si un service d'Horodatage est utilisé pour dater les enregistrements, il répond aux exigences techniques du standard ETSI EN 319421.

4.6.4 Système de collecte des archives

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

4.6.5 Procédures de récupération et de vérification des archives

Les sauvegardes électroniques archivées sont récupérables dans les meilleurs délais.

5 MESURES DE SÉCURITÉ TECHNIQUES

5.1 Mesures de sécurité des systèmes informatiques

5.1.1 Exigences de sécurité techniques spécifiques aux systèmes informatiques

Les fonctions suivantes sont fournies par le système d'exploitation, ou par une combinaison du système d'exploitation, de logiciels et de protection physiques. Un composant d'une Infrastructure de Gestion de Clés comprend les fonctions suivantes :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs) ;
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, 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 ;
- Fonctions d'audits (non repudiation et nature des actions effectuées).

Quand un composant d'Infrastructure de Gestion de Clés est hébergé sur une plateforme évaluée au regard d'exigences d'assurance de sécurité, il est utilisé dans sa version certifiée. Au minimum le composant utilise la même version de système d'exploitation que celle sur lequel le composant a été certifié. Les composants d'Infrastructure de Gestion de Clés sont configurés de manière à limiter les comptes et services aux seuls éléments nécessaires pour supporter les services d'AC.

5.1.2 Niveau de qualification des systèmes informatiques

Aucune exigence.

5.2 Mesures de sécurité des systèmes durant leur cycle de vie

5.2.1 Mesures de sécurité liées aux développements 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 ;
- Les matériels et logiciels sont dédiés aux activités d'Infrastructure de Gestion de Clés. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités d'Infrastructure de Gestion de Clés ;
- Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de l'Infrastructure de Gestion de Clés. Seules les applications nécessaires à l'exécution des activités Infrastructure de Gestion de Clés sont acquises auprès de sources autorisées par politique applicable de l'AC. Les matériels et logiciels de l'AC 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.

5.2.2 Mesures liées à la gestion de la sécurité

La configuration du système d'Infrastructure de Gestion de Clés, ainsi que toute modification ou évolution, est documentée et contrôlée par l'AP. Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration de l'Infrastructure de Gestion de Clés. Une méthode de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'Infrastructure de Gestion de Clés. Lors de son premier chargement, on vérifie que le logiciel de l'Infrastructure de Gestion de Clés est 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.

La configuration du logiciel de PKI et des différentes composantes (pares-feux, routeurs) est revue au minimum annuellement.

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

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

5.3 Mesures de sécurité réseau

L'AC est en ligne accessible par des postes informatiques sous contrôle et uniquement d'un réseau interne à l'OT. L'AC n'est pas hébergé sur le même réseau que l'AE et le SP. Le principe de défense en profondeur est appliqué.

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

Les autres composantes de l'Infrastructure de Gestion de Clés comme l'AE et le SP 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 réseaux non utilisés sont coupés. Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système Infrastructure de Gestion de Clés est hébergé refuse tout service, hormis ceux qui sont nécessaires au système Infrastructure de Gestion de Clés, 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 assurer la confidentialité et l'intégrité des données qui y transitent.

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

5.4 Horodatage / Système de datation

Tous les composants de l'AC sont régulièrement synchronisés avec un serveur *Network Time Protocol* (NTP) relié à une source de temps publique. Le temps fourni par ce serveur de temps est utilisé pour établir l'heure :

- Du début de validité d'un Certificat d'Utilisateur [USSE] ;
- De la révocation d'un Certificat d'Utilisateur [USSE] ;
- De l'affichage de mises à jour de LCR.

6 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'ISG, et ce processus s'inscrit également dans une démarche de contrôle permanent.

6.1 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.

À 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.

6.2 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.

6.3 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.

6.4 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'ISG (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.

6.5 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

6.6 Communication des résultats

Un Rapport de Contrôle de Conformité, incluant le cas échéant la mention des mesures correctives déjà prises ou en cours par la composante, est remis à l'AP.

Le cas échéant, les rapports sont tenus à disposition des auditeurs externes et de l'ANSSI.

7 GOUVERNANCE

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

Le comité de validation des Politiques est intégré dans le Comité exécutif Sécurité des Systèmes d'Information du Groupe BPCE [CERTIC²].

7.1 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.

7.2 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 [CERTIC²], préalablement au comité, sur demande de l'Opérateur Fonctionnel.

7.3 Attributs du comité de validation des Politiques

Le [CERTIC²] 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'ISG.

8 AUTRES DISPOSITIONS

Les pratiques des services de l'ISG sont non-discriminatoires.

8.1 Tarification

Non applicable.

8.2 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.

8.3 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, les établissements des réseaux Caisses d'Épargne, Banques Populaires et Filiales recueillent et traitent des données à caractère personnel concernant les l'Utilisateurs [USSE] .

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'Épargne : La Caisse d'Epargne & vos données personnelles | Caisse d'Epargne

Pour les Banques Populaires : Banque Populaire & vos données personnelles | Banque Populaire

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

8.4 Droit applicable

Les dispositions politiques des Services de l'ISG sont régies par le droit français.

8.5 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.

8.6 Durée et fin anticipée de validité des politiques

8.6.1 Durée de validité

Les politiques des Services de l'ISG deviennent effectives une fois approuvées par l'AP. Elles restent en application au moins jusqu'à la fin de vie des derniers éléments (certificat, jeton d'horodatage) émis au titre de la politique concernée.

8.6.2 Fin anticipée de validité

Selon l'importance des modifications apportées à une politique, l'AP décidera, soit de faire procéder à un audit des Autorités concernées, soit de donner instruction à l'Autorité de prendre les mesures nécessaires pour se rendre conforme dans un délai fixé.

8.6.3 Effets de la fin de validité et clauses restant applicables

La fin de validité d'une politique entraîne la cessation de toutes les obligations et responsabilités de l'Autorité pour les éléments (certificat, jeton d'horodatage) émis au titre de la politique concernée.

8.7 Amendements aux politiques

8.7.1 Procédures d'amendements

L'AP révise les politiques au moins une fois par an. D'autres révisions peuvent être décidées à tout moment à la discrétion de l'AP. Les corrections de fautes d'orthographe ou de frappe qui n'en modifient pas le sens, ainsi que les changements de montant de capital social de BPCE, sont autorisés sans avoir à être notifiés.

8.7.2 Mécanisme et période d'information sur les amendements

L'AP donne un préavis d'un (1) mois au moins aux composantes et à l'OT de son intention de modifier une politique avant de procéder aux changements et en fonction de l'objet de la modification. Ce délai ne vaut que pour des modifications qui porteraient sur le fond (changement de taille de clé, changement de procédure, changement de profil de certificat, …) et non sur la forme.

8.7.3 Circonstances selon lesquelles l'OID est changé

Si l'AP estime qu'une modification de la politique modifie le niveau de confiance assuré par les exigences ou par le contenu de la politique, elle peut instituer une nouvelle politique avec un nouvel identifiant d'objet (OID).