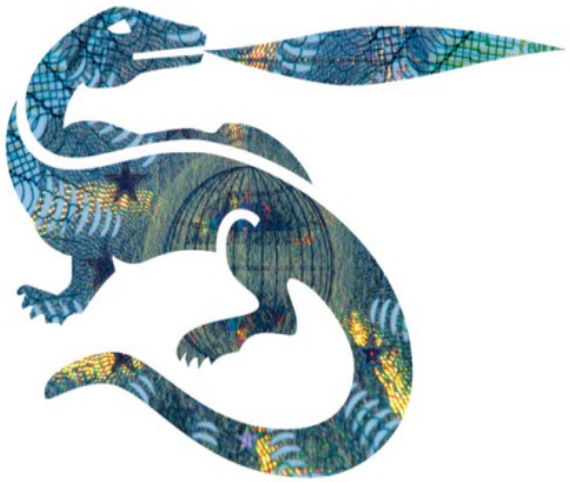
Imprimerie Nationale (INCS)

Politique de Certification
AC Élémentaire Chiffrement
Programme Plateforme de Gestion des Identités Numériques

Document sécurité



Mode de diffusion	**Publique**
Statut du document	**EN** COURS DE RÉDACTION
Date d'application	**1er janvier 2018**

HISTORIQUE DES VERSIONS

Version	Date	Auteur	Nature de la révision Paragraphes modifiés
0.2	20/12/2017	Imprimerie Nationale	Version initiale
1.0	31/12/2017	Imprimerie Nationale	Version validée

SOMMAIRE

I. Introduction

I.1. OBJET DU DOCUMENT ET GENERALITES

Le Groupe Imprimerie Nationale, à travers sa société IN Continu et Services (INCS) a mis en place une Infrastructure de Gestion de clés, baptisée « IN Élémentaire », afin de délivrer des certificats non qualifiés pour les besoins de ses clients.

La responsabilité de cette infrastructure de gestion de clés a été confiée à l'Entité juridique INCS. Dans ce contexte, INCS est PSCE (Prestataire de Service de Certification Électronique).

La présente politique de certification décrit les différents niveaux de responsabilité, les mesures de sécurité (techniques, audits...) ainsi que les profils des certificats. Elle expose également les engagements de l'AC Imprimerie Nationale Élémentaire Chiffrement dans le cadre de la fourniture de ses services de certification électronique pour chiffrement (confidentialité).

En conséquence, et compte tenu de la grande importance des PC pour établir la confiance à l'égard d'un certificat, il est primordial que la présente PC soit consultable non seulement par les Porteurs, mais également par tout Utilisateur de Certificat.

L'IGC Élémentaire est composée d'une autorité racine (ACR) baptisée « ACR Imprimerie Nationale Élémentaire » et d'autorités hiérarchiquement dépendantes (Autorité de Certification Fille ou ACF). L' « ACR Imprimerie Nationale Élémentaire » signe, outre les clés publiques des ACF, les LAR (Liste des Autorités Révoquées).

La présente politique ne concerne que l'AC Imprimerie Nationale Élémentaire Chiffrement, la politique de l'ACR Imprimerie Nationale Élémentaire est décrite dans un document distinct.

La hiérarchie d'autorité de certification est donc la suivante :

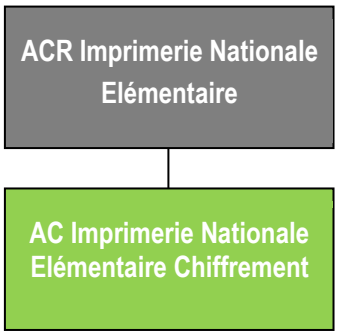


Figure 1 : Hiérarchie des Autorités de Certification

Toutes les AC étant sous la responsabilité d'INCS, le sigle AC désignera l'autorité morale responsable de cette ACR et de cette ACF.

Dans la version courante de la présente PC, l'AC Imprimerie Nationale Élémentaire Chiffrement délivre un certificat (double-usage) :

- De chiffrement (confidentialité) et de signature (intégrité)

Dans le cadre de la présente PC, les certificats sont exclusivement délivrés aux personnes physiques le certificat et avec laquelle ces personnes physiques ont un lien contractuel (cf. définition du Porteur de certificat au § I.3.7). Les

Entités Clientes à laquelle sont rattachées les personnes physiques peuvent appartenir au secteur privé ou au secteur public.

La structure de cette PC est conforme au [RFC3647] « *X.509 Public Key Infrastructure Certificate Policy Certification Practice Statement Framework* » de *l'Internet Engineering Task Force* (IETF).

Compte tenu de la complexité de lecture d'une Politique de Certification pour des Porteurs ou des Utilisateurs de certificats non spécialistes du domaine, INCS publie des Conditions Générales d'Utilisation tels que définis dans [RFC3647].

qui les utilisent (ainsi que les clés privées associées) dans le contexte de leurs activités en relation avec l'Entité Cliente identifiée dans Nom du document et identification

La présente PC nommée « POLITIQUE DE CERTIFICATION – AC Imprimerie Nationale Élémentaire Chiffrement » est la propriété d'INCS.

Cette Politique de Certification est identifiée dans le tableau suivant par les OID suivants :

Profil de certificat	OID associé
Certificat de confidentialité	1.2.250.1.295.1.1.10.1.1.110.0

I.2. ENTITES DE L'IGC

La notion d'autorité de certification (AC) telle qu'utilisée dans le présent document est définie au § I.6.1.

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation) et s'appuie pour cela sur une infrastructure technique dite infrastructure de gestion de clés (IGC). Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.

L'IGC s'appuie sur les services fonctionnels suivants :

- Génération des bi-clés : Ce service génère la bi-clé des futurs Porteurs et remet la clé publique à certifier au service de génération des certificats
- Génération de certificats : Ce service génère les certificats électroniques des futurs Porteurs à partir des informations fournies par l'autorité d'enregistrement.
- Révocation : Ce service traite les demandes de révocation de certificats et détermine les actions à mener dont la génération de la liste des certificats révoqués (LCR ou CRL).
- Publication : Ce service met à disposition des Utilisateurs de certificats (UC) et des Porteurs ou responsables de certificats les informations nécessaires à l'utilisation des certificats émis par les AC (Conditions Générales d'Utilisation, politiques de certification, certificats d'AC, …) ainsi que les résultats des traitements du service de gestion des révocations de certificats (LCR)
- Recouvrement : Ce service traite les demandes de recouvrement de clés privées des porteurs (notamment identification et authentification du demandeur) et détermine les actions à mener. Dans le cas d'une décision positive, le recouvrement est réalisé par la fonction de séquestre et recouvrement.
- Séquestre : Ce service fournit la capacité de séquestrer de manière sécurisée les clés privées des porteurs, puis de les recouvrer en cas de besoin, sur la base de demandes authentifiées et traitées par le service de gestion des recouvrements.

La présente PC définit les exigences de sécurité pour toutes les fonctions décrites ci-dessus pour délivrer des certificats aux Porteurs.

La Déclaration des Pratiques de Certification (DPC) décrit l'organisation opérationnelle de l'IGC et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrits dans la PC.

I.2.1. Autorité administrative INCS

L'autorité administrative INCS (AAI) est composée d'un COMITÉ DE SURVEILLANCE de l'IGC au sein d'INCS. Ce comité est responsable des AC (ACR et ACF) dont elle garantit la cohérence et la gestion du référentiel de sécurité, ainsi que sa mise en application. Le référentiel de sécurité est composé de la présente PC, de la DPC associée, des conditions générales d'utilisation et des procédures mises en œuvre par les composantes de l'IGC. L'AAI valide la PC et la DPC. Elle s'assure également de la cohérence de la DPC par rapport à la PC. Elle autorise et valide la création et l'utilisation des composantes de l'AC. Elle suit les audits et les contrôles de conformité effectués par les composantes de l'IGC, décide des actions à mener et veille à leur mise en application.

I.2.2. Les autorités de certification

L'autorité de certification fille (ACF) génère et révoque les certificats à partir des demandes envoyées par l'Autorité d'Enregistrement. L'ACF met en œuvre les services de génération de certificats, de révocation de certificats, d'information sur l'état des certificats, de journalisation et d'audits.

I.2.3. L'autorité d'enregistrement (AE)

L'AE est utilisée pour la mise en œuvre des services d'enregistrement de demandes de certificats, de remise de certificats, de révocation de certificats, de journalisation et d'audit. En particulier, l'AE a pour rôle de vérifier l'identité des futurs Porteurs de certificat, ainsi que celle des Mandataires de Certification (MC).

L'AE est sous la responsabilité d'INCS.

Une partie des procédures de gestion des certificats (délivrance, révocation, etc.) s'appuie sur une autorité d'enregistrement technique tierce, en charge du système d'information des AE.

I.2.4. Mandataire de Certification (MC)

Les mandataires de certification habilité le représentant légal de l'Entité Cliente sont des personnes physiques mandatées par le représentant légal de l'Entité Cliente autre qu'INCS et ayant le pouvoir de :

- authentifier les futurs Porteurs de l'Entité Cliente,
- effectuer une demande de certificat ou de renouvellement de certificat portant le nom de l'Entité auprès de l'AE
- effectuer une demande de révocation de certificat portant le nom de l'Entité
- remettre le cas échéant les supports de clés privées (cartes à puce) à leurs Porteurs

Le MC n'a, en aucun cas, accès aux moyens lui permettant d'activer et d'utiliser la clé privée associée aux certificats de clés publiques délivrés par l'AC aux Porteurs.

Le MC est en relation directe avec l'AE de l'AC.

Les engagements et obligations des MC sont précisés dans une lettre d'engagement qu'ils doivent signer.

Cette lettre d'engagement stipule notamment que le MC doit effectuer de façon indépendante les contrôles d'identité des futurs Porteurs, et respecter les parties de la présente PC et de la DPC qui lui incombent.

En cas de remplacement pour quelque cause que ce soit d'un MC de ses fonctions, l'Entité doit le signaler à l'AC sans délai. Le cas échéant lui désigner un successeur si aucun autre MC n'est encore en fonction.

I.2.5. Le Service de Publication (SP)

Le SP est utilisé pour la mise en œuvre du service de publication (voir § II).

Le SP agit conformément à la PC et DPC associée.

I.2.6. Opérateur technique

Se référer à la DPC.

I.2.7. Porteur de certificat

Est désigné comme « Porteur de certificat », toute entité détentrice d'une bi-clé et du certificat de clé publique associé délivré par l'AC Imprimerie Nationale Élémentaire Chiffrement d'INCS.

Dans la présente PC, cette entité (le Porteur) ne peut être qu'une personne physique, acteur du secteur privé ou du secteur public, possédant une carte et des certificats émis par l'*AC Imprimerie Nationale Élémentaire Personnel*. Cette personne utilise sa clé privée et le certificat correspondant dans le cadre de ses activités professionnelles, c'est-à-dire ses activités en relation avec l'Entité Cliente identifiée dans le certificat et avec laquelle il a un lien contractuel (cf. III.2.2).

En pratique, il existe trois types de Porteurs : les responsables légaux (RL) d'une Entité Cliente, les mandataires de certification d'une Entité Cliente (MC), et les Porteurs « finaux ».

La présente PC impose que la clé privée du Porteur soit stockée sur un support physique (carte à puce) et que la mise en œuvre de cette clé nécessite une authentification (soumission du code PIN à la carte).

Le Porteur respecte les conditions qui lui incombent et qui sont définies dans la présente PC. Ces conditions sont reprises dans les Conditions Générales d'Utilisation qu'il a explicitement acceptées lors de sa demande de certificat.

I.2.8. Entité Cliente

La personne morale (société / la collectivité territoriale / l'établissement public / l'association, etc.) cocontractante d'INCS, indiquée dans la Demande de Certificat, à laquelle le Porteur est rattaché, et au nom de laquelle ce dernier utilise les Certificats électronique. Le Représentant Habilité de l'Entité Cliente légale devra signer le Formulaire de demande de Certificats. Il peut néanmoins recourir à un Mandataire de certification tant pour la phase de demande de Certificat que pour la phase de remise des Supports.

I.2.9. Utilisateurs de certificats (UC)

Un Utilisateur de certificat est toute application, personne physique ou morale, système informatique, matériel qui utilise un certificat de Porteur conformément à la présente PC et les pratiques de sécurité édictées par les responsables d'application ou le responsable de son Entité, afin de valider les fonctions de sécurité mises en œuvre à l'aide des certificats émis au titre de la présente PC.

L'UC utilise :

- un certificat et un dispositif de chiffrement pour chiffrer des données ou un message (courriel) à destination du Porteur du certificat ;
- un certificat et un dispositif de vérification de signature pour vérifier l'intégrité et l'origine de données ou de messages (courriels) émis par le Porteur du certificat.

L'Utilisateur de certificat peut détenir son propre certificat. Un Porteur qui reçoit un certificat d'un autre Porteur devient un Utilisateur de certificat. Dans le cadre de cette PC, l'Utilisateur de certificat doit valider la chaîne de certification (validation du certificat du Porteur, du certificat de l'ACF et de l'ACR) et contrôler la non-révocation des certificats (certificat du Porteur et certificat de l'ACF élémentaire) par le biais du service de publication mis à sa disposition.

I.3. USAGE DES CERTIFICATS

I.3.1. Domaines d'utilisation applicables

1. Bi-clés et certificats de l'AC

La bi-clé de l'AC Imprimerie Nationale Élémentaire Chiffrement sert à signer les certificats et les listes de certificats révoqués (LCR) qu'elle émet.

L'AC Imprimerie Nationale Élémentaire Chiffrement dispose d'une bi-clé unique pour signer les certificats et les LCR. Cette bi-clé est exclusivement utilisée à cette fin.

Le certificat rattaché à cette bi-clé est signé par l'autorité de niveau supérieur.

2. Bi-clés et certificats des Porteurs

La présente PC traite des bi-clés et certificats émis par l'AC Imprimerie Nationale Élémentaire Chiffrement à destination des catégories de Porteurs identifiées au § I.3.7 (personnes physiques) afin que ces dernières puissent :

- déchiffrer électroniquement des données (documents ou messages) dans le cadre d'échanges dématérialisés avec les catégories d'Utilisateurs de certificats identifiées au chapitre § I.3.8 ci-dessus ;
- assurer l'intégrité et l'origine de données (documents ou messages), *sans consentement quant au contenu des données*, dans le cadre d'échanges dématérialisés avec les catégories d'Utilisateurs de certificats identifiées au chapitre § I.3.8 ci-dessus.

Remarque :

- Il est expressément entendu qu'un Porteur de certificat ne peut user de sa clé privée et de son certificat qu'à des fins de confidentialité ou d'intégrité. En cas d'usage non autorisé d'une clé privée et de son certificat par son Porteur, la responsabilité de ce dernier pourrait être engagée.
- Il est également expressément entendu que l'Utilisateur du certificat ne peut faire confiance à ce dernier que dans le cadre d'échanges dématérialisés avec le Porteur.

I.3.2. Utilisation interdite des certificats

Les utilisations de certificats émis par l'AC Imprimerie Nationale Élémentaire Chiffrement à d'autres fins que celles prévues par la présente PC (cf. § I.4.1) n'est pas autorisée. Cela signifie que l'AC ne peut, en aucun cas, être tenue pour responsable d'une utilisation des certificats qu'elle émet autre que celle prévue dans la présente PC.

La signature électronique de données par un certificat émis par l'AC Imprimerie Nationale Élémentaire Chiffrement apporte uniquement des garanties d'authenticité et d'intégrité des données signées et, en aucun cas, la garantie du consentement du signataire quant au contenu de ces données.

L'AC s'engage à faire respecter ces restrictions aux Porteurs et aux Utilisateurs potentiels de ces certificats. À cette fin, l'AC publie à leur destination les Conditions Générales d'Utilisation (CGU). En particulier, la délivrance du certificat à un Porteur est soumise à l'acceptation explicite de ces CGU (mention indiquée dans le formulaire de demande que le Porteur doit signer).

I.4. GESTION ET APPLICATION DE LA POLITIQUE

I.4.1. Entité gérant la présente politique

L'AAI est responsable de la gestion et de la validation de la présente PC.

Point de contact :

Service SSI
Rue des Frères Beaumont
59128 – Flers-en-Escrebieux
SSI@imprimerienationale.fr

Toute remarque ou commentaire peut être transmis à ce point de contact.

I.4.2. Entité déterminant la conformité de la DPC avec cette PC

L'AAI est responsable de la vérification de la conformité de la DPC avec la présente PC. Elle procède ainsi à des contrôles de conformité et à des audits afin d'autoriser ou non l'émission des certificats. Les audits peuvent être confiés à une société tierce choisie par l'AAI.

I.4.3. Procédure d'approbation de la conformité de la DPC

La DPC sera déclarée conforme à la PC à l'issue d'un processus d'approbation élaboré par l'INCS.

Cette DPC sera revue régulièrement (au moins une fois par an) par le comité de surveillance qui constitue l'AAI pour :

- Assurer sa conformité aux normes de sécurité attendues par les applications qui référencent des familles de certificat porteur,
- Mettre à jour la liste des applications concernées par la PC,
- Adapter aux évolutions technologiques.

Le processus d'approbation sera suivi pour toute mise à jour de la DPC.

I.5. DOCUMENTS DE REFERENCE

I.5.1. Réglementation

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ; http://www.cil.cnrs.fr/CIL/spip.php?rubrique281
Règlement européen nº 2016/679 du 27 avril 2016 (Règlement Général sur la Protection des Données).
Règlement européen nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur
[ORDONNANCE] Ordonnance nº 2005-1516 du 8 Décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&dateTexte=vig
Article 801-1 du code de procédure pénale

Article 1366 et suivant du *Code civil* relatif à la signature électronique
[DécretRGS] Décret n°2010-112 du 2 Février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n°2005-1516 http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&dateTexte=vig
Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=vig
Arrêté du 26 Juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441678&dateTexte=vig
Loi n°2000-321 du 12 Avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629288&dateTexte=vig
Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=id
Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024502658&categorieLien=id
Directives dites « Paquet telecom » qui comprend : - une directive (2009/140/CE) qui amende trois directives existantes : - directive accès (2002/19/CE) - directive autorisation (2002/20/CE) - directive cadre (2002/21/CE) - une directive (2009/136/CE) qui amende deux directives existantes : - directive service universel (2002/22/CE) - directive vie privée et communications électroniques (2002/58/CE) - un règlement (CE) N° 1211/2009 instituant l'Organe des régulateurs européens des communications électroniques (ORECE)
Décret n° 2006-212 du 23 février 2006 relatif à la sécurité des activités d'importance vitale http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000634536&dateTexte=&categorieLien=id
Décret n° 2012-491 du 16 avril 2012 relatif à l'accès aux points d'importance vitale http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025703623&dateTexte=&categorieLien=id

Décret n° 2011-1425 en date du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024749915&dateTexte=&categorieLien=id
Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023707312&categorieLien=id
Article 226-4-1 du Code pénal (usurpation d'identité) Art. 226-16 et suivants du Code pénal et Art. R. 625-10 et suivants du Code pénal (atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques)
Conseil de l'Europe - Convention sur la cybercriminalité dite de Budapest du 23 Novembre 2001

I.5.2. Documents techniques

[RFC 3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

I.6. TERMINOLOGIE ET ABREVIATIONS

I.6.1. Terminologie

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.

Autorité de Certification (AC) : autorité à qui un ou plusieurs Utilisateurs se fient pour créer et attribuer des certificats. [ISO/IEC 9594-8; ITU-T X.509].

Bi-clé : Paire de clés asymétriques, constituée d'une clé publique et de la clé privée correspondante.

Cérémonie de clés : Une procédure par laquelle une bi-clé d'AC est générée et/ou sa clé publique certifiée.

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]. Le certificat contient des informations d'identification du propriétaire de la bi-clé.

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 asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

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

CMS : Ce système est chargé de la gestion du cycle de vie des cartes à puce des Porteurs et de leurs certificats. Ce système effectue les demandes de certificats des Porteurs, les demandes de renouvellement de certificats et les demandes de révocation. Il s'interface donc avec l'IGC pour demander à l'IGC la réalisation de ces différentes fonctions.

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].

Déclaration des Pratiques de Certification (DPC) : une déclaration des pratiques qu'une entité (agissant en tant qu'Autorité de Certification) applique dans le cadre de fourniture de ses services de certification (demande, émission, renouvellement et révocation de certificats) en conformité avec la PC qu'elle s'est engagée à respecter. [Définition PC type RGS].

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

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 et qui doivent être protégées (par ex. un PIN, une phrase secrète, …).

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.

IGC (Infrastructure de Gestion de Clés) : également appelée Infrastructure à Clé Publique (ICP), c'est l'infrastructure requise pour produire, distribuer, gérer et archiver des clés, des certificats et des Listes de Certificats Révoqués ainsi que la base dans laquelle les certificats et les LCR/LAR doivent être publiés. [2nd DIS ISO/IEC 11770-3 (08/1997)].

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

Liste de Certificats Révoqués (LCR) : liste signée numériquement par une AC et qui contient des identités de certificats déclarés invalides avant leur date de fin de validité (inscrite dans le certificat) ou qui ne sont plus dignes de confiance. 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. Quand la liste contient uniquement des certificats d'AC, le terme Liste des Autorités Révoquées (LAR) est utilisé.

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), utilisée pour conserver et mettre en œuvre la clé privée d'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 5280]. En dehors de cette période (avant la date de début de validité et après la date de fin de validité), le certificat est réputé non valide.

Plan de secours (après sinistre) : plan défini par une AC pour remettre en place tout ou partie de ses services d'IGC 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/LAR : 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 de Certification (PC) : ensemble de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications possédant des exigences de sécurité communes. [ISO/IEC 9594-8; ITU-T X.509].

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 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.

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

Révocation : procédure d'opposition à l'encontre du certificat qui a pour objet de supprimer la garantie d'engagement de l'AC avant la fin de la période de validité. Cette révocation est mise en œuvre à la demande de l'une des parties selon des modalités spécifiques.

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

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 certification (AC) 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 et la vérification de la chaine de certification. La validation d'un certificat électronique nécessite au préalable d'approuver le certificat de l'autorité Racine (certificat auto-signé).

I.6.2. Abréviations

AAI	Autorité Administrative INCS
AC	Autorité de Certification
ACF	Autorité de Certification Fille
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
ANSSI	Agence Nationale de la Sécurité des Systèmes d'information
CMS	*Credentials Management System*
DPC	Déclaration des Pratiques de Certification
HSM	*Hardware Security Module*
ICD	*International Code Designator*
IGC	Infrastructure de Gestion de Clés
INCS	Imprimerie Nationale Continu et Services (entité juridique du Groupe Imprimerie Nationale responsable de l'IGC)
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization*
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
LDAP	*Lightweight Directory Access Protocol*
LRAR	Lettre recommandée avec accusé de réception
MC	Mandataire de Certification
OID	*Object Identifier*
PC	Politique de Certification
OSC	Opérateur de Services de Certification
RL	Responsable légal
RSA	Rivest Shamir Adleman
SHA-256	*Secure Hash Algorithm 256*
SP	Service de Publication
UC	Utilisateur de certificat

II. Responsabilités concernant la mise à disposition des informations devant être publiées

II.1. ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

Le service de publication (SP) est en charge de la publication des données devant être publiées à destination des Porteurs de certificats, et des Utilisateurs de certificats (UC).

II.2. INFORMATIONS DEVANT ETRE PUBLIEES

L'AC publie à destination des Porteurs de certificats et des Utilisateurs de certificats (UC) :

- La présente PC : http://www.imprimerienationale.fr/GIN/PC
- Les Conditions Générales d'Utilisation des Services de certifications de l'IGC : http://www.imprimerienationale.fr/GIN/CGU/Conditions Générales d'Utilisation certificats non qualifiés.pdf
- Les différents formulaires nécessaires pour les demandes de révocation :
  - Formulaire de demande de révocation d'un porteur : http://www.imprimerienationale.fr/GIN/CGU/PASSIN Formulaire de demande de révocation d'un certificat porteur non qualifié.pdf
  - Formulaire de demande de révocation d'un MC : http://www.imprimerienationale.fr/GIN/CGU/Révocation du Mandataire de certification non qualifié.pdf
- Les certificats en cours de validité de l'ACR Imprimerie Nationale Élémentaire et de l'ACF :
  - Certificats de la chaîne de confiance : http://www.imprimerienationale.fr/GIN/AC/AC-EL-C.p7b
  - Certificat ACR Imprimerie Nationale Élémentaire : http://www.imprimerienationale.fr/GIN/ACR-EL-P.cer
  - Certificat AC Imprimerie Nationale Élémentaire Chiffrement : http://www.imprimerienationale.fr/GIN/ACF-EL-C.cer
- La Politique de Certification de l'ACR Imprimerie Nationale Élémentaire : http://www.imprimerienationale.fr/GIN/PC
- Les listes d'autorités révoquées (LAR) :
  - http://www.imprimerienationale.fr/GIN/CRL/AC-EL-P.crl
  - http://crl.imprimerienationale.fr/GIN/AC-EL-P.crl
- Les listes des certificats révoqués (LCR) :
  - http://www.imprimerienationale.fr/GIN/CRL/cert/ACF-EL-C.crl
  - http://crl.imprimerienationale.fr/GIN/cert/ACF-EL-C.crl

L'état de révocation des certificats (serveur OCSP) : http://ocsp-ac-el-c.imprimerienationale.fr

Sauf indications contraires, les autres informations sont réputées confidentielles.

En particulier, INCS ne publie pas les détails relatifs à ses pratiques (version complète de la PDC).

La consultation de la DPC est soumise à l'autorisation de l'AC. Elle doit faire l'objet d'une demande argumentée auprès de l'AC.

Les Conditions Générales d'Utilisation décrivent entre autres :

- Les conditions d'usage des certificats et leurs limites
- L'identifiant (OID) de la PC applicable
- Les obligations et responsabilités des différentes parties, notamment les exigences relatives à la vérification du statut de révocation d'un certificat pour les Utilisateurs

II.3. DELAIS ET FREQUENCE DE PUBLICATION

Toute nouvelle version de la présente PC est publiée sur le site du Groupe Imprimerie Nationale dans les 48 heures ouvrées après sa date de mise à jour et sa validation par l'AAI. Les formulaires de demande, les Conditions Générales d'Utilisation sont publiés dès que nécessaire afin que soit assurée la cohérence entre les informations publiées et les engagements et pratiques effectifs de l'AC.

Ces informations sont accessibles sur le site les jours ouvrés.

Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux § IV.9 et § IV.10

Les certificats d'AC et les informations permettant aux Utilisateurs de certificats de s'assurer de l'origine des certificats émis par l'AC Imprimerie Nationale Élémentaire Chiffrement sont diffusés préalablement à toute diffusion de certificats de Porteurs et/ou de LAR/LCR correspondantes.

Les systèmes publiant ces certificats sont accessibles 7j/7 et 24h/24.

II.4. CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées à destination des Utilisateurs de certificats est libre d'accès en lecture et protégé contre les modifications non autorisées.

L'accès en modification aux systèmes de publication des informations d'état des certificats s'effectue au travers une authentification (à 2 facteurs).

L'accès en modification aux systèmes de publication des autres informations s'effectue au travers une authentification de type ID-Mot de passe basé sur une politique de gestion stricte des mots de passe.

III. Identification et authentification

III.1. NOMMAGE

III.1.1. Type de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.

Dans chaque certificat X.509, l'émetteur (champ « *issuer* ») et le Porteur (champ « *subject* ») sont identifiés par un DN (*Distinguished Name*) de type X.501.

III.1.2. Utilisation de noms explicites

Le DN du champ *issuer* des certificats émis par l'AC Imprimerie Nationale Élémentaire Chiffrement identifie cette ACF.

Attributs du DN	Nom de l'attribut	Valeur
CN	*commonName*	AC Imprimerie Nationale Élémentaire Chiffrement
OU	*organizationalUnitName*	ICD + N° SIRET INCS : 0002 41049449600046
O	*organizationName*	Groupe Imprimerie Nationale
C	*countryName*	FR

Remarque :

L' ICD '0002' correspond au Système Informatique pour le Répertoires des Entreprises et des Établissements (SIRENE).

Le DN du champ *subject* des certificats émis par l'AC Imprimerie Nationale Élémentaire Chiffrement permet d'identifier le Porteur du certificat.

Attributs du DN	Nom de l'attribut	Valeur
CN	CN	Prénom et Nom de l'état civil du Porteur
SN	Surname	Nom du porteur **(attribut optionnel)**
GN	Givenname	Prénom du porteur **(attribut optionnel)**
SerialNumber	SerialNumber	numéro unique généré aléatoirement pour garantir l'unicité du DN et résoudre ainsi les cas d'homonymie
OI	OrganizationIdentifier	NTRFR-SIREN de l'Entité Cliente de rattachement du Porteur
OU	OrganizationUnit	0002 SIREN de l'Entité Cliente de rattachement du Porteur
O	Organization	Nom de l'Entité Cliente de rattachement du Porteur
C	Country	FR

NB : l'IN ne délivre des certificats qu'aux entités de droit français.

III.1.3. Anonymisation ou pseudonymisation des Porteurs

L'AC Imprimerie Nationale Élémentaire Chiffrement n'émet pas de certificat comportant une identité anonyme ou une identité pseudonyme.

III.1.4. Règles d'interprétation des différentes formes de nom

Les UC peuvent se servir des certificats d'AC contenus dans les chaînes de certification (voir § ci-dessus), pour mettre en œuvre et valider des fonctions de sécurité en vérifiant entre autres les identités (DN) des Porteurs incluses dans les certificats émis par l'AC Imprimerie Nationale Élémentaire Chiffrement.

III.1.5. Unicité des noms

Les identités portées par l'AC Imprimerie Nationale Élémentaire Chiffrement dans les certificats sont uniques au sein du domaine de certification de l'AC.

L'AC Imprimerie Nationale Élémentaire Chiffrement assure cette unicité par son processus d'enregistrement : un DN attribué à un Porteur ne peut être attribué à un autre Porteur.

L'attribut SerialNumber, contenant un numéro unique généré aléatoirement par une composante de l'IGC, est utilisé pour résoudre les cas d'homonymie (CN du certificat à émettre correspond au CN d'un certificat déjà émis pour deux personnes physiques distinctes).

L'extension *Subject Alternative Name* contenant l'adresse de courriel (RFC822) contribue également à identifier de manière univoque le titulaire du certificat.

L'unicité d'un certificat est basée sur l'unicité de son numéro de série au sein du domaine de l'AC. Ce numéro est propre au certificat et non pas au Porteur. Il ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un Porteur donné.

L'AC est responsable de l'unicité des noms de ses Porteurs et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

III.1.6. Identification, authentification et rôle des marques déposées

L'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par la communauté d'Utilisateur et les clients des marques déposées, des marques notoires et des signes distinctifs, ainsi que des noms de domaine.

III.2. VALIDATION INITIALE DE L'IDENTITE

III.2.1. Méthode pour prouver la possession de la clé privée

L'opération de génération de la bi-clé du Porteur est réalisée par l'AC (génération centralisée). Cette dernière assure l'attribution au Porteur de cette bi-clé en important la clé privée et le certificat de clé publique associé dans la carte qu'il possède.

III.2.2. Validation de l'identité d'une entité « personne morale » (entreprise ou administration)

La validation de l'identité d'une Entité Cliente de rattachement d'un Porteur est effectuée dans le cadre de l'enregistrement auprès de l'AE de l'une des personnes suivantes :

- Un responsable légal de cette Entité Cliente
- Un MC pour cette Entité Cliente

III.2.3. Validation de l'identité des personnes physiques

La validation initiale d'une personne physique est effectuée dans le cadre de l'enregistrement auprès de l'AE ou d'un MC de l'une des personnes suivantes :

- Un responsable légal (RL) de cette Entité Cliente (enregistrement par l'AE)
- Un MC pour cette Entité Cliente (enregistrement par l'AE)
- Un futur Porteur appartenant à cette Entité Cliente (enregistrement par un MC)

L'identité de la personne physique est vérifiée au travers du contrôle d'une pièce d'identité officielle (comportant une photo) en cours de validité (Carte Nationale d'Identité, Passeport, Carte de Séjour). L'identification des Porteurs est réalisée dans le cadre d'un face-à-face physique par l'AE ou le MC effectuant l'enregistrement.

Dans tous les cas, le porteur doit préalablement être en possession de certificats d'authentification et de signature, émis par l'*AC Imprimerie Nationale Élémentaire Personnel* sur un support physique. Ces certificats sont émis selon les politiques identifiées par les OID de la forme suivante : 1.2.250.1.295.1.1.10.1.1.*p.v*, où *p* vaut 101 ou 102, *v* est un entier supérieur ou égal à 1.

1. Enregistrement d'un RL

L'enregistrement d'un responsable légal est la première étape suivant l'établissement d'un contrat entre l'Entité Cliente dont il est responsable et INCS.

L'enregistrement d'un RL nécessite la validation par l'AE de l'identité « personne physique » du Porteur et de son statut de responsable légal vis-à-vis de l'Entité Cliente.

Le dossier d'enregistrement du RL doit comprendre :

- La demande de certificat écrite, datée de moins de trois mois, signée par le RL
- Les Conditions Générales d'Utilisation signées par le RL
- La photocopie d'une pièce d'identité officielle du RL en cours de validité, signée par le RL et annotée avec la mention « copie certifiée conforme à l'original »
- Des informations d'identification de l'Entité Cliente :

  Pour une entreprise :
  - Tout document attestant de la qualité du RL
  - Toute pièce, valide au moment de l'enregistrement, portant le numéro d'identification de l'Entité Cliente (extrait KBIS ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements, avis de situation juridique de l'INSEE) ou, à défaut, une autre pièce valide attestant l'identification unique de l'entreprise qui figurera dans le certificat

  Pour une administration :
  - Toute pièce, valide au moment de l'enregistrement, portant le numéro d'identification de l'Entité Cliente (avis de situation juridique de l'INSEE) ou, à défaut, une autre pièce valide attestant l'identification unique de l'administration qui figurera dans le certificat
  - Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative (les éventuelles délibérations, décrets et/ou arrêtés de nomination, désignation concernant l'autorité administrative)
- Des informations permettant de contacter le RL : courriel ou adresse postale, optionnellement n° téléphone

L'ensemble de ces documents est remis à l'AE.

2. Enregistrement d'un MC

L'enregistrement d'un MC nécessite la validation par l'AE de l'identité « personne physique » du MC, de son rattachement à l'Entité Cliente et de son rôle de MC.

Le dossier de demande d'enregistrement du MC doit comprendre :

- La demande écrite, datée de moins de trois mois, signée par le représentant légal (RL) de l'Entité Cliente et le MC
- Un mandat, daté de moins de trois mois, désignant le mandataire, signé par le RL et par le MC pour acceptation.
- Les Conditions Générales d'Utilisation signées par le MC
- Un engagement signé, daté de moins de trois mois, du futur MC à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs et à signaler à l'AE son départ de l'Entité Cliente
- La photocopie d'une pièce d'identité officielle du MC en cours de validité, signée par le MC et annotée avec la mention « copie certifiée conforme à l'original »
- Des informations permettant de contacter le MC : courriel ou adresse postale, optionnellement n° téléphone

L'ensemble de ces documents est remis à l'AE.

3. Enregistrement d'un Porteur via un MC

L'enregistrement d'un Porteur via un MC nécessite la validation par le MC de l'identité « personne physique » du Porteur et de son rattachement à l'Entité Cliente.

Le dossier de demande de certificat établi avec le MC doit comprendre :

- La demande de certificat AC Imprimerie Nationale Élémentaire Chiffrement mentionnant l'identité du Porteur, datée de moins de trois mois, co-signée par le Porteur et le MC.
- L'acceptation des Conditions Générales d'Utilisation par le Porteur

III.2.4. Informations non vérifiées du Porteur

Les certificats émis par l'AC Imprimerie Nationale Élémentaire Chiffrement ne contiennent aucune information non vérifiée à l'exception de l'UPN et de l'adresse électronique du porteur.

III.2.5. Validation de l'autorité du demandeur

La validation de l'autorité du demandeur (futur Porteur) est effectuée en même temps que la validation de l'identité de la personne physique, directement par l'AE ou par le MC.

III.2.6. Certification croisée d'AC

Ce point est sans objet dans la présente PC.

III.3. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES

III.3.1. Identification et validation pour un renouvellement courant

L'identification et la validation d'une demande de renouvellement des clés est réalisée en ligne en utilisant les certificats d'authentification et de signature, émis par l'*AC Imprimerie Nationale Élémentaire Personnel* et en cours de validité, en possession du Porteur.

Il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante, qui sera générée par l'AC.

III.3.2. Identification et validation pour un renouvellement après révocation

Les vérifications relatives au renouvellement d'une bi-clé après révocation du certificat sont effectuées conformément à la procédure de demande initiale de certificat (cf. § III.2 ci-dessus).

III.4. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

Les demandes de révocation d'un certificat donnent lieu à une vérification de l'identité du demandeur et à une vérification de son autorité par rapport au certificat à révoquer.

En particulier, les personnes ayant une autorité par rapport au certificat à révoquer sont :

- le Porteur du certificat à révoquer
- le responsable légal de l'Entité Cliente à laquelle appartient le Porteur
- un MC de l'Entité Cliente à laquelle appartient le Porteur

Si le demandeur est le Porteur, ce dernier est authentifié par le biais d'un jeu de Question-Réponse (5 minimum) à travers l'interface client du service en ligne.

Une demande de révocation peut être effectuée :

- en ligne :
  - par le MC ou le Représentant Légal authentifiés avec leur propre certificat ;
  - par le Porteur authentifié par son certificat ;
- par téléphone :
  - le demandeur est authentifié par un jeu de 5 Questions Réponses connues uniquement du demandeur ;
- par courrier :
  - la demande de révocation doit être signée par le demandeur et doit être accompagnée d'une photocopie d'une pièce d'identité officielle du demandeur. L'identité du demandeur est assurée par une vérification de la signature manuscrite par rapport à une signature manuscrite préalablement enregistrée. L'autorité du demandeur par rapport au certificat à révoquer est vérifiée par le service de révocation (seuls le Porteur, le MC et le Représentant Légal ont la possibilité de demander la révocation du Porteur du côté de l'Entité Cliente).
  - La demande peut être transmise par courrier postal ou par email.

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.1. DEMANDE DE CERTIFICAT

IV.1.1. Origine d'une demande de certificat

La demande de certificat AC Imprimerie Nationale Élémentaire Chiffrement émane du MC dûment mandaté par le représentant légal de l'Entité Cliente.

Le consentement préalable du futur Porteur est requis.

IV.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat

Le dossier de demande de certificat est établi par le RL ou par le MC. Ce dossier comporte, *a minima,* les informations suivantes :

- Le nom du futur Porteur à utiliser dans le certificat
- Les données personnelles d'identification du futur Porteur
- Les données d'identification de l'Entité Cliente (correspondant le cas échéant à l'Entité Cliente de rattachement du MC)

Ces données doivent être identiques à celles présentes dans les certificats déjà en possession du Porteur (cf. § III.2.3).

Le dossier contient les éléments décrits en III.2.3.

Dans le cas d'une demande concernant un RL (III.2.3.1) ou un MC (III.2.3.2), le dossier est transmis à l'AE par le demandeur ou en mains propres lors du face-à-face. Le dossier est signé par l'AE lors du face-à-face.

Dans le cas d'une demande pour un Porteur via un MC (III.2.3.3), le dossier de demande est transmis à l'AE par le MC. Le dossier est signé par le MC suite au face-à-face avec le Porteur.

Le dossier papier doit dans tous les cas être transmis dans le délai fixé par l'AE pour validation et pour archivage.

IV.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

IV.2.1. Exécution des processus d'identification et de validation de la demande

L'AE effectue les traitements suivants :

- Vérification du mandat du MC
- Vérification de l'identité du Porteur (identification « personne physique »)
- Vérification de l'identité de l'Entité Cliente (identification « personne morale »)
- Vérification de la cohérence des justificatifs fournis
- Vérification de l'acceptation des conditions générales d'utilisation par le Porteur

Le dossier de demande est conservé dans tous les cas par l'AE, même dans les cas d'une demande effectuée par un MC.

IV.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande de certificat, l'AE informe le Porteur, et le cas échéant le MC. La notification du rejet est effectuée par le biais de la fonction de suivi de l'application accessible en ligne. Le cas échéant, le Porteur peut être informé par le biais du MC.

En cas d'acceptation de la demande, le Porteur peut suivre l'évolution du traitement par l'AC (création éventuelle du support et génération de la bi-clé et du certificat associé).

IV.2.3. Durée d'établissement du certificat

Le certificat est produit dans les secondes suivant la validation de la demande.

IV.3. DELIVRANCE DU CERTIFICAT

IV.3.1. Action de l'AC concernant la délivrance du certificat

Suite à la validation de la demande par l'AE, l'AC déclenche le processus de génération et préparation des éléments destinés au Porteur : génération de la bi-clé et du certificat.

IV.3.2. Notification par l'AC de la délivrance du certificat au Porteur

Le certificat et la bi-clé associée sont directement injectés dans le support du Porteur, via un canal sécurisé.

IV.4. ACCEPTATION DU CERTIFICAT

IV.4.1. Démarche d'acceptation du certificat

L'acceptation du certificat par le Porteur s'effectue de manière explicite sous la forme d'un accord signé. Une fois le certificat et la bi-clé installée sur son support, le Porteur signe un PV d'acceptation du certificat et le retourne à l'AE qui le conservera.

Il est de la responsabilité du Porteur de vérifier la cohérence des informations portées dans le certificat (par exemple l'adresse email) avant toute utilisation.

En cas de refus explicite du certificat par le Porteur, ou en cas de non réception par l'AE de l'accord signé dans un délai de 40 jours après réception de la carte, le certificat est révoqué par l'AC.

L'accord signé est archivé avec le dossier d'enregistrement du Porteur.

IV.4.2. Publication du certificat

L'AC Imprimerie Nationale Élémentaire Chiffrement ne publie pas les certificats émis.

Néanmoins, les certificats émis par l'AC Imprimerie Nationale Élémentaire Chiffrement dans le cadre de cette PC peuvent être publiés dans des annuaires de messagerie tiers. Les conditions de cette publication ne sont pas du ressort de l'AC et sortent du cadre de la présente PC.

IV.4.3. Notification par l'AC aux autres Entités de la délivrance d'un certificat

Sans objet.

IV.5. USAGE DE LA BI-CLE ET DU CERTIFICAT

IV.5.1. Utilisation de la clé privée et du certificat par le Porteur

L'utilisation de la bi-clé du Porteur et du certificat associé est strictement limitée au service de chiffrement et de signature tel que défini en I.3. L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés : *key Usage* et *Extended Key Usage* (*cf.* VI.1.7 ci-dessous).

IV.5.2. Utilisation de la clé publique et du certificat par l'Utilisateur du certificat

L'utilisation d'un certificat Porteur par un UC est limitée aux conditions d'usage définies en I.3 et indiquées dans les extensions *Key Usage* et *Extended Key Usage* du certificat.

IV.6. RENOUVELLEMENT D'UN CERTIFICAT

Conformément au [RFC3647], la notion de « renouvellement de certificat » correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique).

Dans le cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante.

IV.7. DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE

IV.7.1. Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées, selon les recommandations émises par l'ANSSI en matière de cryptanalyse, afin de minimiser les possibilités d'attaques cryptographiques, Ainsi les bi-clés des Porteurs sont renouvelées au minimum tous les 3 ans.

Les bi-clés des Porteurs peuvent être renouvelées par anticipation, suite à la révocation du certificat du Porteur. Les différentes causes de révocation sont décrites en IV.9.1.1.

Le changement de bi-clé entraîne le changement de certificat.

IV.7.2. Origine d'une demande d'un nouveau certificat

La demande d'un nouveau certificat peut être à l'initiative du Porteur ou du MC le cas échéant.

Le Porteur et le MC sont alertés par e-mail de l'arrivée à échéance du certificat du Porteur au moins 1 mois avant la fin de validité du certificat du Porteur.

IV.7.3. Procédure de traitement d'une demande d'un nouveau certificat

La procédure de traitement de la demande de nouveau certificat est la suivante :

- Le MC s'authentifie sur le portail et accède à la liste des Porteurs qu'il gère ;
- Si le certificat du Porteur est en période de renouvellement, le portail lui propose son renouvellement. Le MC vérifie que les informations du Porteur sont toujours valides et accepte le renouvellement du certificat du Porteur
- Le Porteur est notifié de la demande de renouvellement ;
- Le Porteur s'authentifie sur le portail et accède à ses informations et la demande de renouvellement en cours ;

- Si le Porteur accepte le renouvellement, un récapitulatif des informations du certificat à renouveler lui est présenté ;
- Le Porteur signe électroniquement sa demande de renouvellement et les CGU ;
    - Le cas échéant, le porteur peut mettre à jour son adresse e-mail (en cas de changement, une confirmation de cette adresse sera nécessaire avant de pouvoir procéder au renouvellement).
- Le Porteur procède à la génération de sa bi-clé et de son certificat auprès de l'AC ;

Le renouvellement de certificat en ligne utilise un canal sécurisé entre l'AC et le support du Porteur. Ce canal garantit l'intégrité et la confidentialité des données échangées entre l'AC et le support.

IV.7.4. Notification au Porteur de l'établissement du nouveau certificat

Le Porteur effectue le renouvellement lui-même et est par conséquent directement notifié par l'AC.

IV.7.5. Démarche d'acceptation du nouveau certificat

L'acceptation du certificat par le Porteur s'effectue de manière explicite sous la forme d'un accord signé électroniquement.

IV.7.6. Publication du nouveau certificat

Voir chapitre IV.4.2.

IV.7.7. Notification par l'AC aux autres Entités de la délivrance du nouveau certificat

Voir chapitre IV.4.3

IV.8. MODIFICATION DU CERTIFICAT

Conformément au [RFC 3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique et autres qu'uniquement la modification des dates de validité.

Cette opération n'est pas autorisée par la présente PC. En cas de modification d'informations, un nouveau certificat doit être délivré avec génération d'une nouvelle bi-clé et révocation de l'ancien certificat.

IV.9. REVOCATION ET SUSPENSION DES CERTIFICATS

IV.9.1. Causes possibles d'une révocation

1. Certificat Porteur

Les causes de révocations d'un certificat Porteur sont les suivantes :

- compromission, suspicion de compromission, vol, perte de la clé privée
- vol, perte ou dysfonctionnement irréversible du support
- les informations du Porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant la fin de validité du certificat
- non-respect par le Porteur des modalités applicables d'utilisation du certificat
- non-respect par le Porteur ou le MC de leurs obligations découlant de la PC
- erreur détectée dans le dossier d'enregistrement
- non acceptation du certificat par le Porteur après sa délivrance
- le porteur ou une entité autorisée (représentant légal de l'Entité ou MC par exemple) demande la révocation

du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du Porteur et/ou de son support) ;
- décès du Porteur, départ de l'Entité Cliente, cessation d'activité de l'Entité Cliente
- révocation du certificat de l'AC

2. Certificat d'une composante de l'IGC

Les causes de révocations d'un certificat d'une composante de l'IGC sont les suivantes :
- cessation d'activité de l'entité opérant la composante,
- compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de la composante (perte du secret principal, perte du code d'activation et perte de plus de deux secrets partagés),
- non-respect de la politique de certification et de la déclaration des pratiques de certification de l'ACF (détecté lors d'un audit de qualification ou de conformité négatif),
- changement de composante de l'IGC
- obsolescence de la cryptographie au regard des exigences de l'ANSSI (nécessitant renouvellement de la bi-clé de l'AC).

IV.9.2. Origine d'une demande de révocation

1. Certificat Porteur

Les personnes autorisées à demander la révocation d'un certificat Porteur sont les suivantes :
- Le Porteur du certificat au nom duquel le certificat a été émis
- Le cas échéant, un MC de l'Entité Cliente à laquelle est rattaché le Porteur
- Le Responsable Légal de l'Entité Cliente à laquelle est rattaché le Porteur
- L'AC émettrice du certificat ;
- Une composante de l'AC (l'AE) ;

2. Certificat d'une composante de l'IGC

La révocation de l'AC Imprimerie Nationale Élémentaire Chiffrement ne peut être décidée que par l'entité responsable de l'AC ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui en informe l'AC sans délai.

IV.9.3. Procédure de traitement d'une demande de révocation

1. Certificat Porteur

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre III.4.

Une demande de révocation peut être déposée :
- En se connectant sur le portail web. Le demandeur est authentifié par certificat ou par un jeu de Questions Réponses.
- En contactant le service révocation de l'Imprimerie Nationale par téléphone ou par email.
- Par courrier postal auprès du service révocation de l'Imprimerie Nationale.

Les informations suivantes figurent, a minima, dans la demande de révocation de certificat :
- Identité du Porteur du certificat à révoquer
- Identité du demandeur

- Information permettant d'identifier de façon univoque le certificat à révoquer (n° série, …)
- La cause de révocation

Une fois la demande authentifiée et contrôlée, le service de révocation révoque le certificat correspondant et communique le nouveau statut du certificat au service d'information sur l'état des certificats.

Le demandeur, le Porteur (si celui-ci n'est pas le demandeur) ainsi que l'Entité Cliente du Porteur (directement ou via son ou ses MC) sont informés de la révocation du certificat du Porteur.

2. Certificat d'une composante de l'IGC

Les procédures de révocation de certificat d'une composante de l'IGC sont décrites dans la documentation interne de l'AC Imprimerie Nationale Élémentaire Chiffrement.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC Imprimerie Nationale Élémentaire Chiffrement informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides.

IV.9.4. Délai accordé au Porteur pour formuler la demande de révocation

Le Porteur doit demander sans délai la révocation de son certificat dès lors qu'une cause de révocation telle que définie en IV.9.1 est identifiée. À défaut, la demande doit être formulée par le RL ou un des MC rattachés à l'Entité Cliente à laquelle est rattaché le Porteur.

IV.9.5. Délai de traitement par l'AC d'une demande de révocation

1. Certificat Porteur

L'AC traite les demandes de révocation dès que possible suivant sa réception, de préférence immédiatement, et dans un délai inférieur à 72 h. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des Utilisateurs.

La disponibilité du service de révocation est assurée les jours et horaires ouvrés.

L'AC garantit une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de la fonction de gestion des révocations de 1 heure et une durée maximale totale d'indisponibilité de 4 heures par mois.

2. Certificat d'une composante de l'IGC

La révocation du certificat d'une composante de l'IGC est effectuée immédiatement dès la détection d'un évènement décrit dans les causes de révocation possibles.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR) est effectuée immédiatement en particulier en cas de compromission de la clé privée.

IV.9.6. Exigences de vérification de la révocation par les Utilisateurs du certificat

L'Utilisateur d'un certificat de Porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LAR/LCR, OCSP…) est à l'appréciation de l'Utilisateur selon leur disponibilité et les contraintes liées à son application.

IV.9.7. Fréquence d'établissement des LCR

La durée de validité de la LCR est de 4 jours.

Par conséquent, une nouvelle LCR est générée et publiée au moins toutes les 24 heures. L'AC ne met en œuvre le mécanisme de delta LCR. En cas de révocation d'un certificat Porteur, la LCR est immédiatement générée et publiée.

IV.9.8. Délai maximum de publication d'une LCR

Après avoir été générée, la LCR est publiée dans un délai maximum de 30 minutes.

IV.9.9. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

L'AC Imprimerie Nationale Élémentaire Chiffrement dispose d'un répondeur OCSP accessible à l'adresse http://ocsp-ac-el-c.imprimerienationale.fr, en complément de la publication des LCR en ligne. Ce service répond aux exigences d'intégrité, de disponibilité et de délai de publication décrites dans la présente PC.

Le temps de réponse du répondeur OCSP à une requête de demande de statut est inférieur à 10 secondes.

IV.9.10. Exigences de vérification en ligne de la révocation des certificats par les Utilisateurs de certificats

Voir § IV.9.6.

IV.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet

IV.9.12. Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de Porteur, les entités autorisées à effectuer une demande de révocation sont tenues de le faire sans délai après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, l'information de révocation suite à la compromission de la clé privée sera relayée sur le site Groupe Imprimerie Nationale et éventuellement par d'autres moyens (autre sites institutionnels, presse, etc.)

IV.9.13. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC.

IV.10. FONCTIONS D'INFORMATION SUR L'ETAT DES CERTIFICATS

IV.10.1. Caractéristiques opérationnelles

Le service d'information de l'état des certificats, mis à la disposition des Utilisateurs de certificats, dispose d'un mécanisme de consultation libre de la LCR et de la LAR. Les listes de révocation LCR et LAR sont au format V2, publiées en http aux adresses référencées au § II.2.

Le statut des certificats est également accessible en ligne via le répondeur OCSP via l'adresse référencée aux § II.2 et IV.9.9.

IV.10.2. Disponibilité de la fonction

Le service d'information sur l'état des certificats est disponible 24h/24 et 7j/7. Ce service a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2 heures et une durée maximale totale d'indisponibilité par mois de 8 heures.

IV.10.3. Dispositifs optionnels

Ce point est sans objet dans la présente PC.

IV.11. FIN DE LA RELATION ENTRE LE PORTEUR ET L'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC Imprimerie Nationale Élémentaire Chiffrement et le Porteur avant la fin de validité de son certificat, pour une raison ou une autre, ce certificat est révoqué.

IV.12. SEQUESTRE DE CLES ET RECOUVREMENT

Les clés d'AC ne sont, en aucun cas, séquestrées.

IV.12.1. Séquestre de clés

La demande de séquestre de clé privée est effectuée auprès de l'AE conjointement à la demande du certificat correspondant, par le Porteur lui-même.

1. Traitement d'une demande de séquestre

Une demande de séquestre d'une clé privée étant formulée en même temps et par la même personne que la demande de certificat correspondant, le processus d'identification et de validation d'une telle demande correspond à celui d'une demande de certificat.

L'AE transmet ensuite la demande de séquestre à la fonction adéquate de l'IGC.

Suite à la génération de la bi-clé de chiffrement du Porteur, la fonction de génération des éléments secrets du porteur transmet la clé à séquestrer à la fonction de séquestre et recouvrement suivant un processus qui en assurer, de bout en bout, la confidentialité, l'intégrité et l'authentification d'origine.

IV.12.2. Recouvrement

1. Origine d'une demande de recouvrement

Outre le porteur lui-même et les entités autorisées par la loi à accéder aux clés privées séquestrées par une AC, la présente PC n'autorise aucune autre Entité à effectuer une demande de recouvrement.

2. Identification et validation d'une demande de recouvrement

Les vérifications relatives au recouvrement d'une bi-clé sont effectuées conformément à la procédure de demande initiale de certificat (cf. § III.2 ci-dessus).

La clé à recouvrer est identifiée dans la demande de recouvrement en utilisant l'empreinte *(fingerprint)* du certificat associé.

3. Traitement d'une demande de recouvrement

Suite à identification et validation de la demande de recouvrement, la fonction de gestion des recouvrements émet la demande pour effectuer le recouvrement de la clé privée concernée vers la fonction de séquestre et recouvrement de l'IGC, en protégeant cette demande en intégrité et en confidentialité.

La fonction de séquestre et recouvrement authentifie la demande de recouvrement puis saisit les personnes nécessaires pour le recouvrement de la clé privée du porteur. La fonction de séquestre et recouvrement authentifie ces personnes préalablement à l'opération de recouvrement.

L'opération de recouvrement garantit qu'aucune information, autre que la clé privée sur laquelle porte le recouvrement, ne peut être divulguée.

La clé privée recouvrée et le certificat associé sont transmis au demandeur selon le même processus que la délivrance d'une bi-clé et d'un certificat lors d'une demande initiale.

IV.12.3. Destruction des clés séquestrées

Les clés séquestrées sont conservées durant toute la durée de vie de l'AC et seront détruites de manière fiable dans le cadre de la procédure de fin de vie de celle-ci.

IV.12.4. Disponibilité des fonctions liées au séquestre et au recouvrement

La présente PC ne formule aucun engagement sur le sujet.

V. Mesures de sécurité non techniques

V.1. MESURES DE SECURITE PHYSIQUES

V.1.1. Situation géographique et construction des sites

Les sites d'exploitation de l'IGC respectent les règlements et normes en vigueur ainsi qu'éventuellement des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques, ...).

V.1.2. Accès physique

Les moyens et informations de l'IGC utilisés dans le cadre de sa mise en œuvre sont installés dans une salle d'exploitation dont les accès sont contrôlés et réservés aux seules personnes habilitées.

Le système de contrôle des accès permet de garantir la traçabilité des accès aux zones où sont hébergées les IGC. En dehors des heures ouvrables, la sécurité est garantie par la mise en œuvre de moyens de détection d'intrusion physique et logique. Si des personnes non habilitées doivent pénétrer dans les salles d'exploitation, elles sont prises en charge par une personne habilitée qui en assure la surveillance. Ces personnes sont accompagnées en permanence par des personnels habilités.

Les machines sont installées dans un périmètre de confiance qui permet de respecter la séparation des rôles de confiance telles que prévue dans la présente PC. Ce périmètre de sécurité garantit que les fonctions et informations hébergées sur les machines ne sont accessibles qu'aux seules personnes ayant des rôles de confiance reconnus et autorisés. Ces points sont précisés dans la DPC.

V.1.3. Alimentation électrique et climatisation

Des systèmes de protection de l'alimentation électrique et de génération d'air conditionné sont mis en œuvre afin d'assurer la disponibilité et la continuité des services délivrés, en particulier le service de gestion des révocations et le service d'information sur l'état des certificats.

Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et ou constructeurs.

V.1.4. Vulnérabilité aux dégâts des eaux

Les systèmes sont implantés de telle manière qu'ils ne sont pas sensibles aux inondations et autres projections et écoulements de liquides.

V.1.5. Prévention et protection incendie

Afin d'assurer la disponibilité des systèmes informatiques de l'IGC, des systèmes de génération et de protection des installations électriques sont mis en œuvre. Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC telles que définies par leurs fournisseurs.

V.1.6. Conservation des supports

Les différentes informations intervenant dans les activités de l'IGC sont identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité). L'AC maintient un inventaire de ces informations et a mis en place des mesures pour éviter la compromission et le vol de ces informations.

En particulier, les supports (papier, disque dur, clés USB, CD, etc.) de ces informations sont gérés conformément aux besoins de sécurité définis : protection contre le vol, dommages et accès non autorisés…

Les précisions quant aux modalités de conservation de ces supports sont fournies dans la DPC.

V.1.7. Mise hors service des supports

Les supports d'informations sont détruits en fin de vie.

Les procédures et moyens de destruction sont conformes au niveau de confidentialité des informations correspondantes.

V.1.8. Sauvegardes hors site

L'opérateur réalise des sauvegardes hors site permettant une reprise rapide des services d'IGC, suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ses services, en conformité aux engagements de l'AC en termes de disponibilité, en particulier pour les services de gestion des révocations et d'informations sur l'état des certificats.

Les informations sauvegardées hors site respectent les exigences de la présente PC en matière de protection en confidentialité et intégrité de ces informations.

Les fonctions de sauvegarde et de restauration sont assurées par les rôles de confiance ad-hoc conformément aux mesures de sécurité procédurales.

Les précisions quant aux modalités des sauvegardes des informations sont fournies dans la DPC.

V.2. MESURES DE SECURITE PROCEDURALES

V.2.1. Rôles de confiance

Les personnes doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité. Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflits d'intérêts préjudiciables à l'impartialité des opérations au sein de l'IGC.

Les rôles de confiance de l'AC sont classés en 5 groupes :

- Le responsable de sécurité - Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes. 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.
- Le responsable d'application - Le responsable d'application est chargé, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- Le responsable d'exploitation – Le responsable d'exploitation assure le maintien des systèmes en conditions opérationnelles de fonctionnement. Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes

et des réseaux de la composante.

- L'opérateur - Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- Le contrôleur ou auditeur – son rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournie par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification et aux politiques de sécurité de la composante. L'auditeur est désigné par l'AAI.

En plus de ces rôles de confiance, l'AC a défini le rôle de Porteur de part de secret. Le Porteur de part de secret a la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité de la part qui lui a été confiée.

V.2.2. Nombre de personnes requises par tâches

Le nombre et le type de rôles et de personnes devant nécessairement être présentes (en tant qu'acteurs ou témoins) peuvent être différents suivant le type d'opérations effectuées.

Pour des raisons de disponibilité, chaque tâche doit pouvoir être effectuée par au moins deux personnes.

Les fonctions sensibles (par exemple les cérémonies de clé) sont réparties sur plusieurs personnes pour des questions de sécurité. La DPC précise le nombre de personnes nécessaires à chaque opération.

V.2.3. Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle,
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes,
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes,
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

Ces contrôles sont décrits dans la DPC de l'AC et sont conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC doit être notifiée par écrit. Ce rôle doit être clairement mentionné et décrit dans sa fiche de poste.

V.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 de non cumul doivent être respectées. Les attributions associées à chaque rôle sont décrites dans la DPC de l'AR et sont conformes à la politique de sécurité de la composante concernée.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et responsable d'exploitation / opérateur,
- contrôleur et tout autre rôle,
- responsable d'exploitation et opérateur.

V.3. MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

V.3.1. Qualifications, compétences et habilitations requises

Chaque personne amenée à travailler au sein de l'AC 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 certification de l'IGC est informée de ses responsabilités relatives aux services de l'IGC et des procédures liées à la sécurité du système et au contrôle du personnel.

Le personnel d'encadrement possède l'expertise approprié et est familier des procédures sécuritaires.

V.3.2. Procédures de vérification des antécédents

L'AC 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 (salarié hors période d'essai), il est notamment vérifié que chaque personne n'a pas fait l'objet de condamnation de justice (extrait B3 du casier judiciaire) en contradiction avec leurs attributions.

Les personnes doivent faire l'objet d'une habilitation spécifique (avec des dispositions dans leur contrat de travail) et leur mission doit être définie par rapport à leur besoin d'en connaître.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

V.3.3. Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère. Les personnels ont connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

V.3.4. Exigences et fréquences en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

V.3.5. Fréquence et séquence de rotation entre différentes attributions

La fréquence et la séquence de rotation entre les différentes attributions sont précisées dans la DPC correspondante à cette PC.

V.3.6. Sanctions en cas d'actions non autorisées

Des sanctions en cas d'actions non autorisées par les politiques et procédures établies par la PC et les processus et procédures internes à l'IGC, soit par négligence, soit par malveillance, sont prévues. Ces sanctions sont précisées dans la DPC.

V.3.7. Exigences vis-à-vis du personnel de prestataires externes

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC respecte également les exigences du présent § V.3. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires.

V.3.8. Documentation fournie au personnel

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, il lui est remis la ou les politique(s) de sécurité qui le concerne(nt).

V.4. PROCEDURES DE CONSTITUTION DES DONNEES 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.

V.4.1. Types d'événements à enregistrer

Chaque composante opérant une composante de l'IGC journalise, au minimum, les événements tels que décrit ci-dessous sous forme électronique. La journalisation est automatique depuis le démarrage du système et sans interruption jusqu'à son arrêt.

- 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,
- Événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à la défaillance de la fonction de journalisation,
- Connexion / déconnexion des Utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes,

1. Informations enregistrées pour chaque évènement

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

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

Suivant le type d'événement 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'événement,
- Toute information caractérisant l'événement (par exemple pour la génération d'un certificat, son numéro de série).

Les opérations de journalisation sont effectuées au cours du processus concerné. En cas de saisie manuelle, l'écriture s'effectue, sauf exception, le jour même jour ouvré que l'événement.

2. Événements enregistrés par l'AE

Les évènements enregistrés par l'AE sont les suivants :

- Réception d'une demande de certificat (initiale et renouvellement),
- Validation / rejet d'une demande de certificat,
- Envoi du SSCD au Porteur et accusé de réception,
- Acceptation ou rejet explicite par le Porteur,
- Activation du support par le Porteur,
- Réception d'une demande de révocation,
- Validation / rejet d'une demande de révocation,

3. Événements enregistrés par l'AC

Les évènements enregistrés par l'AC sont les suivants :

- Événements liés aux clés de signature et aux certificats d'AC (génération, sauvegarde / récupération, recouvrement, destruction, …),
- Génération des bi-clés des Porteurs,
- Génération des certificats des Porteurs,
- Personnalisation des supports et génération des codes d'activation,
- Publication et mise à jour des informations liées aux AC (PC, certificats d'AC, CGU, etc.)
- Génération puis publication des LCR,
- Requêtes et réponses OCSP.

4. Événements divers

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, mots de passe ou code Porteur, …).

5. Imputabilité

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'événements.

V.4.2. Fréquence de traitement des journaux d'événements

Les journaux d'événements sont contrôlés et analysés par un responsable de sécurité afin d'identifier les anomalies liées à des tentatives en échec suivant la fréquence définie au § V.4.8.

V.4.3. Période de conservation des journaux d'événements

Les journaux d'évènements sont conservés sur site pendant au moins 5 ans. Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous 1 mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

V.4.4. Protection 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).

Les systèmes générant les journaux d'événements (exceptés les systèmes de contrôle d'accès physique) sont synchronisés sur une source fiable de temps UTC (cf. § VI.8).

V.4.5. Procédure de sauvegarde 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 associe à toutes les archives une date de génération des archives.

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

V.4.6. Système de collecte des journaux d'événements

Le système de collecte des journaux peut être interne ou externe aux composantes de l'IGC. Le système assure la collecte des archives en respectant le niveau de sécurité relatif à l'intégrité, la disponibilité et la confidentialité des données.

V.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement

Sans objet.

V.4.8. Évaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont contrôlés au moins 1 fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité 1 fois par jour et dès la détection d'une anomalie. Cette analyse donne lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de l'AE et de l'AC est effectué au moins 1 fois par semaine, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

V.5. ARCHIVAGE DES DONNEES

L'archivage des données doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC. Il doit aussi permettre la conservation des données papier liées aux opérations de certification.

V.5.1. Types de données à archiver

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

- Logiciels et fichiers de configuration de chaque composante,
- La politique de certification (PC),
- La déclaration des pratiques de certification (DPC),
- Les certificats et LCR tels qu'émis ou publiés,
- Les dossiers d'enregistrement des MC,
- Les dossiers de demande de certificats comprenant les justificatifs d'identité des Porteurs, le cas échéant de leur entité de rattachement,
- Les journaux d'événements des différentes composantes de l'IGC.

V.5.2. Période de conservation des archives

1. Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable. En l'occurrence, il est archivé pendant au moins cinq ans, comptés au maximum à partir de l'acceptation du certificat par son Porteur.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat peut être présenté par l'AC lors de toute sollicitation par les autorités habilitées. Ce dossier, complété par les mentions consignées par l'AE ou le MC, doit permettre de retrouver l'identité réelle de la personne physique désignée dans le certificat émis par l'AC.

2. Dossiers de demande de recouvrement

Tout dossier de demande de recouvrement accepté doit être archivé pendant au moins cinq ans, comptés à partir de la fin du séquestre par l'AC de la clé privée correspondante.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de recouvrement doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées. Ce dossier, complété par les mentions consignées par l'AE ou le MC, doit permettre de retrouver l'identité réelle de la personne physique ayant demandé et obtenu le recouvrement.

3. Certificats et LCR émis par l'AC

La période de conservation des certificats et des LCR émis par l'AC, ainsi que celle des certificats d'AC et des LAR est de 5 ans après leur expiration.

4. Journaux d'événements

Les journaux d'événements tels que traités au § V.4 est de 5 ans après leur génération.

V.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives :

- Sont protégées en intégrité,
- Sont accessibles aux seules personnes autorisées,
- Peuvent être relues ou exploitées,
- Sont auditées et testées régulièrement (accès, lisibilité, exploitation et l'absence de déformation de formats selon les supports d'archivage)

V.5.4. Procédure de sauvegarde des archives

L'opérateur technique et l'AC ont pour responsabilité de mettre en place et maintenir les mesures requises afin d'assurer l'intégrité et la disponibilité des archives tel qu'exigé dans la présente PC.

V.5.5. Exigences d'horodatage des données

Le § VI.8 précise les exigences en matière de datation et d'horodatage.

V.5.6. Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité des archives tel qu'exigé au § V.5.3.

V.5.7. Procédure de récupération et de vérification des archives

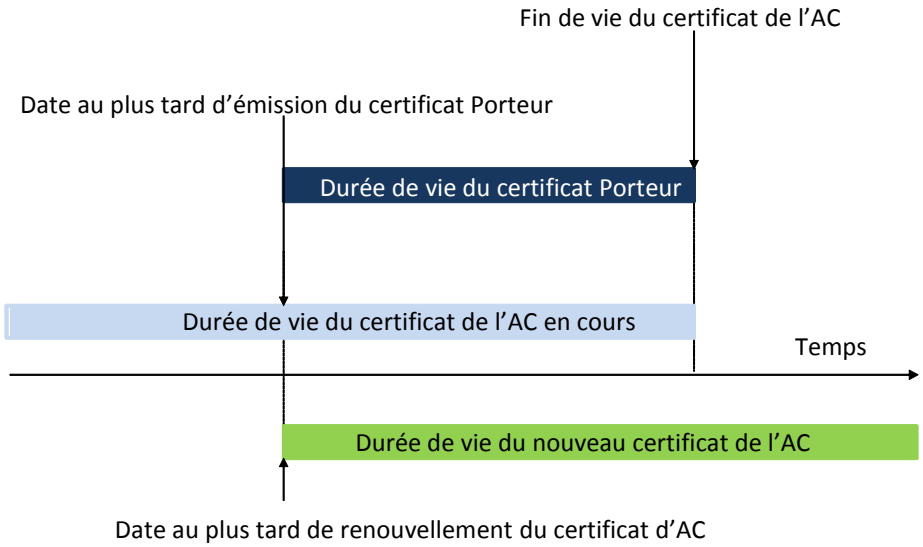
Les archives papier ou électronique doivent pouvoir être récupérées par l'ACF dans un délai de 2 jours ouvrés.

V.6. CHANGEMENT DE CLE D'AC

La durée de vie du 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 les recommandations des autorités nationale ou internationale compétentes en la matière.

L'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 de l'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 de l'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.

V.7. REPRISE SUITE A COMPROMISSION ET SINISTRE

V.7.1. Procédure de remontée et de traitement des incidents et des compromissions

Chaque entité agissant pour le compte de l'IGC met en œuvre des procédures de remontée d'incident et de traitement des incidents. Ceci est réalisé au travers de la sensibilisation et la formation des personnels et au travers de l'analyse des journaux d'événements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui en informe immédiatement l'AC. Le cas de l'incident majeur est impérativement traité dès réception et la publication de l'information de révocation du certificat, s'il y a lieu, est faite dans la plus grande urgence, voire immédiatement, par tout moyen utile ou disponible. Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses Porteurs devient insuffisant pour son utilisation prévue restante, alors l'AC informe tous les Porteurs et les tiers Utilisateurs de certificats avec lesquels l'AC a passé des accords. De plus tous les certificats concernés sont révoqués.

V.7.2. Procédure en cas de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)

Chaque composante de l'IGC dispose d'un plan de continuité d'activité et de service qui permet de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC, des engagements de l'AC en ce qui concerne les fonctions liées à la publication et à la révocation des certificats.

Ce plan de continuité est testé au moins une fois par an et les mesures correctives, le cas échéant, sont mises en place.

V.7.3. Procédure en cas de compromission de la clé privée d'une composante

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant est immédiatement révoqué comme précisé au § IV.9. De plus, l'AC respecte les engagements suivants :

- Informer sans délai: tous les Porteurs, les Entités Clientes avec lesquelles l'AC a passé des accords et les Utilisateurs,
- Indiquer sans délai que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.
- Le cas échéant procéder à un dépôt de plainte auprès des autorités compétentes.

V.7.4. Capacité de continuité d'activité en cas de sinistre

Les différentes composantes de l'IGC disposent des moyens (techniques, organisationnels et humains) nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC (cf. § V.7.2).

V.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.

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 nouvelle entité garantit un niveau de confiance adéquat, le maintien des garanties financières ainsi qu'une continuité de service (notamment archivage, maintien de la confidentialité, interopérabilité des certificats, etc.).

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. Ainsi, les certificats émis seront révoqués sans délai et les entités informées de la révocation des certificats.

En cas de transfert d'activité, l'AC préviendra les Porteurs de certificats dans le cas où les changements envisagés peuvent avoir des répercussions sur les engagements pris et ce, au moins, sous le délai d'un mois. De même, elle effectuera une information auprès des autorités administratives. En particulier, les contacts auprès de la SGMAP et de l'ANSSI seront avertis.

VI. Mesures de sécurité techniques

VI.1. GENERATION ET INSTALLATION DE BI-CLES

VI.1.1. Génération des bi-clés

1. Clé de l'AC

La génération des bi-clés associées au certificat d'AC se déroule lors d'une cérémonie de clés à l'aide d'une ressource cryptographique matérielle qualifiée au niveau Standard.

Les cérémonies de clés se déroulent sous le contrôle d'au moins trois personnes ayant des rôles de confiance (maître de cérémonie et témoins dont au moins est externe à l'AC). Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement approuvé par l'AC. Les rôles des personnes impliquées dans les cérémonies de clés sont précisés dans la DPC.

Suite à leur génération, les parts de secrets (données d'activation) sont remises à des Porteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même Porteur ne peut détenir plus d'une part de secret de l'AC à un moment donné. Chaque part de secrets est mise en œuvre par son Porteur.

2. Clés des Porteurs

Les bi-clés des Porteurs sont générées par l'AC dans un environnement sécurisé par un module cryptographique, puis transférées de manière sécurisée dans le support du Porteur (cf. § III.2.3).

VI.1.2. Transmission de la clé privée à son propriétaire

La clé privée est transmise au Porteur de manière sécurisée, importée directement dans le support en sa possession.

VI.1.3. Transmission de la clé publique du Porteur à l'AC

Sans objet (la bi-clé du Porteur est générée par l'AC).

VI.1.4. Transmission de la clé publique de l'AC aux Utilisateurs de certificats

Les clés publiques de vérification de signature de l'AC sont diffusées auprès des Utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

La clé publique de l'AC Imprimerie Nationale Élémentaire Chiffrement est diffusée dans un certificat signé par l'ACR Imprimerie Nationale Élémentaire. La clé publique de l'ACR Imprimerie Nationale Élémentaire est diffusée dans un certificat auto-signé.

Les certificats de l'ACR Imprimerie Nationale Élémentaire et de l'AC Imprimerie Nationale Élémentaire Chiffrement sont disponibles aux URL citées au chapitre II.2 de la présente PC.

VI.1.5. Tailles des clés

Les recommandations des organismes nationaux et internationaux compétents (relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage…) sont périodiquement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats Porteurs et AC doivent ou ne doivent pas être modifiés.

1. Clés d'AC

ACR Imprimerie Nationale Élémentaire

La bi-clé est de type RSA 4096 bits

L'algorithme d'empreinte est SHA-256 (dont l'OID est 1.2.840.113549.1.1.11).

AC Imprimerie Nationale Élémentaire Chiffrement

La bi-clé est de type RSA 2048 bits

L'algorithme d'empreinte est SHA-256 ou SHA-512.

2. Clés Porteurs

Les bi-clés sont de type RSA 2048 bits

L'algorithme d'empreinte est SHA-256

VI.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité

Les équipements utilisés pour la génération des bi-clés d'AC et des bi-clés des Porteurs sont des ressources cryptographiques matérielles qualifiées au niveau renforcé par l'ANSSI et respectent donc les normes de sécurité correspondant à la bi-clé (voir § VI.1.5).

VI.1.7. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'ACR et du certificat associé est strictement limitée à la signature de certificats et des LAR.

L'utilisation de la clé privée de l'AC Imprimerie Nationale Élémentaire Chiffrement et du certificat associé est strictement limitée à la signature de certificats et de LCR.

L'utilisation de la clé privée du Porteur et du certificat associé est strictement limitée aux usages décrits en I.3.1.2.

VI.2. MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

VI.2.1. Standards et mesures de sécurité pour les modules cryptographiques

Les modules cryptographiques des AC (pour la génération et la mise en œuvre de ses clés de signature et pour la génération des bi-clés des Porteurs) sont qualifiés au niveau renforcé, selon les exigences de l'ANSSI pour le niveau ** du RGS.

VI.2.2. Dispositifs de chiffrement des Porteurs

Les dispositifs des Porteurs sont produits et personnalisés dans le cadre des PC identifiées en III.2.3.

VI.2.3. Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC Imprimerie Nationale Élémentaire Chiffrement pour l'export / l'import hors / dans du module cryptographique. La génération de la bi-clé est traitée au § VI.1.1, l'activation de la clé privée au § VI.2.9 et sa destruction au § VI.2.11.

Le contrôle des clés privées de signature de AC est assuré par du personnel de confiance (Porteurs de secret d'IGC) et met en œuvre un outil de partage des secrets (3 exploitants parmi 5 doivent s'authentifier).

VI.2.4. Séquestre de la clé privée

Les clés privées d'AC (ACR ou ACF) ne sont en aucun cas séquestrées.

VI.2.5. Copie de secours de la clé privée

Les bi-clés d'AC (ACR et ACF) sont sauvegardées sous le contrôle de plusieurs personnes à des fins de disponibilité. Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles. Les sauvegardes sont transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'AC. Les sauvegardes de clés privées des AC sont stockées dans des ressources cryptographiques matérielles, ou sous forme chiffrée offrant un niveau de sécurité équivalent au stockage dans des ressources cryptographiques matérielles.

La fonction de séquestre bénéficie des mêmes mesures de sécurité et de reprise.

VI.2.6. Archivage de la clé privée

Les clés privées d'AC et de Porteurs ne sont jamais archivées.

VI.2.7. Transfert de la clé privée vers / depuis le module cryptographique

1. Clés privées d'AC

Les clés d'AC sont générées, activées et stockées dans des ressources cryptographiques matérielles.

Quand elles ne sont pas stockées dans des ressources cryptographiques matérielles ou lors de leur transfert, les clés privées d'AC sont chiffrées par l'algorithme AES (FIPS 197). Une clé privée d'AC ne peut pas être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et en la présence et l'authentification de plusieurs personnes détenant des rôles de confiance.

2. Clés privées des Porteurs

Le transfert de la clé privée du Porteur s'effectue conformément aux exigences du § VI.1.2.

VI.2.8. Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC stockées dans des ressources cryptographiques matérielles sont protégées avec le même niveau de sécurité que celui avec lequel elles ont été générées.

VI.2.9. Méthode d'activation de la clé privée

1. Clés privées d'AC

Les clés privées d'AC ne peuvent être activées dans le module cryptographique qu'avec un minimum de 3 personnes dans des rôles de confiance et qui détiennent des données d'activation de l'AC en question.

2. Clés privées des Porteurs

Les clés privées des Porteurs sont protégées par la donnée d'activation (déjà configurée) présente dans le support du Porteur pour son certificat d'authentification (cf. § III.2.3).

Le support se bloque au bout de plusieurs tentatives infructueuses de saisie du code PIN. Ce mécanisme protège le support en cas de recherche du code PIN par un tiers non autorisé.

VI.2.10. Méthode de désactivation de la clé privée

1. Clés privées d'AC

Les ressources cryptographiques matérielles dans lesquelles des clés d'AC ont été activées ne sont pas laissées sans surveillance ou accessibles à des personnes non autorisées. Après utilisation, les ressources cryptographiques matérielles sont désactivées. Les ressources cryptographiques sont ensuite stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

Les ressources cryptographiques de signature de l'AC sont en ligne uniquement afin de signer des certificats Porteurs et des LCR après avoir authentifié la demande de certificat et la demande de révocation.

2. Clés privées des Porteurs

Se référer à la politique de certification du certificat d'authentification du support (cf. § III.2.3).

VI.2.11. Méthode de destruction des clés privées

1. Clés privées d'AC

Les clés privées d'AC sont détruites quand elles ne sont plus utilisées ou quand les certificats auxquels elles correspondent sont expirés ou révoqués. La destruction d'une clé privée implique la destruction des copies de sauvegarde, des données d'activation et l'effacement de la ressource cryptographique qui la contient, de manière à ce qu'aucune information ne puisse être utilisée pour la retrouver. La destruction d'une clé privée d'AC est effectuée en présence de témoins et fait l'objet d'un procès-verbal.

2. Clés privées des Porteurs

Après génération, exportation de la bi-clé hors module cryptographique et chargement sur le support, la clé privée est effacée de façon sécuritaire du système de chargement.

VI.2.12. Niveau de qualification du module cryptographique et des dispositifs de chiffrement

Les modules cryptographiques utilisés par l'ACR Imprimerie Nationale Élémentaire et l'AC Imprimerie Nationale Élémentaire Chiffrement sont qualifiés au niveau renforcé selon les exigences de l'ANSSI pour le niveau ** du RGS.

Les dispositifs de signature et de chiffrement utilisés par l'AC sont qualifiés au niveau renforcé selon les exigences de l'ANSSI pour le niveau ** du RGS.

VI.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES

VI.3.1. Archivage des clés publiques

Les clés publiques de l'AC et des Porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

VI.3.2. Durée de vie des bi-clés et des certificats

La durée de validité du certificat de l'AC Imprimerie Nationale Élémentaire Chiffrement est de 6 ans. La durée de vie de la bi-clé correspondante est équivalente, soit 6 ans également. La fin de validité du certificat d'AC est postérieure à la fin des certificats Porteurs qu'elle émet.

Les certificats des Porteurs couverts par la présente PC ont une durée de validité de 3 ans maximum. La durée de vie des bi-clés est équivalente, soit 3 ans également.

VI.4. DONNEES D'ACTIVATION

VI.4.1. Génération et installation des données d'activation

1. Données d'activation des clés privées d'AC

Les données d'activation des clés privées d'AC sont générées durant les cérémonies de clés (Se reporter au § VI.1.1). Les données d'activation sont générées automatiquement selon un schéma à seuil de Shamir (type M (3) of N (5)). Dans tous les cas les données d'activation sont remises à leurs Porteurs après génération pendant la cérémonie des clés. Les Porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

2. Données d'activation des clés privées des Porteurs

Le code d'activation des clés privées produites dans le cadre de la présente PC est en possession du Porteur préalablement à la demande de certificat (cf. § III.2.3).

VI.4.2. Protection des données d'activation

1. AC

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Les Porteurs de données d'activation sont responsables de leur gestion et de leur protection. Un Porteur de données d'activation ne peut détenir plus d'une donnée d'activation d'une même AC à un même instant.

2. Porteur

Se référer à la politique de certification du certificat d'authentification du support (cf. § III.2.3).

VI.4.3. Autres aspects liés aux données d'activation

Les données d'activation ne sont en aucun cas transmises à une entité tierce, en particulier dans le cas où les ressources cryptographiques sont changées ou retournées au constructeur pour maintenance. Les autres aspects de la gestion des données d'activation sont précisés dans la DPC.

VI.5. MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

VI.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

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

- Identification et Authentification forte des rôles de confiance (accès physique et logique) ;
- Gestion des droits d'accès basée sur des profils respectant le principe du moindre privilège ;

- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, gestion droits d'accès aux fichiers)
- Interdiction de la réutilisation d'objets ;
- Exige l'utilisation de la cryptographie lors des communications ;
- Assure la séparation rigoureuse des tâches ;
- Protection contre les virus informatiques
- Protection du réseau contre toute intrusion illicite
- Fournit une autoprotection du système d'exploitation.
- Fonction d'audits

VI.5.2. Niveau de qualification des systèmes informatiques

Quand un composant de l'AC Imprimerie Nationale Élémentaire Chiffrement est hébergé sur une plateforme évaluée au regard d'exigences d'assurance de sécurité, il doit être utilisé dans sa version certifiée. Au minimum le composant utilise la même version de système d'exploitation que celle sur lequel le composant a été certifié.

VI.6. MESURES DE SECURITE DES SYSTEMES PENDANT LEUR CYCLE DE VIE

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risques conduite par l'AC.

VI.6.1. Mesures de sécurité liées au développement des systèmes

Les développements des systèmes sont contrôlés par les mesures suivantes :

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

VI.6.2. Mesures liées à la gestion de la sécurité

La configuration du système d'AC, ainsi que toute modification ou évolution, est documentée et contrôlée par l'AC.

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

VI.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes

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

VI.7. MESURES DE SECURITE RESEAU

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement souhaité par l'AC et pour contrer les attaques de type déni de service ou d'intrusion. En l'occurrence, le réseau est équipé de routeurs, firewalls avec système de détection des intrusions IPS avec émission d'alertes

L'AC garantit que les composants du réseau local sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de leur conformité avec les exigences spécifiées par l'AC.

VI.8. HORODATAGE / SYSTEME DE DATATION

Il n'y a pas d'horodatage utilisé par l'AC mais une datation des évènements qui permet à l'AC de séquencer les événements à partir de l'heure système de l'IGC de l'AC.

Des procédures automatiques ou manuelles sont utilisées pour synchroniser les horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près.

VII. Profil des certificats et des LCR

VII.1. PROFILS DE CERTIFICATS

Les certificats émis par l'ACR Imprimerie Nationale Élémentaire et l'AC Imprimerie Nationale Élémentaire Chiffrement sont des certificats au format X.509 v3. Les champs des certificats d'AC et des certificats des Porteurs sont définis par le RFC 5280.

VII.1.1. Certificat de l'AC Imprimerie Nationale Élémentaire Chiffrement

Remarque : il existe deux certificats pour cette AC (partageant la même bi-clé), un signé en utilisant une empreinte SHA-256, l'autre utilisant SHA-512.

Les principaux champs du certificat de l'AC Imprimerie Nationale Élémentaire Chiffrement (émis par l'ACR Imprimerie Nationale Élémentaire) sont les suivants :

Basic Certificate Field	**Value**		
Version	2 (=version 3)		
Serial number	Défini par l'outil		
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = ACR Imprimerie Nationale Élémentaire		
notBefore	YYMMDDHHMMSS (date de la cérémonie des clés)		
NotAfter	YYMMDDHHMMSS (date de la cérémonie des clés + 10 ans)		
Subject	**Attribute type**	**Attribute value**	**Directory String1**
	C	FR	PrintableString
	O	Groupe Imprimerie Nationale	UTF8String
	OU	0002 410494496	UTF8String
	OI	NTRFR-410494496	UTF8String
	CN	AC Imprimerie Nationale Élémentaire Chiffrement	UTF8String

[1] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Basic Certificate Field	**Value**
Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)
Key size	4096
Signature (algorithm & OID)	sha512WithRSAEncryption (1.2.840.113549.1.1.13) ou Sha256WithRSAEncryption (1.2.840.113549.1.1.11)

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Identifiant de la clé de l'ACR Imprimerie Nationale Élémentaire (défini par l'outil)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Défini par l'outil
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Certificate Policies	**FALSE**	
policyIdentifier		anyPolicy (2.5.29.32.0)
policyQualifier-cps		http://www.imprimerienationale.fr/GIN/PC
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
CRL Distribution Points	**FALSE**	
distributionPoint		URL = http://www.imprimerienationale.fr/GIN/CRL/ACR.crl URL = http://crl.imprimerienationale.fr/GIN/ACR.crl

VII.1.2. Certificat Porteur d'authentification émis par l'AC Imprimerie Nationale Élémentaire Chiffrement

Les principaux champs du certificat Porteur sont les suivants ; les attributs en orange sont optionnels et peuvent ne pas apparaître dans les certificats. :

Champs de base	**Valeur**
Version	2 (=version 3)
Serial Number	Défini par l'outil

Champs de base	Valeur
Issuer DN	CN = AC Imprimerie Nationale Élémentaire Chiffrement OI = NTRFR-410494496 OU = 0002 410494496 O = Groupe Imprimerie Nationale C = FR
Subject DN	CN = [*Prénom et Nom de l'état civil du Porteur*] SN = [*Nom du porteur*] GN = [*Prénom du porteur*] SerialNumber = [*numéro unique généré aléatoirement pour garantir l'unicité du DN et résoudre ainsi les cas d'homonymie*] OI = NTRFR-[*SIREN de l'Entité Cliente de rattachement du Porteur*] OU = 0002 [*SIREN de l'Entité Cliente de rattachement du Porteur*] O = [*Nom de l'Entité Cliente de rattachement du Porteur*] C = FR
PublicKeyAlgorithm	sha256WithRSAEncryption
Taille des clés	2048 bits
Durée de vie	3 ans

Extensions	Criticité	Valeur
Authority Key Identifier	N	Identifiant de la clé publique de l'AC Imprimerie Nationale Élémentaire Chiffrement
Basic Constraints	N	Contraintes de base : SubjectType=EndEntity PathLengthConstraint=aucun
Certificate Policies **policyIdentifier** **policyQualifier-cps**	N	Stratégies de certificat : 1.2.250.1.295.1.1.10.1.1.110.0 http://www.imprimerienationale.fr/GIN/PC
CRL Distribution Points	N	Point de distribution de la LCR : URL= http://www.imprimerienationale.fr/GIN/CRL/cert/ACF-EL-C.crl URL= http://crl.imprimerienationale.fr/GIN/cert/ACF-EL-C.crl
Key Usage	O	keyEncipherment, digitalSignature
Subject Key Identifier	N	Identifiant de la clé publique du Porteur
Subject Alternative Name	N	Autre nom de l'objet : Nom Principal (UPN) Nom RFC822
Extended Key Usage	N	emailProtection
Authority Information Access	N	http://ocsp-ac-el-c.imprimerienationale.fr http://www.imprimerienationale.fr/GIN/AC/AC-EL-C.p7b

VII.1.3. Formes de nom

Les formes de noms respectent les exigences du § III.1.1 pour l'identité des Porteurs et de l'AC qui est portée dans les certificats émis par l'AC.

VII.1.4. Identifiant d'objet (OID) de la politique de certification

Les certificats Porteurs contiennent l'OID du modèle de certificat (voir & 0).

VII.1.5. Extensions propres à l'usage de la politique

Sans objet

VII.1.6. Syntaxe et sémantique des qualifiants de politique

Sans objet

VII.1.7. Interprétation sémantique de l'extension critique « Certificate Policies »

Pas d'exigence formulée.

VII.2. PROFIL OCSP

Le certificat du répondeur OCSP de l'AC Imprimerie Nationale Élémentaire Chiffrement est produit conformément au profil suivant :

Champs de base	**Valeur**
Version	2 (=version 3)
Serial Number	Défini par l'outil
Issuer DN	Voir § VII.1.1
Subject DN	CN = [*Nom du service OCSP*] OI = NTRFR-410494496 OU = 0002 410494496 O = Groupe Imprimerie Nationale C = FR
PublicKeyAlgorithm	sha256WithRSAEncryption
Taille des clés	2048 bits
Durée de vie	1 an

Extensions	**Criticité**	**Valeur**
Authority Key Identifier	N	Identifiant de la clé publique de l'AC Imprimerie Nationale Élémentaire Chiffrement
Basic Constraints	N	Contraintes de base : SubjectType=EndEntity

		PathLengthConstraint=aucun
Certificate Policies **policyIdentifier** **policyQualifier-cps**	N	Stratégies de certificat : **1.2.250.1.295.1.1.10.1.1.110.0** http://www.imprimerienationale.fr/GIN/PC
Key Usage	O	digitalSignature
Subject Key Identifier	N	Identifiant de la clé publique de la plateforme
Extended Key Usage	N	OCSP Signing
OCSP No Check	N	Null

VII.3. PROFILS DE LCR

L'AC Imprimerie Nationale Élémentaire Chiffrement émet des LCR dont les caractéristiques sont :

Caractéristiques des LCR	Durée de validité Périodicité de mise à jour Version de la LAR (v1 ou v2) Extensions URL http de publication	: 4 jours : quotidienne : v2 : Numéro de la LCR et AKI : Voir § II.2

Les principaux champs de la LCR sont :

Champ de base	**Valeur**
Version	2
Signature	Identifiant de l'algorithme de signature de l'AC Imprimerie Nationale Élémentaire Chiffrement SHA-256 RSA 2048
Issuer DN	Voir § VII.1.1
This Upadte	Date de génération de la LCR
Next Update	Date de prochaine mise à jour de la LCR
Revoked certificates	Liste des numéros de série des certificats Porteurs révoqués

Extensions	**Criticité**	**Description**
Authority Key Identifier	N	Identifiant de la clé publique de l'AC Imprimerie Nationale Élémentaire Chiffrement
CRL Number	N	Numéro de série de la LCR

VIII. Audit de conformité et autres évaluations

Les audits et les évaluations concernent :

- D'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification selon le schéma de qualification des prestataires de service de confiance conformément au décret RGS
- Et d'autre part, ceux que doit réaliser, ou faire réaliser l'AAI afin de s'assurer que l'ensemble de son IGC, et le cas échéant l'ensemble des MC, respecte les engagements affichés dans cette PC et les pratiques identifiées dans la DPC associée.

L'AC se réserve le droit de réaliser des audits inopinés auprès des MC au même titre que le personnel de son IGC.

VIII.1. FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AAI procède à un contrôle de conformité de cette composante. L'AAI procède également un fois par an à un contrôle de conformité de l'ensemble de son IGC dans le cadre de la qualification RGS de l'AC.

Un contrôle de conformité de l'AC a été effectué avant la première mise en service pour l'obtention de la qualification RGS au niveau ** de l'AC Imprimerie Nationale Élémentaire Chiffrement.

La reconnaissance du respect par l'AC des exigences de la présente PC est effectuée dans le cadre du schéma de qualification des prestataires de services de confiance mis en place et géré par l'ANSSI en France (se reporter au [PROG_ACCRED]) conformément au [DécretRGS].

VIII.2. IDENTITES / QUALIFICATIONS DES EVALUATEURS

Le contrôle d'une composante doit être assigné par l'AAI à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée. Ils doivent être habilités, le cas échéant.

VIII.3. RELATIONS ENTRE EVALUATEURS ET ENTITE EVALUEE

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

VIII.4. SUJETS COUVERTS PAR LES EVALUATIONS

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

VIII.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AAI, 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'AAI qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AAI et doit respecter ses politiques de sécurité internes.

- En cas de résultat "à confirmer", l'AAI 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'AAI confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

VIII.6. COMMUNICATION DES RESULTATS

Les résultats des contrôles de conformité sont communiqués uniquement et seulement à la composante contrôlée ainsi qu'au responsable de l'AAI. Ils incluent les mesures correctives de la composante déjà prises ou en cours.

Compte tenu du caractère confidentiel des résultats, ces derniers ne seront pas publiés sans l'autorisation de l'ensemble des parties, ni transmis à d'autres interlocuteurs sans leur accord.

Les résultats des audits de conformité doivent toutefois être tenus à disposition de l'organisme en charge de la qualification de l'AC.

IX. Autres problématiques métiers et légales

IX.1. TARIFS

IX.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

La tarification est établie sur la base d'une offre globale de services d'INCS intégrant un ensemble de prestations dont la délivrance et la gestion des certificats numériques et des supports. Cette tarification, révisable annuellement, est définie dans les conditions générales de services.

IX.1.2. Tarifs pour accéder aux certificats

Les certificats sont gratuitement accessibles aux Utilisateurs.

IX.1.3. Tarifs pour accéder aux informations d'état et de révocation des certificats

Les informations d'état et de révocation des certificats sont accessibles gratuitement sur le serveur de publication.

IX.2. RESPONSABILITE FINANCIERE

INCS s'engage à respecter la présente PC. Toute condition supplémentaire non portée dans ce document ne pourra valablement être considérée comme une obligation d'INCS.

IX.2.1. Couverture par les assurances

INCS applique des niveaux de couverture d'assurance raisonnables et a souscrit à cet effet une assurance responsabilité civile au titre de la réalisation de son activité professionnelle.

IX.2.2. Autres ressources

INCS est en capacité financière de remplir sa mission.

IX.2.3. Couverture et garantie concernant les Entités utilisatrices

Les entités utilisatrices doivent être en capacité financière de pouvoir accomplir leur mission.

En cas de dommage pour un client causé par une des AC sous contrôle d'INCS, celle-ci fera appel à son assurance pour couvrir une partie des dommages du client dans la limite de la responsabilité d'INCS définie dans les conditions générales de services INCS et aux présentes.

IX.3. CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

IX.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- les parties non publiques de la DPC de l'AC et les procédures internes associées,
- les clés privées de l'AC, de ses composantes et des Porteurs de certificats
- les données d'activation associées aux clés privées d'AC ainsi quelle celles associées aux clés privées des

Porteurs (avant que ces données soient transmises aux Porteurs),
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les éléments relatifs à la cérémonie des clés, comprenant l'identité des Porteurs de secrets
- les causes de révocations, sauf accord explicite du Porteur,
- les dossiers d'enregistrement des Porteurs,
- les rapports des audits.

Seules les personnes habilitées peuvent y accéder.

IX.3.2. Informations hors périmètre des informations confidentielles

Les informations concernant l'IGC publiées par le SP sont considérées comme non confidentielles, elles sont communiquées selon le principe du besoin d'en connaître.

IX.3.3. Responsabilité en termes de protection des informations confidentielles

L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au § IX.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage ainsi qu'à leur sauvegarde.

De plus, lorsque ces données sont échangées, l'AC doit en garantir l'intégrité.

L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français notamment la divulgation aux autorités judiciaires et/ou administratives. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des Porteurs à des tiers dans le cadre de procédures légales. Elle doit également donner accès au Porteur à son dossier d'enregistrement, le cas échéant au MC et aux opérateurs d'AE en lien avec l'Entité Cliente de rattachement du Porteur.

IX.4. PROTECTION DES DONNEES PERSONNELLES

IX.4.1. Politique de protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi n°78-17 du 6 janvier 1978 modifiée dite « Informatique et Libertés ».

Conformément à la loi informatique et libertés (article 40 de la loi du 6 janvier 1978), l'AC donne aux Porteurs de certificat un droit d'accès et de modification de leurs données personnelles en cas de données inexactes, incomplètes ou équivoques au moment de leur collecte. Pour exercer ce droit, les Porteurs doivent se mettre en relation avec l'Autorité d'Enregistrement. En cas de rectification des données personnelles, l'AC se réserve le droit de révoquer le certificat en cours de validité en cas d'incidence sur son contenu.

IX.4.2. Informations à caractère personnel

L'AC considère que les informations suivantes sont des informations à caractère personnel :
- Les dossiers d'enregistrement des Porteurs, des MC ;
- Les demandes de certificat des Porteurs ;
- Les demandes de révocation ;
- Les causes de révocation des certificats des Porteurs.

IX.4.3. Informations à caractère non personnel

Dans ce contexte, aucune responsabilité de quelque nature qu'elle soit ne pourra être engagée.

IX.4.4. Responsabilité en termes de protection des données personnelles

Voir § IX.4.1

L'AC a mis en place et respecte des mesures de protection des données à caractère personnel notamment afin de garantir leur sécurité et ce dans le respect des principes de proportionnalité et de transparence.

IX.4.5. Notification et consentement d'utilisation des données personnelles

L'AC s'engage à respecter la finalité de la collecte et de traitement des données à caractère personnel.

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles identifiées dans cette PC ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du propriétaire des données), décision judiciaire ou autre autorisation légale.

IX.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

L'AC agit conformément à la réglementation en vigueur sur le territoire français et dispose de procédures de divulgation d'informations personnelles aux autorités judiciaires et administratives sur leur demande expresse.

IX.4.7. Autres circonstances de divulgation d'informations personnelles

Sans objet

IX.5. DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

La PC s'inscrit dans le cadre du respect des droits de propriété intellectuelle et industrielle. INCS conserve tous les droits de propriété intellectuelle et est propriétaire de la présente PC et de la DPC associée, des certificats qu'elle émet et des informations de révocation correspondantes qu'elle publie.

IX.6. INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Les obligations communes aux composantes de l'IGC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ainsi que des éventuelles données d'activation ;
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par cette PC et des documents qui en découlent ;
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante) ;
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AAI et l'organisme de qualification ;
- mettre en œuvre les mesures adaptées pour la correction des écarts détectés lors de ces contrôles de conformité ;

- respecter les accords ou contrats qui les lient entre elles ou aux Porteurs ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques, organisationnels et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité ;
- mettre en œuvre des actions de sensibilisation et de formation ;
- mettre en place une documentation de la responsabilité de chacun des acteurs concernés.

IX.6.1. Autorité de certification

L'AC s'engage à :

- Pouvoir démontrer aux Utilisateurs de ses certificats qu'elle a émis un certificat pour un Porteur donné et que ce dernier a accepté ce certificat conformément au § 4.4 ;
- Garantir et maintenir la cohérence de sa DPC avec sa PC ;
- Respecter et faire respecter les parties des DPC concernées par les différentes composantes ;
- Prendre toutes les mesures raisonnables pour s'assurer que ses Porteurs sont au courant de leurs droits et utilisation en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un Porteur et l'AC est formalisée dans un lien contractuel ou hiérarchique précisant les droits et obligations des parties et notamment les garanties apportées par l'AC ;
- Diligenter des audits ;
- Sensibiliser les différents acteurs à la sécurité et aux technologies mises en œuvre.

INCS doit prendre les dispositions nécessaires pour couvrir les responsabilités liées à ses activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence dûment prouvée, d'elle-même ou de l'une de ses composantes, qu'elle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération et le détournement des données personnelles des Porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AC.

IX.6.2. Autorité d'Enregistrement

Les obligations de l'AE sont :

- L'identification et l'authentification du Porteur, le cas échéant au travers du MC, et l'identification de son Entité Cliente ;
- La vérification du dossier d'enregistrement du futur Porteur, la validation et le traitement des demandes de certificats ;
- La vérification du dossier d'enregistrement des futurs MC ;
- La délivrance du support personnalisé au Porteur, le cas échéant via le MC ;
- L'identification de l'émetteur d'une demande de révocation, la validation et le traitement de cette demande ;
- Le respect de la PC et de la DPC associée de l'AC ;
- L'assurance de la connaissance et de l'acceptation par le Porteur de ses obligations (reprises dans les Conditions Générales d'Utilisation) ;
- L'assurance du respect par les opérateurs d'AE et les MC de leurs obligations respectives (parties de la PC/DPC les concernant, lettres d'engagement, etc.) ;

IX.6.3. Opérateur de services de certification

L'opérateur de services de certification a le devoir de mettre en œuvre et d'opérer l'IGC dans le respect des exigences énoncées dans la PC et la DPC associée.

IX.6.4. Porteurs de certificats

Les Porteurs des certificats ont pour obligation de :

- Communiquer des informations exactes et à jour lors de la demande de certificat (demande initiale ou renouvellement) ;
- Protéger le support qui leur a été remis, leurs clés privées ainsi que les données d'activation ;
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant (décrites dans les CGU et la PC) ;
- Informer l'AC de toute modification concernant les informations contenues dans leur certificat ;
- Effectuer, sans délai, une demande de révocation de leur certificat auprès de l'AE, ou le cas échéant du MC, en cas de survenance de l'un des événements énumérés au § IV.9.1.

IX.6.5. Utilisateurs de certificats

Les Utilisateurs de certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Pour chaque certificat de la chaîne de certification, du certificat du Porteur jusqu'au certificat de l'ACR, vérifier la signature de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- Vérifier et respecter les obligations des Utilisateurs de certificats exprimés dans la présente PC.

IX.7. LIMITE DE GARANTIE

L'AC garantit au travers de ses services d'IGC :

- Son identification et authentification grâce à son certificat signé par l'ACR Imprimerie Nationale Élémentaire ;
- L'identification et l'authentification des Porteurs grâce aux certificats qu'elle leur délivre ;
- La gestion des certificats correspondants et des informations de validité des certificats selon la présente PC.

Ces garanties sont exclusives de toute autre garantie de l'AC.

Il est expressément entendu que INCS ne saurait être tenu pour responsable ni d'un dommage résultant d'une faute ou négligence d'un Client et/ou de ses Porteurs ni d'un dommage causé par un fait extérieur ou un cas de force majeur, notamment en cas de :

- Utilisation de la clé privée pour un autre usage que celui défini dans le certificat associé ;
- Utilisation d'un certificat pour une autre application que les Applications autorisées ;
- Utilisation d'un certificat pour garantir un autre objet que l'identité du Porteur ;
- Utilisation d'un certificat révoqué ;
- Mauvais modes de conservation de la clé privée du certificat du Porteur ;
- Utilisation d'un certificat au-delà de sa limite de validité ;
- Non-respect des obligations des autres Intervenants (se reporter au § IX.6.5) ;
- Faits extérieurs à l'émission du certificat tel qu'une défaillance de l'application pour laquelle il peut être utilisé ;
- Cas de force majeur tels que définis par les tribunaux français.

IX.8. LIMITE DE RESPONSABILITE

La responsabilité de l'AC peut seulement être engagée dans les cas limitativement énumérés ci-dessous:

- en cas de dommage direct prouvé causé à un Porteur ou une application / Utilisateur de certificat à la suite d'un manquement aux procédures définies dans la PC et à la DPC associée, la faute de l'AC devant être dûment prouvée ;
- en cas de compromission prouvée, entièrement et directement imputable à l'AC.

L'AC décline toute responsabilité à l'égard de l'usage qui est fait des certificats qu'elle a émis dans des conditions et à des fins autres que celles prévues dans la présente PC ainsi que dans tout autre document contractuel applicable associé, en particulier :

- utilisation d'un certificat pour un usage autre que les usages mentionnés au § I.3.1.2 ;
- utilisation d'un certificat révoqué ;
- utilisation d'un certificat au-delà de sa limité de validité.

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

L'AC ne saurait être tenue responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente PC lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1148 du Code civil.

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

L'AC décline toute responsabilité concernant les dommages indirects (notamment tout préjudice financier ou commercial) et, par conséquent, n'ouvre pas droit à réparation.

En tout état de cause, les éventuelles indemnisations que INCS pourrait être amenée à versée au titre d'un manquement à ses obligations ne sauraient dépasser le(s) montant(s) prévus au § IX.9 ci-après.

IX.9. INDEMNITES

Si une faute prouvée d'INCS dans l'exécution de ses obligations stipulées dans la présente PC en qualité d'AC est établie et a causé directement un dommage, INCS indemnisera la personne/Entité Cliente concernée dans la limite définie au contrat de services

IX.10. DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

IX.10.1. Durée de validité

La PC devient effective à sa date de validation par l'AAI figurant aux présentes.

La PC de l'AC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

IX.10.2. Fin anticipée de validité

La publication d'une nouvelle version de la PC type *Certificats électroniques de personnes* [RGS_v-2-0_A2] rédigée par l'ANSSI, peut entraîner, en fonction des évolutions demandées, la nécessité pour l'AAI de faire évoluer la PC qu'elle met en œuvre.

La mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié aux modifications des exigences de sécurité contenues dans la présente PC.

IX.10.3. Effet de la fin de validité et clauses restant applicables

Les clauses restant applicables au-delà de la fin d'utilisation de la PC sont celles concernant l'archivage des données. Toutes les autres obligations deviennent caduques et sont remplacées par celles décrites dans la ou les PC encore en vigueur.

IX.11. NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AAI s'engage :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'AC et de ses différentes composantes ;
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

IX.12. AMENDEMENTS A LA PC

IX.12.1. Procédures d'amendement

L'AAI révise sa PC et sa DPC périodiquement au moins une fois par an et :

- à chaque évolution des systèmes de l'IGC ou des procédures internes à l'IGC ayant un impact sur la PC/DPC ;
- à chaque fois qu'une évolution remarquable de l'état de l'art ou d'une législation/réglementation en vigueur le justifie ;
- ou lorsque les résultats des contrôles d'audit de conformité l'imposent (non-conformité par rapport à la PC type).

Ces amendements sont toutefois effectués en restant conforme aux exigences des PC type et des éventuels documents complémentaires du RGS.

L'adoption des amendements s'effectue dans les mêmes conditions que l'adoption de la PC et ce conformément au principe du parallélisme des formes.

En cas de modification majeure de la PC et conséquemment de la DPC, l'AAI procède à une vérification de la conformité de la PC par rapport aux PC type applicables, et de la conformité de la DPC avec cette nouvelle version de la PC. La DPC n'est applicable qu'après validation de l'AAI.

IX.12.2. Mécanismes et périodes d'information sur les amendements

L'AAI donne un préavis de deux mois au moins aux composantes de l'AC de son intention de modifier sa PC avant de procéder aux changements et en fonction de l'objet de la modification.

Ce délai ne vaut que pour des modifications qui porteraient sur le fond (changement de taille de clé, changement de procédure, changement de profil de certificat, …) et non sur la forme de la PC et de la DPC.

NB : les corrections typographiques ou orthographiques ne nécessitent pas de notification de la part de l'AAI.

IX.12.3. Circonstances selon lesquelles l'OID doit être changée

L'OID de l'ACF étant inscrit dans les certificats qu'elles émettent, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis doit se traduire par une évolution de l'OID, afin que les Utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

Toutefois, les Porteurs et Utilisateurs de certificat peuvent facilement identifier et accéder sur le site de publication à la version de la PC sous laquelle le certificat concerné a été émis par l'AC. Le site diffuse en effet, outre la version courante de la PC, l'ensemble des anciennes versions, chacune de ces versions faisant clairement apparaître la date de publication et par conséquent la période sur laquelle elle était en vigueur.

NB : le RGS impose en théorie l'évolution de l'OID en cas de changements majeurs de la PC. Toutefois dans la pratique cela n'est pas respecté. L'AC doit a minima s'assurer que les Porteurs/Utilisateurs puissent accéder facilement à la version de PC sous laquelle le certificat concerné a été émis.

IX.13. DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

L'AAI met en place des politiques et des procédures pour le traitement des réclamations et le règlement des litiges émanant des Entités Clientes pour lesquelles elle fournit des services électroniques de confiance.

IX.14. JURIDICTION COMPETENTE

Les dispositions de la politique de certification sont régies par le droit français. En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique et à défaut de règlement amiable, la compétence est celle des Tribunaux du siège social de l'INCS.

IX.15. CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

La présente PC est sujette aux lois, règles, règlements, ordonnances, décrets et ordres nationaux d'état, locaux et étrangers concernant les IGC, mais non limité aux IGC, restrictions à l'importation et à l'exportation de logiciels ou de matériels cryptographiques ou encore d'informations techniques.

Les textes législatifs et réglementaires applicables à la PC sont, notamment, ceux indiqués au § I.5 ci-dessus.

IX.16. DISPOSITIONS DIVERSES

IX.16.1. Accord global

Sans objet

IX.16.2. Transfert d'activités

Voir § V.8

IX.16.3. Conséquences d'une clause non valide

Au cas où une clause des présentes PC s'avèrerait être non valide au regard de la loi applicable, ceci ne remettrait pas en cause la validité et l'applicabilité des autres clauses.

IX.16.4. Application et renonciation

Sans objet

IX.16.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

INCS ne saurait être tenu pour responsable et n'assume aucun engagement pour tout retard dans l'exécution ou pour toute inexécution d'obligations résultant de la présente Politique de Certification lorsque les circonstances qui en sont à l'origine relèvent de la force majeure au sens de l'article 1148 du Code Civil.

IX.17. AUTRES DISPOSITIONS

La présente PC ne formule pas d'exigence spécifique sur le sujet.