Mesures communes, définitions et acronymes applicables aux politiques de sécurité 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 3
1.1 PRESENTATION GENERALE 3
1.2 IDENTIFICATION DU DOCUMENT 3
1.3 PUBLICATION DU DOCUMENT 3
2 DEFINITIONS ET ACRONYMES 4
2.1 ACRONYMES 4
2.2 DEFINITIONS 6
3 MESURES DE SÉCURITÉ NON TECHNIQUES 12
3.1 MESURES DE SECURITE PHYSIQUES 12
3.2 MESURES DE SECURITE PROCEDURALES 14
3.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL 15
3.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT 16
3.5 ARCHIVAGE DES DONNEES 19
3.6 CHANGEMENT DE CLE D'AC 20
3.7 REPRISE SUITE A COMPROMISSION ET SINISTRE 21
3.8 FIN DE VIE D'INFRASTRUCTURE DE GESTION DE CLES 22
4 AUDITS 25
4.1 FREQUENCES ET CIRCONSTANCES DES AUDITS 25
4.2 IDENTITE ET QUALIFICATIONS DES AUDITEURS 25
4.3 RELATIONS ENTRE AUDITEURS ET ENTITES AUDITEES 25
4.4 SUJETS COUVERTS PAR LES AUDITS 25
4.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES AUDITS 25

1 INTRODUCTION

1.1 Présentation générale

Le Groupe BPCE, pour ses réseaux Caisse d'Epargne, Banque Populaire et Filiales, met en œuvre pour ses Clients 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 appelée : « 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.

Elle est identifiée par un numéro d'identification unique, l'OID : **1.3.6.1.4.1.40559.000.1**

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

1.3 Publication du document

Avant toute publication officielle, le document est validé par le comité de suivi des Autorités.

Le présent document est publié sur l'URL :http://www.dossiers-securite.bpce.fr/docs/pc-ucg/Mesures_communes_octobre2014.pdf.

L'ensemble des informations associées notamment les versions antérieures de ces documents avec leur période de validité, sont également publiées sur le site http://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
- Directeur de la Sécurité des Systèmes d'informations Groupe
- 50 Avenue Pierre Mendes France
- 75201 Paris Cedex 13
- rssi-pssi-icg@bpce.fr

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

CEN Comité Européen de Normalisation

CISSI Commission Interministérielle pour la SSI

CC Critères Communs

CN Common Name

CSR Certificate Signing Request

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
LDAP	Lightweight Directory Access Protocol
MC	Mandataire de Certification
NTP	Network Time Protocole
OCSP	Online Certificate Status Protocol
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
PGP	Politique 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
SHA	Secure Hash Algorithm (norme fédérale américaine)
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

Agent – Personne physique agissant pour le compte d'une autorité administrative.

Applications utilisatrices – Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins de signature du porteur du certificat. Dans le cadre de la présente Autorité de Certification, il s'agit des applications de dématérialisation des contrats

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].

Autorités administratives – Ce terme générique désigne les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité d'Archivage - Autorité responsable de la gestion d'un service d'archivage.

Autorité de Certification (AC) – Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, 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 de cette politique de certification. Dans le cadre de la PC Type, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre I.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier ou certifier la famille de certificats correspondante.

Autorité d'enregistrement – Ce terme générique désigne les entités en charge d'enregistrer les informations clients ou entreprise afin de répertorier les éléments nécessaires à la constitution d'un certificat et sa gestion.

Autorité de Gestion des Preuves (AGP) - Autorité responsable de la gestion d'un service de gestion des preuves.

Autorité d'Horodatage – Autorité responsable de la gestion d'un service d'horodatage.

Autorité de Signature – Autorité responsable de la gestion d'un service de signature.

Certificat : clé publique d'une entité, ainsi que d'autres informations, rendues impossibles à contrefaire grâce au chiffrement par la clé privée de l'autorité de certification qui l'a émis [ISO/IEC 9594-8; ITU-T X.509].

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 du Contrat. Il s'agit nécessairement d'une personne ou d'une entité connue du réseau de la banque

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'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

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'un certificat et des obligations du Porteur, conformément à la Politique de Certification de l'AC. Les CGU doivent être connues du Clients. Elles sont intégrées dans le processus de signature électronique de contrat et sont une étape obligatoire pour la complétude du processus.

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.

CSR (Certificate Signing Request) – Message envoyé à l'Autorité de Certification pour demander la génération d'un certificat. Ce message contient des informations d'identification du demandeur ainsi que sa clé publique, le tout étant signé par sa clé privée. Dans le cas de la présente Politique de Certification, les CSR sont conformes au standard PKCS#10.

Déclaration des pratiques de certification (DPC) – Une DPC identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Demande de certificat : message transmis par l'AE à l'AC pour obtenir l'émission d'un certificat.

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

Dispositif de création de signature – Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour stocker et mettre en œuvre sa clé privée de signature.

Données d'activation : Des valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent (bi-clés) et qui sont protégées (par ex. un PIN, une phrase secrète, code OTP, …).

Dossier d'enregistrement – Ensemble de documents permettant au Chargé de Clientèle et à l'AE Technique de valider la demande d'enregistrement d'un futur Client.

Entité – Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

Etablissement : Membre du réseau Banque Populaire ou du réseau Caisse d'Epargne

Fonction de génération des certificats – Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du porteur provenant soit du porteur, soit de la fonction de génération des éléments secrets du porteur, si c'est cette dernière qui génère la bi-clé du porteur.

Fonction de génération des éléments secrets du porteur – Cette fonction génère les éléments secrets à destination du porteur, si l'AC a en charge une telle génération, et les prépare en vue de leur remise au porteur (par exemple, personnalisation de la carte à puce destinée au porteur, courrier sécurisé avec le code d'activation, etc.). De tels éléments secrets peuvent être, par exemple, directement la bi-clé du porteur, les codes (activation / déblocage) liés au dispositif de stockage de la clé privée du porteur ou encore des codes ou clés temporaires permettant au porteur de mener à distance le processus de génération / récupération de son certificat.

Fonction de gestion des révocations – Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction de hachage : fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux trois propriétés suivantes :

- Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie ;
- Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie [ISO/IEC 10118-1] ;
- Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

Fonction d'information sur l'état des certificats – Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) et éventuellement également selon un mode requête / réponse temps réel (OCSP).

Fonction de publication – Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.

Fonction de remise au porteur – Cette fonction remet au porteur au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif du porteur, clé privée du porteur, codes d'activation,…).

Gestionnaire de Certificats (GC) – voir Mandataire de Certification.

Infrastructure de Confiance Groupe (ICG) - Infrastructure technique regroupant tous les composants mis en œuvre dans le processus de signature électronique des contrats.

Infrastructure de Gestion de Clés (IGC) – Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de Gestionnaire de Certificats, d'une entité d'archivage, d'une entité de publication, etc.

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.

***Key Ceremony* (ou Cérémonie de Clés) –** Une *Key Ceremony* est une cérémonie notariée (réalisée en effectif restreints devant témoins, éventuellement filmée…) au cours de laquelle sont réalisées des opérations relatives au cycle de vie des clés d'AC. Par exemple la *Key Ceremony* associée à la création d'un certificat d'AC regroupera les procédures de génération de la bi-clé, de génération du certificat d'AC, de génération et de partage des parts de secrets liés à l'activation de la clé privée… On réalisera une *Key Ceremony* notamment pour la création, la révocation et le renouvellement d'un certificat d'AC racine ou d'AC fille.

Liste de Certificats Révoqués (LCR) : liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués.

Modules cryptographiques : Un ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé …). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée (FIPS ou critères communs), utilisé pour conserver et mettre en œuvre la clé privée AC.

Période de validité d'un certificat : La période de validité d'un certificat est la période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 2459].

Personne autorisée – Il s'agit d'une personne autre que le porteur qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

PKCS #10 : (Public-Key Cryptography Standard #10) mis au point par RSA Security Inc., qui définit une structure pour une Requête de Signature de Certificat (en anglais: Certificate Signing Request: CSR).

Plan de secours (après sinistre) : plan défini par une AC 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.

Point de distribution de LCR *:* entrée de répertoire ou une autre source de diffusion des LCR; une LCR diffusée via un point de distribution de LCR peut inclure des entrées de révocation pour un sous-ensemble seulement de l'ensemble des certificats émis par une AC, ou peut contenir des entrées de révocations pour de multiples AC. [ISO/IEC 9594-8; ITU-T X.509].

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 Gestion des Preuves (PGP) – 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 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].

Porteur – La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat. Dans le cadre de la présente PC, le terme de Porteur correspond à un Client ou un Prospect.

Porteur de secret : personnes qui détient une donnée d'activation liée à la mise en œuvre de la clé privée d'une AC à l'aide d'un module cryptographique.

Prestataire de services de certification électronique (PSCE) – Un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

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.

Promoteur d'application – Un responsable d'un service de la sphère publique accessible par voie électronique.

Qualificateur de politique : Des informations concernant la politique qui accompagnent un identifiant de politique de certification (OID) dans un certificat X.509. [RFC 3647]

RSA : algorithme de cryptographique à clé publique inventé par Rivest, Shamir, et Adelman.

Système d'information – Tout ensemble de moyen destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Titre d'identité – Carte d'identité nationale, passeport, ou carte de séjour pour les étrangers.

Usager – Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives.

Nota - Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager.

Utilisateur de certificat – L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du porteur du certificat.

Validation de certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de confiance et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC de la chaine de délivrance et la vérification de la signature électronique de l'ensemble des AC contenue dans le chemin de certification.

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 de l'opérateur.

Ces exigences s'appliquent à l'ensemble des infrastructures de confiance mises en œuvre par l'opérateur, notamment l'IGC, le service de signature, le service d'horodatage, le service de gestion de preuve et le service d'archivage.

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. L'archivage des fichiers de preuve (Se reporter au document « Politique de Gestion des Preuves BPCE SA ») de l'AE à valeur légale est hébergé chez un Opérateur Technique choisi par l'AP.

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 rôles de confiance sont classés de la manière suivante :

- Les personnels d'exploitation, dont la responsabilité est le maintien des systèmes qui supportent l'Infrastructure de Confiance Groupe en conditions opérationnelles de fonctionnement.

- Les personnels d'administration, dont la responsabilité est l'administration fonctionnelle des composantes 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.

- Auditeur : tiers désigné par l'AP pour effectuer l'audit de l'ensemble des mesures techniques, physiques, fonctionnelles et organisationnelles permettant de mesurer la conformité de l'Infrastructure de Confiance Groupe par rapport aux PC et DPC. Il est choisi selon des critères d'indépendance et d'expertise dans le domaine de la sécurité informatique et, en particulier, des Infrastructures de Confiance Groupe.

- Détenteur de données d'activation (ou détenteur de secret) : personne désignée par l'AP pour détenir une donnée d'activation de la clé privée d'une AC conformément aux règles de sécurité définies dans la PC, la DPC et des pratiques associées pour l'AC concernée. Cette personne peut posséder plusieurs éléments secrets provenant de plusieurs AC dès lors qu'il ne possède pas plus d'un élément par AC.

- Témoin : personne nommée par l'AP pour attester que l'intégralité des opérations effectuées lors de la cérémonie des clés ont été effectivement réalisées conformément aux documents présentés et approuvés au préalable assurant ainsi l'intégrité des opérations effectuées.

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

L'OT fait vérifier l'identité et les autorisations de tout membre de son personnel amené à 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 DPC et sont conformes à la politique de sécurité de l'OT. 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) et des données d'authentification correspondantes (mots de passe, certificats, etc.).
- Démarrage et arrêt des systèmes informatiques et des applications.
- Evènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation.
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes.

D'autres évènements sont également recueillis. Il s'agit d'évènements concernant la sécurité qui ne sont pas produits automatiquement par les systèmes mis en œuvre :

- Les accès physiques aux zones sensibles.
- Les actions de maintenance et de changements de la configuration des systèmes.
- Les changements apportés au personnel ayant des rôles de confiance.
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les Utilisateurs,...).

En plus de ces exigences de journalisation communes à toutes les composantes et à toutes les fonctions de l'Infrastructure Confiance Groupe, des évènements spécifiques aux différentes fonctions de l'IGC sont également journalisés :

- Réception d'une demande de certificat (initiale et renouvellement).
- Validation / rejet d'une demande de certificat.
- Evènements liés aux clés de signature des Porteurs (Client) et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, destruction,...).
- Génération des certificats de porteurs.
- Transmission des certificats aux porteurs et selon les cas, acceptations / rejets par les Porteurs.
- Publication et mise à jour des informations liées à l'AC.
- Génération d'information de statut d'un certificat (porteur).

Chaque enregistrement d'un évènement dans un journal contient les champs suivants :

- Type de l'évènement.
- Nom de l'exécutant ou référence du système déclenchant l'évènement.
- Date et heure de l'évènement.
- Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements.

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 de la présente PC.

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). Le système de datation des évènements respecte les exigences du § **Erreur ! Source du renvoi introuvable.**. Les ournaux 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 sont 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 données

L'archivage des données 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.
- La politique de certification.
- La déclaration des pratiques de certification.
- Les certificats tels qu'émis ou publiés.
- Les justificatifs d'identité des porteurs et, le cas échéant, les justificatifs d'existence juridique de leur entité de rattachement (pour les entreprises et les administrations).
- Les fichiers de preuves de l'AE (Se reporter au document « Politique de Gestion des Preuves BPCE SA »).
- Les dossiers complets de demandes de certificats.
- Les journaux d'évènements des différentes entités de l'Infrastructure de Confiance Groupe.

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 formulées à l'article 6.8.

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 (Se reporter au 5.5.3).

3.5.5 Procédures de récupération et de vérification des archives

Les sauvegardes électroniques archivées sont récupérables dans les meilleurs délais.

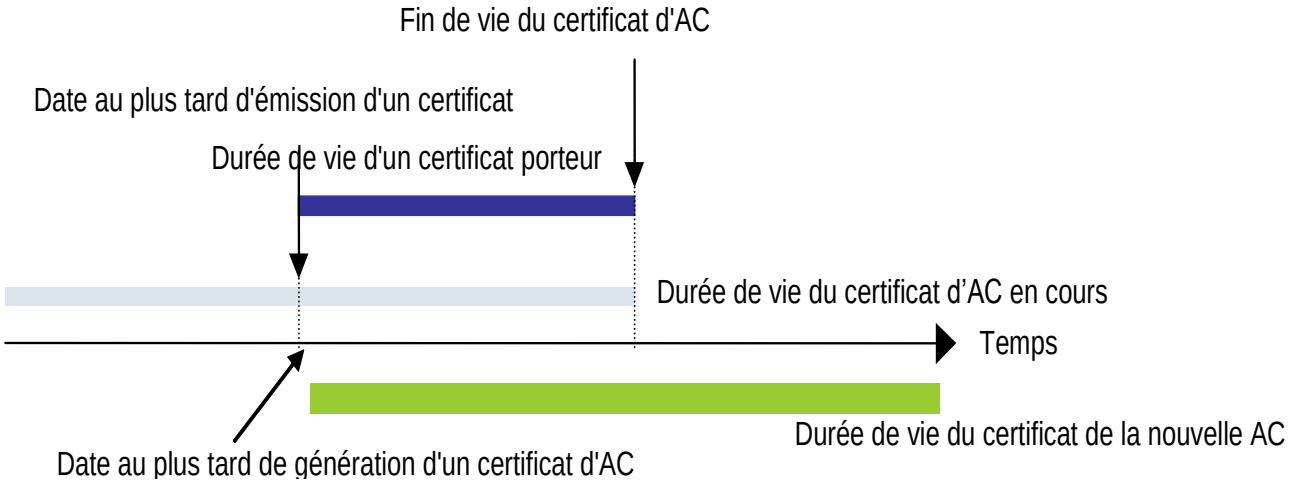
3.6 Changement de clé d'AC

3.6.1 Certificat d'AC

La durée de vie d'un certificat d'AC est déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationales ou internationales compétentes en la matière. La DPC précise les standards utilisés.

Une AC ne peut pas générer de certificats dont la durée de vie dépasse la période de validité de son certificat d'AC. C'est pourquoi, la bi-clé d'une AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats émis.

Dès qu'une nouvelle clé privée est générée pour l'AC, seule celle-ci est utilisée pour générer de nouveaux certificats de porteurs. Le précédent certificat d'AC reste valable pour valider le chemin de certification des anciens certificats émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats porteurs émis à l'aide de cette bi-clé.



Par ailleurs, l'AC change sa bi-clé et le certificat correspondant quand la bi-clé cesse d'être conforme aux recommandations de sécurité cryptographique concernant la taille des clés ou si celle-ci est soupçonnée de compromission ou compromise.

3.6.2 Certificat de Porteur

3.6.2.1 Certificat « Client »

La durée de validité d'un certificat est de 10 minutes maximum.

3.6.2.2 Certificat « Cachet serveur »

La durée de validité d'un certificat est de 3 ans maximum.

3.7 Reprise suite à compromission et sinistre

3.7.1 Procédures de remontée et de traitement des incidents et des compromissions

L'AC a établi un plan de continuité de service. Il est composé des différentes étapes à exécuter dans l'éventualité de la corruption ou de la perte des ressources système, des logiciels et / ou des données et qui pourraient perturber ou compromettre le bon déroulement des services d'AC.

Le plan de continuité de l'AC fait partie du périmètre audité, selon le paragraphe 8 ci-dessous.

Les personnels de l'AC dans un rôle de confiance sont spécialement entraînés à réagir selon les procédures définies dans le plan de reprise d'activité qui concernent les activités les plus sensibles.

Dans le cas où l'AC détecte une tentative de piratage ou une autre forme de compromission, elle mène une analyse afin de déterminer la nature des conséquences et leur niveau. L'AC informe les CT et éventuellement révoque les certificats « cachet serveur ».

L'AC prévient directement et sans délai OpenTrust.

3.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Si le matériel de l'AC est endommagé ou hors service alors que les clés de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des services de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC.

3.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Si la clé de signature de l'AC est compromise, perdue, détruite, ou soupçonnée d'être compromise :

- L'AP, après enquête sur l'évènement décide de révoquer le certificat de l'AC.
- les CT sont avisés dans les plus brefs délais que le certificat d'AC a été révoqué.
- L'AP décide ou non de générer une nouvelle bi-clé d'AC et un nouveau certificat d'AC.

3.7.4 Capacités de continuité d'activité suite à un sinistre

Le plan de reprise d'activité après sinistre traite de la continuité d'activité telle qu'elle est décrite au § 3.7.1. Le SP est installé afin d'être disponible 24 heures sur 24 et 7 jours sur 7.

3.8 Fin de vie d'Infrastructure de Gestion de Clés

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

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'Infrastructure de Gestion de Clés ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'Infrastructure de Gestion de Clés comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

3.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'Infrastructure de Gestion de Clés

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC :

- Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats).
- Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la PC.

Des précisions quant aux engagements suivants sont ainsi annoncées par l'AC dans sa PC :

- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des porteurs ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire.
- L'AC communique à OpenTrust, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC devra communiquer à OpenTrust, selon les différentes composantes de l'Infrastructure de Gestion de Clés concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats.
- L'AC tient informé OpenTrust de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

3.8.2 Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité est progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, assurera la révocation des certificats et la publication des LCR conformément aux engagements pris dans la PC.

L'AC procède aux actions suivantes :

- La notification des entités affectées,
- Le transfert de ses obligations à d'autres parties,
- La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC :

- S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats,
- Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante,
- Révoque son certificat,
- Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité,
- Informe (par exemple par récépissé) tous les porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

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