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

Référence du document	
1.3.6.1.4.1.40559.000	1er juillet 2013

BPCE : Société anonyme à directoire et conseil de surveillance,

au capital de 467 226 960 €.

Siège social : 50 avenue Pierre Mendes France

75201 Paris Cedex 13. RCS n° 493 455 042.

SOMMAIRE

1 DÉFINITIONS ET ACRONYMES

1.1 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 Preuves
AE	Autorité d'Enregistrement
AGP	Autorité de Gestion de Preuves
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
API	Application Programming Interface
AS	Autorité de Signature
BPCE SA	Banque Populaire Caisse d'Epargne
CEN	Comité Européen de Normalisation
CISSI	Commission Interministérielle pour la SSI
CN	Common Name
COSSIG	Comité Sécurité des Systèmes d'Information Groupe
CSR	Certificate Signing Request
CRL	Certificat Révocation List
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
GC	Gestionnaire de Certificats
.HSM	Hardware Sécurity Module
ICG	Infrastructure de Confiance Groupe
IGC	Infrastructure de Gestion de Clés
ITCE	Informatique & Technologie Caisse d'Epargne
KC	Key Ceremony
LAR	Liste des certificats d'AC Révoqués

LCP	Light Weight Certificat Policy
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
NTP	Network Time Protocole
OC	Opérateur de Certification
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
PA	Politique d'Archivage
PC	Politique de Certification
PGP	Politique de Gestion des Preuves
PH	Politique d'Horodatage
.PKI	Public Keys Infrastructure
PP	Profil de Protection
PS	Politique de Signature
PSCE	Prestataire de Services de Certification Électronique
RSA	Rivest Shamir Adelman
SP	Service de Publication
.SNMP	Simple Network Management Protocol
.SSI	Sécurité des Systèmes d'Information
UH	Unité d'Horodatage
URL	Uniform Resource Locator

1.2 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

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

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 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

BPCE – Banques Populaires Caisse d'Epargne

BPCE SA – Organe central du Groupe BPCE

Certificat électronique – Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

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

Comité Sécurité Groupe – instance de pilotage de l'Autorité de Certification. Elle comprend notamment le Responsable de l'Autorité de Certification. Le comité de pilotage prend notamment les décisions de mener des analyses de risque et des audits.

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.

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.

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.

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.

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.

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 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,…).

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).

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.

Informatique & Technologies Caisse d'Epargne (ITCE) - GIE informatique de BPCE SA.

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.

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.

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.

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.

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.

Prospect - Personne morale ou personne physique signataire du Contrat. Il s'agit nécessairement d'une personne ou d'une entité inconnue du réseau de la banque et qui n'est pas encore Client.

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.

2 MESURES DE SÉCURITÉ NON TECHNIQUES

Ce chapitre présente un ensemble de mesures non techniques concernant la sécurité de l'infrastructure mise en œuvre par IT-CE pour le compte de l'Autorité. 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.

2.1 Mesures de sécurité physique

2.1.1 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.

2.1.2 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).

2.1.3 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'Autorité en matière de disponibilité pour l'ensemble des fonctions sensibles de son infrastructure.

2.1.4 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).

2.1.5 Prévention et protection incendie

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

2.1.6 Conservation des supports

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

2.1.7 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.

2.1.8 Sauvegardes hors site

Afin de permettre une reprise après incident conforme aux engagements pris par l'Autorité, l'opérateur technique met en place 2 sites redondés permettant dans cette forme de garantir l'externalisation des données.

2.2 Mesures de sécurité procédurales

2.2.1 Rôles de confiance

Les opérations réalisées par l'opérateur technique sont classées selon leur niveau de sensibilité. Les opérations sensibles suivent des procédures définies qui s'appuient sur les rôles de confiance. Ces procédures respectent les principes de séparation des responsabilités et du moindre privilège.

Les documents techniques de l'opérateur décrivent les rôles de confiance qui lui sont propres. Ces rôles sont les suivants :

- Responsable sécurité : Il est chargé de la mise en œuvre de la politique de sécurité de l'Autorité. Il gère les contrôles d'accès physiques aux équipements des systèmes de l'infrastructure. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats.

- Responsable d'application : Il est chargé de la mise en œuvre des politiques définies par l'Autorité niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

- Administrateur système : Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de l'infrastructure. Il assure l'administration technique des systèmes et des réseaux correspondants.

- Exploitant : Un exploitant au sein de l'infrastructure réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre.

- Auditeur système : Il s'agit d'une personne autorisée à voir les archives et les fichiers de traces de manière à investiguer sur les anomalies éventuelles rencontrées par les composantes de l'infrastructure.

De plus, l'Autorité compte les rôles de confiance suivants :

- Responsable de l'Autorité (voir les responsabilités attribuées dans chacune des politiques). Le responsable décide de la création de l'Autorité, ou a été désigné par le précédent Responsable de l'Autorité pour assurer ce rôle. Il est le valideur des exigences prises dans chacune des politiques.

- Rôles de porteurs de secrets : il s'agit des personnes présentes au moment de la cérémonie des clés et qui disposent d'une part du secret permettant de faire fonctionner les fonctions cryptographiques sensibles de l'Autorité de Certification.

L'ICG est régie par un comité de pilotage présidé par le RSSI du Groupe BPCE et dénommé Comité Sécurité Groupe.

2.2.2 Nombre de personnes requises par tâches

En fonction des opérations réalisées, une ou plusieurs personnes avec des rôles différents seront requises.

Les documents techniques de mises en œuvre des différentes politiques précisent pour chaque type d'opération le nombre de personnes et de rôles requis.

2.2.3 Identification et authentification pour chaque rôle

Toute personne intervenant dans le fonctionnement de l'infrastructure doit avoir préalablement été notifiée du rôle correspondant.

La procédure d'habilitation correspondante est définie. Elle est détaillée dans les documents techniques de mise en œuvre.

L'affectation d'un rôle est tracée.

Le rôle peut donner les habilitations suivantes :

- Accès physique aux locaux et jusqu'aux systèmes.

- Accès logique aux services techniques, à l'aide d'un compte et d'un authentifiant (le cas échéant, un certificat).

2.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être affectés à une même personne, quand la définition du rôle le permet.

Les cumuls de rôles de confiance suivants sont interdits :

- Responsable de sécurité et administrateur système ou exploitant.

- Auditeur système et tout autre rôle.

2.3 Mesures de sécurité vis-à-vis du personnel

2.3.1 Qualifications, compétences et habilitations requises

Le personnel travaillant pour l'une des composantes de l'infrastructure est soumis à une clause de confidentialité vis-à-vis de son employeur.

Les fonctions demandées à chaque membre du personnel doivent être compatibles avec ses compétences. Notamment, le personnel d'encadrement doit avoir l'expertise nécessaire et être familier des procédures de sécurité.

L'Autorité informe chaque personne disposant d'un rôle de confiance :

- De ses responsabilités relatives aux services de l'ICG.
- Des procédures qu'elle doit respecter, concernant la sécurité du système et le contrôle du personnel.

Les rôles de confiance sont affectés par des personnes exerçant elles-mêmes une fonction de sécurité. Elles sont précisées dans la procédure d'habilitation décrite dans les documents techniques de l'opérateur.

2.3.2 Procédures de vérification des antécédents

Le personnel travaillant pour l'une des composantes de l'ICG est soumis à une procédure de vérification de ses antécédents lors de sa prise de fonction.

Pour les rôles de confiance, des vérifications sont menées en plus tous les 3 ans.

Les vérifications porteront sur les points suivants :

- Les éventuelles condamnations en justice de la personne ne devront pas être contraires à ses fonctions.
- Les rôles de confiance ne devront pas se trouver dans un conflit d'intérêt préjudiciable à l'impartialité de leurs tâches.

2.3.3 Exigences en matière de formation initiale

Le personnel travaillant pour l'une des composantes de l'ICG doit être préalablement formé.

Cette formation lui permet notamment de prendre conscience des enjeux de sécurité liés à sa fonction.

2.3.4 Exigences et fréquence en matière de formation continue

En fonction des évolutions apportées au fonctionnement de l'ICG (concernant les systèmes techniques ou les procédures), le personnel reçoit une formation, ou les informations nécessaires à la bonne réalisation de ses activités.

2.3.5 Fréquence et séquence de rotation entre différentes attributions

Des changements dans les affectations de rôles peuvent avoir lieu soit en cas de départ, ou de mutation d'un membre du personnel, soit suite à un audit.

2.3.6 Sanctions en cas d'actions non autorisées

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

2.3.7 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.

2.3.8 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.

2.4 Procédures de constitution des données d'audit

2.4.1 Type d'évènements à enregistrer

Les événements listés ci-dessous concernent l'ensemble des composantes de l'ICG.

Les événements systèmes suivants sont enregistrés de manière automatique pour chacun des serveurs composant l'infrastructure :

- 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.
- Évènements 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 les tentatives non réussies correspondantes.

Les événements suivants sont enregistrés, de manière automatique ou manuelle :

- Accès physiques aux salles hébergeant les composants de l'infrastructure.
- Actions de maintenance et de changements de la configuration des systèmes
- Changements apportés au personnel.
- Actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...).

Concernant la gestion du cycle de vie des certificats, les événements ci-dessous sont enregistrés de manière automatique ou manuelle :

- Réception d'une demande de certificat.

- Validation / rejet d'une demande de certificat.
- Évènements liés aux clés de signature et aux certificats d'AC (génération (*Key Ceremony*), sauvegarde / récupération, révocation, renouvellement, destruction,...).
- Génération des éléments secrets du Porteur (bi-clé, codes d'activation,…).
- Génération des certificats des porteurs.
- Publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.).
- Réception d'une demande de révocation.
- Validation / rejet d'une demande de révocation.
- Génération puis publication des LCR.

Les journaux du service d'horodatage sont conservés sur le serveur d'horodatage depuis sa mise en activité. La journalisation effectuée par les unités d'horodatage concerne les évènements relatifs à l'administration (modification de la configuration, mise à jour d'une politique de confiance), à l'horloge (synchronisation, perte de calibrage, etc.) et à la gestion d'un jeton d'horodatage.

Pour chaque événement, les informations suivantes sont enregistrées :

- Type de l'évènement.
- Nom / identifiant de l'exécutant ou référence du système déclenchant l'évènement.
- Date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée).
- Résultat de l'évènement (échec ou réussite).

De plus pour les événements concernant les certificats, les informations suivantes sont enregistrées :

- Destinataire de l'opération (Porteur du certificat).
- Nom 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.
- Autre information caractérisant l'évènement (notamment, pour la génération d'un certificat, le numéro de série de ce certificat).

Les événements à journaliser automatiquement sont enregistrés au cours du processus. Les événements qui sont journalisés manuellement le sont le même jour ouvré que l'événement.

2.4.2 Fréquence de traitement des journaux d'évènements

Les journaux des composantes de l'infrastructure sont analysés suite à la détection d'une anomalie. En fonction de cette anomalie, un rapprochement des journaux de chacune des composantes est mis en œuvre par l'opérateur technique.

2.4.3 Période de conservation des journaux d'évènements

Les journaux d'événement sont conservés sur site pendant au moins un mois.

Ils sont archivés, via la sauvegarde des serveurs, au plus tard un mois après leur génération.

2.4.4 Protection des journaux d'évènements

Le mode de conservation des journaux d'événements protège leur intégrité, et leur disponibilité.

Le système de datation des événements respecte les exigences décrites dans la Politique d'horodatage de l'ICG.

2.4.5 Procédure de sauvegarde des journaux d'évènements

Les procédures de sauvegarde des journaux sont globales et quotidiennes.

2.4.6 Système de collecte des journaux d'évènements

La collecte des journaux nécessite :

- D'accéder aux journaux disponibles directement sur les serveurs
- De récupérer les sauvegardes nécessaires si ces journaux ne sont plus disponibles sur les serveurs

2.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement

Sans objet.

2.4.8 Évaluation des vulnérabilités

Le contrôle des journaux des événements fonctionnels est réalisé à la demande en cas de litige, ou pour analyse de comportement du système d'information.

2.5 Archivage des données

2.5.1 Types de données à archiver

En plus des journaux d'événements, un certain nombre de données sont archivées par l'opérateur.

Les données archivées sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques.
- Les Politiques de Certification.
- Les DPC.
- Les certificats d'AC et LCR tels qu'émis ou publiés.
- Les journaux d'évènements des différentes entités.

2.5.2 Période de conservation des archives

Les durées de conservation sont définies dans les documents de mise en œuvre correspondant et respectent les exigences légales.

2.5.3 Protection des archives

Les archives sont stockées sur un site externe.

2.5.4 Procédure de sauvegarde des archives

Une procédure de sauvegarde des archives est définie. Les documents de mise en œuvre décrivent les moyens associés.

2.5.5 Exigences d'horodatage des données

Les journaux d'événements doivent être datés (voir le paragraphe 2.4.4).

2.5.6 Système de collecte des archives

Sans objet.

2.5.7 Procédures de récupération et de vérification des archives

Le circuit de demande et de validation d'accès à une archive est explicité dans les documents de mise en œuvre correspondants.

Les conditions de services liées à l'archivage sont maîtrisées par l'Opérateur de Service.

2.6 Changement de clé d'AC

L'Autorité de Certification a une durée de validité de 30 ans. Les certificats qu'elle émet ont une durée de vie de 10 minutes.

L'AC ne peut pas émettre de certificat qui serait encore valide au moment de la date de fin de validité de l'AC.

Le certificat d'AC sera renouvelé pour permettre l'émission de nouveaux certificats et toutes les nouvelles demandes devront être signées par le nouveau certificat d'AC.

L'ancien certificat d'AC servira pour valider les certificats précédemment émis, et pour signer les CRL.

2.7 Reprise suite à compromission et sinistre

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

Des procédures de remontée et de traitement des incidents sont mises en place par l'opérateur. La documentation de l'opérateur détaille le fonctionnement de ces procédures.

Ces procédures s'appuient notamment sur le personnel de l'opérateur et sur les journaux d'événements.

L'opérateur met en œuvre des scripts qui remontent des alertes automatiquement :

- Vers la supervision SNMP
- Vers le système de supervision globale

Sur détection d'une alerte la partie pilotage et exploitation de la supervision détermine une fiche d'action qui permet d'identifier et de résoudre l'anomalie rencontrée.

Dans le cas d'un incident majeur tel que la compromission d'une clé d'AC, le responsable de l'Autorité en est informé dans les plus brefs délais. Les incidents majeurs sont traités en première urgence. Cela peut donner lieu à la révocation d'un certificat d'AC.

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

L'infrastructure est bi-site en mode actif/actif l'arrêt d'un site n'arrête pas le service offert, toutes les demandes sont dirigées sur le site opérationnel.

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

L'infrastructure est bi-site en mode actif/actif l'arrêt d'un site n'arrête pas le service offert, toutes les demandes sont dirigées sur le site opérationnel.

Chaque site dispose d'une clé d'AC dédiée et en cas de corruption d'une des clés, les demandes sont orientées vers l'AC encore valide. L'ICG reste opérationnelle dans ce cadre.

2.7.4 Capacités de continuité d'activité suite à un sinistre

L'infrastructure est bi-site en mode actif/actif l'arrêt d'un site n'arrête pas le service offert, toutes les demandes sont dirigées sur le site opérationnel.

2.8 Fin de vie de l'IGC

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

L'AC a pris les dispositions nécessaires pour couvrir les coûts permettant de respecter un certain nombre d'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.

Les dispositions présentées ci-dessous, quand elles concernent l'opérateur technique, figurent dans le contrat entre l'Autorité et l'opérateur.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC 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'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

2.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à les transférer à une autre entité.

Le transfert d'activité ne comporte pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré, et la reprise de cette activité est organisée par l'AC en collaboration avec la nouvelle entité.

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

- Assurer la continuité du service d'archivage ;
- Assurer la continuité du service de révocation.

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 s'engage à les informer de ce transfert aussitôt que possible et, au moins, 1 mois avant.

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.

2.8.2 Cessation d'activité affectant l'AC

La cessation d'activité comporte une incidence sur la validité des certificats émis antérieurement à la cessation concernée, et une procédure spécifique est mise en œuvre dans ce cas.

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 s'engage à les informer de cette cessation aussitôt que possible et, au moins, 1 mois avant la cessation effective.

En cas de cessation d'activité, l'AC s'engage à respecter les principes suivants :

- Prévenir les Porteurs et les AE au moins un mois en avance ;

- La clé privée d'émission des certificats ne sera transmise en aucun cas ;
- Toutes les mesures nécessaires seront prises pour la détruire ou la rendre inopérante ;
- Le certificat d'AC sera révoqué ;
- Tous les certificats émis encore en cours de validité seront révoqués.

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.

Les représentants du comité de pilotage de l'AC devront se réunir pour réaliser les opérations sensibles de désactivation des clés d'AC, et de révocation des certificats préalablement émis.

3 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 dans une démarche de contrôle permanent.

3.1 Fréquences et circonstances des audits

Avant la première mise en service d'une composante de l'infrastructure. ou suite à toute modification significative au sein d'une composante, l'Autorité. fera procéder à un contrôle de conformité de cette composante.

L'Autorité procède à un contrôle régulier de conformité de l'ensemble de son infrastructure une fois tous les deux ans.

Des contrôles internes peuvent également être déclenchés sur décision du Comité Sécurité Groupe, sur des périmètres donnés.

3.2 Identité et qualifications des auditeurs

L'Autorité s'engage à mandater des contrôleurs qui soient compétents en sécurité des systèmes d'information, en particulier dans le domaine d'activité de la composante contrôlée.

3.3 Relations entre auditeurs et entités auditées

L'Autorité veillera à ce que l'équipe d'audit n'appartienne pas à l'entité opérant la composante contrôlée, quelle que soit cette composante, et à ce qu'elle soit dûment autorisée à pratiquer les contrôles visés.

3.4 Sujets couverts par les audits

Le programme d'audit est établi sur un cycle de deux ans.

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.

3.5 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