## Imprimerie Nationale (INCS)

# Politique de Certification

## Programme Plateforme de Gestion des Identités Numériques

### Document sécurité

| | |
|---|---|
| **Mode de diffusion** | **Publique** |
| **Statut du document** | **VALIDEE** |
| **Date d'application** | **02 juillet 2014** |

## HISTORIQUE DES VERSIONS

| Version | Date | Auteur | Nature de la révision<br>Paragraphes modifiés |
|---|---|---|---|
| 1.0 | 02/07/2013 | Imprimerie Nationale | Version initiale |
| 1.1 | 07/2013 | Imprimerie Nationale | Corrections |
| 1.2 | 07/2013 | Imprimerie Nationale | Corrections |
| 1.3 | 16/06/2014 | Imprimerie Nationale | Corrections suite aux remontées de l'étape 1 de l'audit RGS<br>Mise en cohérence de l'OID |
| 1.4 | 02/07/2014 | Imprimerie Nationale | Corrections mineures remontées lors de l'audit RGS |
| | | | |
| | | | |
| | | | |

# SOMMAIRE

# I. Introduction

## I.1. OBJET DU DOCUMENT ET GENERALITES

Le Groupe Imprimerie Nationale, à travers sa société IN Continu et Services (INCS), met en place son Infrastructure de Gestion de clés afin de gérer les certificats dont elle a besoin pour ses propres services d'une part et de gérer les certificats de ses clients dans le cadre de l'offre de services de la plateforme de services de confiance. La responsabilité de cette infrastructure de Gestion de Clés est confiée à l'entité juridique INCS.
INCS offre donc des services de certification ayant pour objectif la mise en œuvre de fonctions de sécurité (authentification, signature, chiffrement) dans le cadre de la plateforme de gestion des identités numériques. A ce titre, INCS devient PSCE.
Dans ce cadre, INCS déploie trois autorités racines correspondant aux trois niveaux de confiance :

- Une autorité racine Imprimerie Nationale élémentaire,
- Une autorité racine Imprimerie Nationale standard qui sera certifiée RGS 2*,
- Une IGC Imprimerie Nationale renforcée qui sera certifiée RGS 3*.

La présente politique de certification décrit les différents niveaux de responsabilité, les mesures de sécurité (techniques, audits...) ainsi que les profils des certificats et ce conformément aux dispositions du Référentiel Général de Sécurité.
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 consultée et soit acceptée non seulement par les porteurs de Certificat, mais également par tout utilisateur de Certificat.
Les ACR auto-signent leurs certificats et signent les LAR et certificats des AC filles. Les AC filles délivrent les certificats aux porteurs.
La hiérarchie d'autorité de certification est donc la suivante :

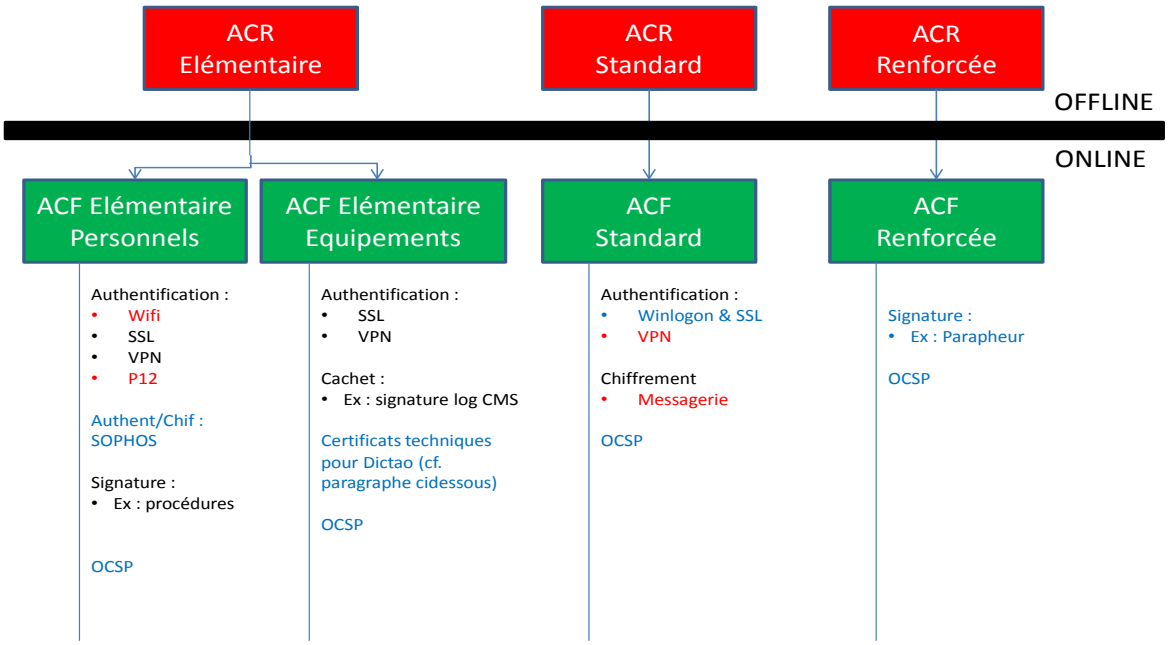



**Figure 1 : Hiérarchie des Autorités de Certification**

Dans la mesure où les trois ACR mises en œuvre respectent les mêmes exigences, ce document constitue la Politique de Certification (PC) des ACR de l'Imprimerie Nationale et a pour objet de décrire la gestion du cycle de vie des certificats et bi-clés associés des ACR et des ACF. Il constitue également le cadre général applicable aux ACF qui feront l'objet de politiques complémentaires afin d'encadrer leurs spécificités.
Les ACR et les ACF étant sous la responsabilité d' INCS, nous désignerons sous le sigle AC l'autorité morale responsable des ACR et des ACF.
La présente politique ne concerne que les ACR.
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).

### I.2. NOM DU DOCUMENT ET IDENTIFICATION

La présente PC nommée « POLITIQUE DE CERTIFICATION – AC Racines Imprimerie Nationale » est la propriété d'INCS.
Cette Politique de Certification est identifiée par les numéros des OID des ACR listés ci-dessous.
Compte tenu de la très grande similarité entre les différentes ACR d'INCS le présent document rassemble toutes les PC des ACR ; le tableau ci-dessous présente le nom de chaque ACR et le numéro d'identifiant d'objet (OID) correspondant.

La présente PC est identifiée dans le tableau suivant par l'OID suivant :

| Nom de l'AC Racine | OID associé |
|---|---|
| AC RACINE IMPRIMERIE NATIONALE ELEMENTAIRE | 1.2.250.1.295.1.1.10.5.2.109.1 |
| AC RACINE IMPRIMERIE NATIONALE STANDARD | 1.2.250.1.295.1.1.11.5.2.109.1 |
| AC RACINE IMPRIMERIE NATIONALE RENFORCEE | 1.2.250.1.295.1.1.12.5.2.109.1 |

### I.3. ENTITES DE L'IGC

La notion d'autorité de certification (AC) telle qu'utilisée dans le présent document est définie au chapitre §I.7.1.
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 AC (ACR ou ACF) et remet la clé publique à certifier au service de génération des certificats
- Génération de certificats : Ce service génère les certificats électroniques des ACR ou des ACF à partir des informations fournies par l'autorité d'enregistrement.
- Révocation : Ce service traite les demandes de révocation de certificat d'AC (ACR ou ACF) et détermine les actions à mener dont la génération de la liste des AC révoquées (LAR ou ARL).
- Publication : Ce service met à disposition des utilisateurs de certificats (UC) et des porteurs de certificats les informations nécessaires à l'utilisation des certificats émis par les AC (Conditions générales, politiques de certification, certificats d'AC, …) ainsi que les résultats des traitements du service de gestion des révocations de certificats (LAR, avis d'information, …).

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

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.3.1. Autorité administrative INCS

L'autorité administrative INCS (AAI) est composée d'un COMITE 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 autorise et valide la création et l'utilisation des composantes de l'AC. Elle suit les audits et les contrôles de conformité effectuées par les composantes de l'IGC, décide des actions à mener et veille à leur mise en application.

### I.3.2. Les autorités de certification

Les autorités de certification racines (ACR) génèrent et révoquent les certificats à partir des demandes envoyée par l'Autorité d'Enregistrement. Les AC mettent en œuvre les services de génération de certificats, de révocation de certificats, de journalisation et d'audits.
L'AAI a la possibilité de déléguer une partie des services.
Elle délègue à l'Opérateur de certification, la génération et la révocation des certificats des ACR et des ACF.

### I.3.3. 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 et journalisation et d'audit.
L'AE est constituée de représentants de l'AAI qui garantissent le nommage des ACR et ACF lors des cérémonies de clés.

### I.3.4. 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.3.5. L'opérateur de services de certification

L'OSC assure des prestations techniques nécessaires au processus de certification, conformément à la présente PC et DPC.
L'OSC est techniquement dépositaire des clés privées des ACR utilisées pour la signature des certificats d'ACF. Sa responsabilité se limite au respect des procédures que l'AC définit afin de répondre aux exigences de la présente PC.

### I.3.6. Porteurs de certificats

Est désigné comme porteur, toute entité détentrice d'une bi-clé et d'un certificat associé délivré par l'IGC d'INCS. Le porteur peut être une personne physique ou morale, un équipement informatique ou une application. Lorsque le porteur n'est pas une personne physique, il est représenté par la personne qui en est responsable. Cette personne doit être détentrice d'un certificat délivré par l'AC afin d'effectuer la demande de certificat pour l'entité dont elle est responsable.

### I.3.7. Utilisateurs de certificats

Application, personne physique ou morale, système informatique, matériel qui utilise un certificat de porteur conformément à la politique de sécurité du Groupe Imprimerie Nationale, afin de valider les fonctions de sécurité mises en œuvre à l'aide des certificats d'authentification, de signature ou de chiffrement. 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 les certificats d'AC et contrôler les LAR .

## I.4. USAGE DES CERTIFICATS

### I.4.1. Bi-clé et certificats d'AC

Une bi-clé d'ACR sert à signer des certificats d'ACR et ACF et des LAR. Un certificat électronique d'ACR identifie les chaînes de certification d' INCS utilisées dans le cadre de ses propres applications ou pour les clients qui accepteraient de la reconnaître comme autorité de certification.
Les bi-clés d'ACF en ligne servent à signer les certificats des porteurs et les listes des certificats révoqués (LCR).
Les chaînes de certificats issues d'INCS sont constituées comme suit :

- Certificat d'ACR (AC hors ligne) : certificat électronique auto-signé d'une ACR,
- Certificat d'ACF (ACF en ligne) : certificat électronique délivré à une ACF par l'ACR,
- Certificat porteur : certificat électronique délivré par une ACF en ligne.

### I.4.2. Utilisation interdite des certificats

Les utilisations de certificats émis par les ACR à d'autres fins que celles prévues par la présente PC ne sont pas autorisées. Cela signifie que l'AC ne peut être tenue en aucun cas pour responsable d'une utilisation des certificats qu'elle émet autre que celle prévue dans la présente PC.
Les certificats ne peuvent être utilisés que conformément aux lois en vigueur et applicables, en particulier seulement dans les limites autorisées par les lois sur l'importation et l'exportation.

## I.5. APPLICATION DE LA POLITIQUE

### I.5.1. Organisme responsable de la présente politique

La présente politique est sous la responsabilité de l'AAI.

### I.5.2. Personne responsable

Coordonnées de la personne responsable de l'élaboration de la PC

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

### I.5.3. Personne déterminant la conformité de l'implémentation de la présente PC/DPC

L'AAI procède à des contrôles de conformité et à des audits afin d'autoriser ou non l'émission des certificats. Les audits sont confiés à une société tierce choisie par l'AAI.

### I.5.4. Procédure d'approbation du présent document

Cette procédure 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.

## I.6. DOCUMENTS DE REFERENCE

### I.6.1. 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 ;<br>http://www.cil.cnrs.fr/CIL/spip.php?rubrique281 |
| Directive 1999/93/CE du Parlement Européen et du Conseil en date du 13 Décembre 1999 sur un cadre communautaire pour les signatures électroniques. |
| Ordonnance n°2005-1516 du 8 Décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.<br>http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&dateTexte=vig |
| Article 801-1 du code de procédure pénale |
| Article 1316 et suivante du Code Civil relatif à la signature électronique |
| Décret n°2010-112 du 2 Février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n°2005-1516<br>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<br>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<br>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<br>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<br>http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=id |
| Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques<br>http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024502658&categorieLien=id |
| Directives dites « Paquet telecom »qui comprend :<br>- une directive (2009/140/CE) qui amende trois directives existantes : |

| |
|---|
| - directive accès (2002/19/CE)<br>- directive autorisation (2002/20/CE)<br>- directive cadre (2002/21/CE)<br>- une directive (2009/136/CE) qui amende deux directives existantes :<br>- directive service universel (2002/22/CE)<br>- directive vie privée et communications électroniques (2002/58/CE)<br>- 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)<br><br>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 |
| <u>Principaux projets en cours :</u><br>Projet de règlement européen concernant la protection des données à caractère personnel<br>Projet de directive européenne concernant la protection des systèmes d'information en date du 7 février 2013 |

### I.6.2. Documents techniques

| |
|---|
| Référentiel général de sécurité – version 1.0<br>http://www.ssi.gouv.fr/fr/reglementation-ssi/referentiel-general-de-securite/liste-des-documents-constitutifs-du-rgs-v1-0.html<br>Référentiel Général de Sécurité V2 ( en cours d'élaboration) |

## I.7. TERMINOLOGIE ET ABREVIATIONS

### I.7.1. 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].
**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 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) utilise pour approuver ou rejeter des demandes de certificat (émission, gestion, renouvellement et révocation de certificats). [RFC 3647].
**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 qui ne sont plus valables 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 2459].
**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 signature électronique de l'ensemble des AC contenues dans le chemin de certification. Elle inclut également la validation du certificat de l'ensemble des AC du chemin de certification. La validation d'un certificat électronique nécessite au préalable de choisir le certificat auto-signé qui sera pris comme référence.

### I.7.2. Abréviations

| | |
|---|---|
| **AAI** | **Autorité Administrative INCS** |
| **AC** | Autorité de Certification |
| **ACF** | Autorité de Certification Fille |
| **ACR** | Autorité de Certification Racine |
| **ANSSI** | Agence Nationale de la Sécurité des Systèmes d'information |
| **CMS** | Credentials Management System |
| **DPC** | Déclaration des Pratiques de Certification |
| **HSM** | Hardware Security Module |
| **IGC** | Infrastructure de Gestion de Clés |
| **INCS** | **Imprimerie Nationale CS (entité juridique du Groupe Imprimerie Nationale responsable des ACR)** |
| **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 |
| **OID** | Object Identifier |
| **PC** | Politique de Certification |
| **OSC** | Opérateur de Services de Certification |
| **RSA** | Rivest Shamir Adelman |
| **SHA-256** | Secure Hash Algorithm 256 |
| **SP** | Service de Publication |
| **UC** | Utilisateur de certificat |

# II. Responsabilités concernant la mise à disposition devant être publiées

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

Le service de publication est en charge de la publication des données identifiées au & II.2.

## II.2. INFORMATIONS DEVANT ETRE PUBLIEES

L'AC s'assure que les termes et conditions applicables à l'usage des certificats qu'elle délivre sont mis à la disposition des porteurs et des UC. L'AC, via le SP, rend disponibles les informations suivantes:

- La présente PC : http://www.imprimerienationale.fr/GIN/PC
- Les certificats d'ACR et d'ACF en cours de validité : http://www.imprimerienationale.fr/GIN/AC
- Les informations permettant aux utilisateurs de certificats de s'assurer de l'origine des certificats d'ACR et de leur état,
- Les LAR de l'ACR Elémentaire :
  - http://www.imprimerienationale.fr/GIN/CRL/AC-EL-P.crl
  - http://crl.imprimerienationale.fr/GIN/AC-EL-P.crl
- Les LAR de l'ACR Standard :
  - http://www.imprimerienationale.fr/GIN/CRL/AC-ST-P.crl
  - http://crl.imprimerienationale.fr/GIN/AC-ST-P.crl
- Les LAR de l'ACR Renforcée :
  - http://www.imprimerienationale.fr/GIN/CRL/AC-RF-P.crl
  - http://crl.imprimerienationale.fr/GIN/AC-RF-P.crl

A contrario, les autres informations sont qualifiées de confidentielles.

## II.3. DELAIS ET FREQUENCE DE PUBLICATION

Toute nouvelle PC est publiée sur le site d'INCS dans les 24 h ouvrées après sa date de mise à jour. Elle est accessible sur le site 7 j sur 7 et 24 h sur 24.
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 chapitres § IV.9 et § IV.10
Les certificats d'ACR (ACR ou ACF) et les informations permettant aux utilisateurs de certificats de s'assurer de l'origine des certificats d'ACR doivent être diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LAR/LCR correspondants. Les systèmes publiant ces certificats sont accessibles 24 heures / 24 et 7 jours / 7.

## 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 pour les utilisateurs de certificats et protégé contre les modifications non autorisées.

# III. Identification et authentification

## III.1. NOMMAGE

### III.1.1. Type de noms

Les identités utilisées sont décrites suivant la norme X 500.
Dans chaque certificat X 509, le fournisseur (Issuer) et le porteur (subject) sont identifiés par un DN (Distinguished Name).

### III.1.2. Certificats d'ACR

L'identité de l'ACR de la gamme élémentaire de production dans le certificat de l'ACR est la suivante :

| Champ | Valeur |
|---|---|
| cn= | ACR Imprimerie Nationale Elémentaire |
| ou= | 0002 41049449600046 |
| o= | Groupe Imprimerie Nationale |
| c= | FR |

L'identité de l'ACR de la gamme élémentaire de test dans le certificat de l'ACR est la suivante :

| Champ | Valeur |
|---|---|
| cn= | TEST AC Imprimerie Nationale Elémentaire |
| ou= | SIREN |
| o= | Groupe Imprimerie Nationale |
| c= | FR |

L'identité de l'ACR de la gamme standard de production dans le certificat de l'ACR est la suivante :

| Champ | Valeur |
|---|---|
| cn= | ACR Imprimerie Nationale Standard |
| ou= | 0002 41049449600046 |
| o= | Groupe Imprimerie Nationale |
| c= | FR |

L'identité de l'ACR de la gamme standard de test dans le certificat de l'ACR est la suivante :

| Champ | Valeur |
|---|---|
| cn= | TEST AC Imprimerie Nationale Standard |
| ou= | SIREN |
| o= | Groupe Imprimerie Nationale |
| c= | FR |

L'identité de l'ACR de la gamme renforcée de production dans le certificat de l'ACR est la suivante :

| Champ | Valeur |
|---|---|
| cn= | ACR Imprimerie Nationale Renforcée |

| | |
|---|---|
| ou= | 0002 41049449600046 |
| o= | Groupe Imprimerie Nationale |
| c= | FR |

L'identité de l'ACR de la gamme renforcée de test dans le certificat de l'ACR est la suivante :

| **Champ** | **Valeur** |
|---|---|
| cn= | TEST AC Imprimerie Nationale Renforcée |
| ou= | SIREN |
| o= | Groupe Imprimerie Nationale |
| c= | FR |

### III.1.3. Nécessité d'utilisation de noms explicites

Les certificats d'ACR et ACF émis par la présente PC comportent des noms explicites et nominatifs.

### III.1.4. Pseudonymisation des porteurs

S'agissant des ACR et d'ACF, les notions de pseudonymisation sont sans objet.

### III.1.5. Règles d'interprétation des différentes formes de nom

Les UC (applications, réseaux, machines, organisme extérieurs, …) et les porteurs peuvent se servir des certificats d'AC contenus dans les chaînes de certification autorisées (voir § ci-dessus), pour mettre en œuvre et valider des fonctions de sécurité en vérifiant entre autres les identités (DN) des AC telles que contenues dans les certificats d'AC.

### III.1.6. Unicité des noms

Les identités portées par les ACR et les ACF dans les certificats sont uniques au sein du domaine de certification de l'AC.
Les AC assurent cette unicité par leur processus d'enregistrement.
En cas de différent au sujet de l'utilisation d'un nom pour un certificat, l'AC a la responsabilité de résoudre le différent en question.

### III.1.7. 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

La preuve de la possession de la clé privée par l'AC est réalisée par les procédures de génération (voir § 6.1.2) de la clé privée correspondant à la clé publique à certifier et le mode de transmission de la clé publique (voir § 6.1.3).

### III.2.2. Validation de l'identité d'un organisme

La validation de l'identité de l'organisme est assurée par INCS qui communique les données d'identification à inclure dans l'identité de l'AC (ACR ou ACF) (voir § III.1.1) à l'OSC au préalable de la cérémonie des clés.

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

Ce point est sans objet dans la présente PC.

### III.2.4. Informations non vérifiées du porteur

Les certificats ne contiennent pas d'information non vérifiée.

### III.2.5. Validation de l'autorité du demandeur

Les certificats des AC sont émis au nom d'INCS.

### 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

Le renouvellement de la bi-clé d'une AC (ACR ou ACF) entraîne automatiquement la génération et la fourniture d'un nouveau certificat d'AC.

### III.3.1. Identification et validation pour un renouvellement courant

Les vérifications relatives au renouvellement d'une bi-clé sont effectuées conformément aux procédures initiales (voir III.2 ci-dessus).

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

Les vérifications relatives au renouvellement d'une bi-clé après révocation du certificat de clé publique correspondant sont effectuées conformément aux procédures initiales (voir III.2 ci-dessus).

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

Les demandes de révocation d'une AC (ACR ou ACI) donnent lieu à une authentification du demandeur qui doit être habilité à demander la révocation de l'AC.

# IV. Exigences opérationnelles sur le cycle de vie des certificats

## IV.1. DEMANDE DE CERTIFICAT

### IV.1.1. Origine d'une demande de certificat

INCS est responsable de la création des ACR hors ligne et des ACF en ligne.

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

Une demande de création c'ACR ou d'ACF en ligne contient l'identifiant de l'ACR hors ligne qui doit lui signer son certificat.

## IV.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

INCS identifie et authentifie la demande de création d'ACR et d'ACF en ligne.

### IV.2.2. Acceptation ou rejet de la demande

INCS accepte ou rejette la demande de création d'ACF en ligne. En cas d'acceptation, une cérémonie de clés est alors organisée.

### IV.2.3. Durée d'établissement du certificat

La durée maximale de traitement d'une demande de certificat est définie dans la DPC.

## IV.3. DELIVRANCE DU CERTIFICAT

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

Les ACR et les ACF « en ligne » sont générées pendant une cérémonie des clés (voir VI.1).
Au préalable de la cérémonie des clés, INCS vérifie le contenu des documents de nommage des AC, en termes de complétude et d'exactitude des informations présentes. Ce document est utilisé comme base de réalisation de la cérémonie des clés de création des ACR et des ACF.
Les certificats d'ACR et d'ACF sont signés par l'ACR pendant la cérémonie des clés (voir VI.1).
INCS vérifie en fin de cérémonie de clés d'AC que les certificats d'AC produits sont conformes aux documents de nommage.

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

La notification est effectuée à la fin de la cérémonie des clés de l'AC par la remise en mains propres du certificat d'AC à un représentant de l'AAI présent à la cérémonie des clés.

## IV.4. ACCEPTATION DU CERTIFICAT

### IV.4.1. Démarche d'acceptation du certificat

L'AC vérifie que le certificat contient les informations décrites dans le document de nommage signé par INCS. Dès que l'AC confirme l'adéquation entre le certificat et le document de nommage, l'AC accepte le certificat d'AC émis.

### IV.4.2. Publication du certificat

Les certificats d'AC sont publiés par le service de publication.

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

Ce point est sans objet dans la présente PC.

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

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

Les utilisations des bi-clés et des certificats sont définies au § I.4 ci-dessus. 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 (voir § VI.1.7 ci-dessous).

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

Les certificats d'AC ne peuvent être utilisés par un UC qu'à des fins de validation d'une chaîne de confiance.
Il est de la seule responsabilité de l'UC de s'assurer de la validité des certificats délivrés par l'ACR ou l'ACF à l'aide des listes de certificats d'autorité révoquées publiées par le SP.

## 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 de l'ACR ou ACF).
Dans le cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. Cette opération n'est donc pas autorisée par la présente PC.

## 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,
- pour que l'ACR puisse continuer à délivrer des certificats d'ACF d'une durée constante,
- en cas de compromission, suspicion de compromission, vol, dysfonctionnement ou perte des moyens de reconstruction de la clé privée d'une des AC.

Le changement de bi-clé entraîne le changement de certificat, la procédure à suivre est identique à la procédure initiale de certification décrite aux § III.2, § IV.1, § IV.3 et § IV.4 ci-dessus.

## 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.

## IV.9. REVOCATION ET SUSPENSION DES CERTIFICATS

### IV.9.1. Causes possibles d'une révocation

#### *1. Révocation d'ACR*

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

- cessation d'activité de l'ACR,
- compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'ACR (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'ACR,
- changement d'informations dans le certificat,
- obsolescence de la cryptographie au regard des exigences de l'ANSSI.

#### *2. Révocation d'ACF*

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

- cessation d'activité de L'ACF,
- compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'ACF (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,
- non-respect de la politique de certification et de la déclaration des pratiques de certification de l'ACF,
- changement d'informations dans le certificat,
- obsolescence de la cryptographie au regard des exigences de l'ANSSI.

### IV.9.2. Origine d'une demande de révocation

La révocation d'un certificat d'AC (ACR ou ACF) ne peut être demandée que par l'entité responsable de l'AC considérée c'est-à-dire INCS, ou par les autorités judiciaires via une décision de justice.

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

Lorsque la décision est prise de révoquer l'une des AC opérationnelles appartenant à la chaîne de confiance d'un certificat de Porteur (ACF ou ACR), les actions suivantes sont réalisées :

- Tous les certificats des porteurs en cours de validité, délivrés par cette AC sont révoqués et inclus dans la LCR,
- Les responsables des applications utilisatrices et les porteurs sont notifiés,
- Une demande de révocation pour le certificat de l'AC est transmise à l'AC racine à laquelle l'AC est subordonnée.

Lorsque la décision est prise de révoquer l'un des certificats de l'AC et que le motif de cette révocation est la compromission (avérée ou supposée) de la clé privée correspondante, les actions suivantes sont réalisées :

- Tous les certificats des porteurs en cours de validité, délivrés depuis la date de compromission (assortie d'une période de sûreté) par cette AC sont révoqués et inclus dans la LCR,
- Les responsables des applications utilisatrices et les porteurs sont notifiés,
- Une demande de révocation pour le certificat de l'AC est transmise à l'AC racine à laquelle l'AC est subordonnée.

S'il y a lieu, l'émission de certificats « de remplacement » pour les Porteurs sera assurée dans les meilleurs délais.

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

L'AAI doit immédiatement demander la révocation d'un des certificats d'AC dès lors qu'une cause de révocation telle que définie au § IV.9.1 est identifiée.

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

L'AC traite les demandes de révocation dès que possible suivant sa réception et de préférence immédiatement et dans un délai maximum de 24 h.

### 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, dLCR, 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 LAR

Les LAR sont émises tous les ans. En cas de révocation d'AC, les LAR sont publiées dès qu'elles sont générées.

### IV.9.8. Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Voir § IV.9.6.

### IV.9.9. Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Voir § IV.9.6.

### IV.9.10. Autres moyens disponibles d'information sur les révocations

Sans objet

### IV.9.11. Exigences spécifiques en cas de compromission de la clé privée

Les mesures mises en œuvre par les ACR sont définies dans la DPC.

### IV.9.12. 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

La fonction de consultation de l'état des certificats, mise à la disposition des utilisateurs de certificats, dispose d'un mécanisme de consultation libre des LAR. Ces LAR sont au format V2, publiées en http aux adresses référencées au § II.2.

### IV.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7. Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4 heures et une durée maximale totale d'indisponibilité par mois de 16 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'ACR et l'ACF avant la fin de validité du certificat, pour une raison ou une autre, le certificat de l'AC doit être révoqué.

## IV.12. SEQUESTRE DE CLES ET RECOUVREMENT

Ce point est sans objet dans la présente PC.

### IV.12.1. Politique et pratiques de recouvrement par séquestre de clés

Ce point est sans objet dans la présente PC.

### IV.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Ce point est sans objet dans la présente PC.

# V. Mesures de sécurité non techniques

## V.1. MESURES DE SECURITE PHYSIQUES

### V.1.1. Situation géographique et construction des sites

Les cérémonies de clés sont effectuées sur le site de l'OSC.
Le site d'exploitation de l'OSC respecte les règlements et normes en vigueur et son installation tient compte des résultats de l'analyse de risques, du métier d'OSC, par exemple certaines exigences spécifiques de type inondation, explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques,...) réalisées par l'OC.
Le site d'exploitation de l'OSC de l'IGC ACR se trouve géographiquement sur le territoire français métropolitain.
Les AC en ligne sont exploitées sur le site de l'Imprimerie Nationale.
L'installation est redondée et installée dans deux salles d'hébergement distinctes.
La construction du site respecte les règlements et normes en vigueur. Son installation tient compte des résultats de l'analyse de risques, du métier d'opérateur selon la méthode EBIOS.
De plus, le site a été certifié OIV (Opérateur d'importance vitale).
Dans ce cadre, les risques spécifiques de type inondation, explosion et attaque terroriste ont été spécifiquement étudiés.

### 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 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 renforcée 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 seront précisés dans la DPC.
*Nota* - On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions.

### 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 continuité des services délivrés.
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).
Les supports (papier, disque dur, clés USB, CD, etc.) correspondant à ces informations sont traités et conservés conformément à ces besoins de sécurité.
Les précisions quant aux modalités de conservation des supports sont fournies dans la DPC.

### V.1.7. Mise hors service des supports

Les supports sont détruits en fin de vie.

### 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.
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.

### 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. La DPC précise le nombre d'exploitants 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'ACR et doivent être 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'ACR et être 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.

### 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 doit être 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 doivent avoir 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 doit recevoir 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

Les sanctions en cas d'actions non autorisées sont précisées dans la DPC correspondante à cette PC.

### 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 doit également respecter les exigences du présent chapitre § V.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

### V.3.8. Documentation fournie au personnel

Chaque personnel doit disposer 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 doit lui être remis la ou les politique(s) de sécurité qui le concernent.

## 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, doivent rendre 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 doit, au minimum, journaliser les événements tels que décrit ci-dessous sous forme électronique. La journalisation doit être 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,
- Evénements 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,

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, …).

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

- Réception d'une demande de certificat (initiale et renouvellement),
- Validation / rejet d'une demande de certificat,
- Evénements liés aux clés de signature et aux certificats d'AC (génération, sauvegarde / récupération, destruction, …),
- Génération des certificats des porteurs,
- Publication et mise à jour des informations liées aux AC,
- Réception d'une demande de révocation,
- Validation / rejet d'une demande de révocation,
- Génération puis publication des LAR.

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).

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.
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).

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

Les journaux d'événements doivent être contrôlés et analysés par un responsable de sécurité afin d'identifier les anomalies liées à des tentatives d'échec (voir § V.4.8).

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

Les journaux d'évènements doivent être conservés sur site pendant au moins 5 ans. Ils doivent être 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 doit être 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 doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les journaux d'évènements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

### V.4.5. Procédure de sauvegarde des journaux d'événements

La journalisation doit être 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 doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.
Les journaux d'évènements doivent être 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

Le journal d'événements permet d'imputer chaque opération sensible à toute personne, organisme ou système ayant un rôle identifié dans la présente PC.

### V.4.8. Evaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC doit être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.
Les journaux d'évènements doivent être contrôlés au moins 1 fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.
Les journaux doivent être analysés dans leur totalité au moins 1 fois par semaine et dès la détection d'une anomalie. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) doit être effectué au moins 1 fois par mois, 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,
- La déclaration des pratiques de certification,
- Les certificats tels qu'émis ou publiés,
- Les registres et scripts de cérémonie de clés,
- Les journaux d'événements des différentes composantes de l'IGC.

### V.5.2. Période de conservation des archives

**Certificats d'ACR et d'ACF**

La période de conservation de ces certificats, ainsi que les LAR produites est de 5 ans après leur expiration.

**Journaux d'événements**

Les journaux d'événements tels que traités au § V.4 est de 10 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

Le responsable de l'OSC et l'Opérateur de certification 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 chapitre § VI.8 précise les exigences en matière de datation et d'horodatage.

### V.5.6. Système de collecte des archives

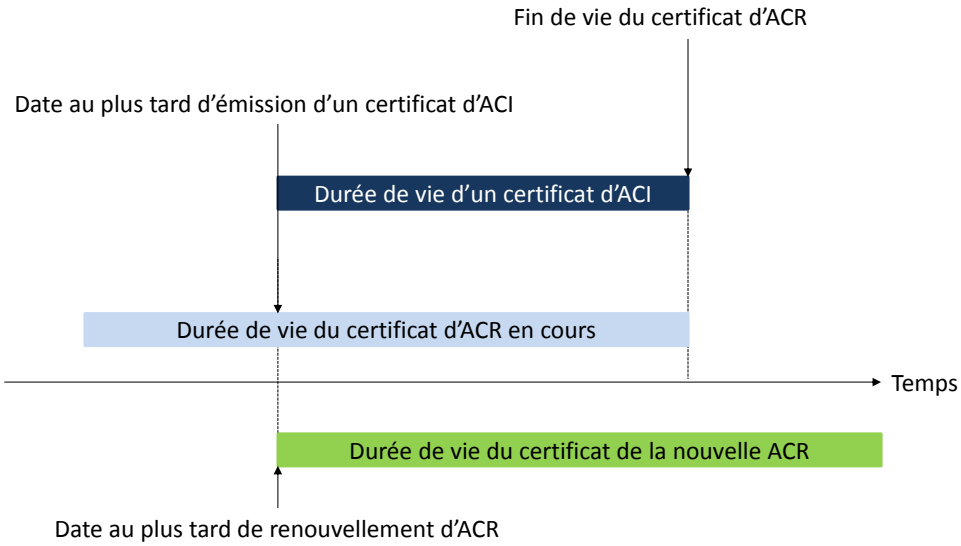
Le système devra assurer la collecte des archives en respectant le niveau de sécurité des archives tel qu'exigé au § V.5.3.

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

Les archives papier ou électronique doivent pouvoir être récupérées par l'ACR dans un délai de 48 heures ouvrées.

## V.6. CHANGEMENT DE CLE D'AC

La durée de vie d'un certificat d'AC est déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationale ou internationale compétentes en la matière. La DPC précise les standards utilisés.
Une AC ne peut pas générer de certificats dont la durée de vie dépasse la période de validité de son certificat d'AC. C'est pourquoi, la bi-clé d'une AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats émis.
Dès qu'une nouvelle clé privée est générée pour l'AC, seule celle-ci est utilisée pour générer de nouveaux certificats de porteurs. Le précédent certificat d'AC reste valable pour valider le chemin de certification des anciens certificats émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats porteurs émis à l'aide de cette bi-clé.




Par ailleurs, l'ACR 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 doit mettre 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 d'une ACR ou d'une ACF, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès réception et la publication de l'information de révocation du certificat, s'il y a lieu, doit être 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 doit informer tous les porteurs et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords. De plus tous les certificats concernés doivent être 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 doit être testé  au moins une fois par an et les mesures correctives, le cas échéant, doivent être mises en place.

### V.7.3. Procédure en cas de reprise 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 doit être immédiatement révoqué comme précisé au chapitre § IV.9. De plus, l'AC respecte les engagements suivants :

- Informer sans délai les entités suivantes de la compromission : tous les porteurs, les entités avec lesquelles l'AC a passé des accords et les tiers 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 doivent disposer 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. chapitre § 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 doit garantir 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 devront être révoqués sans délai et les entités informées de la révocation des certificats.

# VI. Mesures de sécurité techniques

## VI.1. GENERATION ET INSTALLATION DE BI-CLES

### VI.1.1. Génération des bi-clés

La génération des bi-clés associées aux certificats d'AC (ACR ou ACF) se déroule lors d'une cérémonie de clés à l'aide d'une ressource cryptographique matérielle qualifiée au niveau renforcée.
Les cérémonies de clés se déroulent sous le contrôle d'au moins trois personnes dans des rôles de confiance (maître de cérémonie et témoins). Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement approuvé par l'ACR. 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 secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur.

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

La clé privée des AC reste et est mise en œuvre dans les locaux de l'Opérateur de certification.

### VI.1.3. Transmission de la clé publique à l'ACR

Les clés publiques des AC sont générées lors des cérémonies de clés et signées par les ACR

### 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 doivent être diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.
Les clés publiques des ACR sont transmises dans un certificat auto signé. Ce moyen de transmission ne permettant pas de garantir leur origine, la diffusion du certificat auto signé s'accompagne de l'empreinte numérique du certificat et d'une déclaration d'appartenance de la clé publique.
Ces informations peuvent être récupérées sur le site du Groupe Imprimerie Nationale.

### 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.
Les ACR d'INCS ainsi que les ACF utilisent l'algorithme RSA avec la fonction de hachage SHA-256 dont l'OID est 1.2.840.113549.1.1.11. La taille des bi-clés en ligne est de 2048 bits. La taille de la bi-clé d'une AC « hors ligne » est de 4096 bits.

### 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 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 d'une clé privée d'ACF et du certificat associé est strictement limitée à la signature de certificats, de LCR et de réponses OCSP.

## 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 ressources cryptographiques des AC sont qualifiées au niveau renforcé par l'ANSSI.

### VI.2.2. Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la bi-clé est traitée au chapitre § VI.1.1, l'activation de la clé privée au chapitre § VI.2.8 et sa destruction au chapitre § VI.2.10.
Le contrôle des clés privées de signature des 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.2.3. Séquestre de la clé privée

Les clés privées d'AC (ACR ou ACF) ne font jamais l'objet de séquestre.

### VI.2.4. 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.

### VI.2.5. Archivage de la clé privée

Les clés privées d'AC ne sont jamais archivées.

### VI.2.6. Transfert de la clé privée vers / depuis le module cryptographique

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.

### VI.2.7. Stockage de la clé privée dans un module cryptographique

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

### VI.2.8. Méthode d'activation de la clé privée

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

### VI.2.9. Méthode de désactivation de la clé privée

Les ressources cryptographiques matérielles dans lesquelles des clés d'AC ont été activées ne sont pas laissées sans surveillance ou accessible 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.

### VI.2.10. Méthode de destruction des clés privées

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.

### VI.2.11. Niveau de qualification du module cryptographique et des dispositifs d'authentification, de signature et de chiffrement

Les modules cryptographiques utilisés par l'ACR et les ACF sont certifiés au niveau EAL4+ selon les critères communs.

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

### VI.3.1. Archivage des clés publiques

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

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

Comme une AC ne peut émettre de certificats porteurs d'une durée de vie supérieure à celle de son propre certificat, la bi-clé et le certificat auquel elle correspond sont renouvelés au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats porteurs émis.

## VI.4. DONNEES D'ACTIVATION

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

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 de 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.

### VI.4.2. Protection des données d'activation

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.

### 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 :

- Authentification des rôles de confiance ;
- Contrôle d'accès discrétionnaire ;
- Interdiction de la réutilisation d'objets ;
- Exige l'utilisation de la cryptographie lors des communications ;
- Requiert l'identification des utilisateurs ;
- Assure la séparation rigoureuse des tâches ;
- Fournit une autoprotection du système d'exploitation.

### VI.5.2. Niveau de qualification des systèmes informatiques

Quand un composant d'ACR 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

Le contrôle des développements des systèmes s'effectue comme suit :

- Des matériels et des logiciels achetés de manière à réduire les possibilités qu'un composant particulier soit altéré ;
- Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise aupoint 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 ;
- Les matériels et logiciels sont dédiés aux activités d'IGC. Il n'y a pas d'autre application, matériel, connexion réseau,

ou composant logiciels installés qui ne soit pas dédiés aux activités d'IGC ;
- 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 seront installés 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, on vérifie que le logiciel de l'IGC est bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

### 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

Les composantes des ACR « hors ligne » ne sont jamais connectées à un réseau. Ce point est donc sans objet pour la présente PC.
Les mesures de sécurité réseau concernant les ACF seront traitées dans les PC de ces ACF.

## VI.8. HORODATAGE / SYSTEME DE DATATION

Il n'y a pas d'horodatage utilisé par l'ACR mais une datation des évènements qui permet, à partir d'une date fournie par le système d'exploitation de l'ACR de séquencer les événements.
Des procédures automatiques ou manuelles doivent être utilisées pour maintenir l'heure du système. Les réglages de l'horloge sont des événements susceptibles d'être audités.

# VII. Profil des certificats, OCSP et des LCR

## VII.1. PROFILS DE CERTIFICATS

Les certificats émis par l'AC sont des certificats au format X.509 v3 (populate version field with integer "2"). Les champs des certificats porteurs et AC sont définis par le RFC 5280.

### VII.1.1. Extensions de certificats

#### *1. Certificats d'ACR « hors ligne »*

Les principaux champs des certificats des ACR « hors ligne » sont les suivants :

| **Champ de base** | **Valeur** |
|---|---|
| Version | 2 (=version 3) |
| Serial Number | Défini par l'outil |
| Issuer DN | CN = Imprimerie Nationale (Elémentaire / Sécurisée / Renforcée)<br>OU = SIREN<br>O = Groupe Imprimerie Nationale<br>C = FR |
| Subject DN | |
| PublicKeyAlgorithm | sha256WithRSAEncryption |
| Taille des clés | 4096 bits |
| Durée de vie | 12 ans |

Le certificat d'ACR contient les extensions suivantes :

- Authority Key Identifier (non critique) ;
- Basic Constraints (critique) ;
- Certificate Policies (non critique) ;
- CRL Distribution Points (non critique) ;
- Key usage (critique) ;
- Subject Key Identifier (non critique).

#### *2. Certificats d'AC « en ligne »*

Les principaux champs des certificats des AC « en ligne » sont les suivants :

| **Champ de base** | **Valeur** |
|---|---|
| Version | 2 (=version 3) |
| Serial Number | Défini par l'outil |
| Issuer DN | CN = Imprimerie Nationale (Elémentaire / Sécurisée / Renforcée)<br>OU = SIREN<br>O = Groupe Imprimerie Nationale<br>C = FR |
| Subject DN | |
| PublicKeyAlgorithm | sha256WithRSAEncryption |
| Taille des clés | 2048 bits |
| Durée de vie | 6 ans |

Par défaut les AC « en ligne » sont signée par l'ACR. Le certificat d'AC « en ligne » contient les extensions suivantes :

- Authority Key Identifier (non critique) ;
- Basic Constraints (critique) ;
- Certificate Policies (non critique) ;
- CRL Distribution Points (non critique) ;
- Key usage (critique) ;
- Subject Key Identifier (non critique)

### VII.1.2. Identifiant d'algorithme

L'identifiant d'algorithme utilisé est Sha-256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}.

### 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 d'AC (ACR ou ACI) ne contiennent pas l'OID de la présente PC (voir & I.2).

### 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 « Cerificate Policies »

Pas d'exigence formulée

## VII.2. PROFILS DE LAR

Toutes les AC « hors ligne » ont une LAR.
Les caractéristiques des LAR sont :

| | |
|---|---|
| **Caractéristiques des LAR** | Durée de validité : 14 mois.<br>Périodicité de mise à jour : à chaque cérémonie de clé d'AC<br>Version de la LAR (v1 ou v2) : v2<br>Extensions : Numéro de la LAR et AKI<br>URL http de publication : Voir § II.2 |

## VII.3. PROFIL OCSP

Ce point est sans objet dans la présente PC.

# VIII. Audit de conformité et autres évaluations

Les audits et les évaluations concernent ceux que doit réaliser, ou faire réaliser l'AAI afin de s'assurer que l'ensemble de son IGC est bien conforme à ses engagements affichés dans cette PC et aux pratiques identifiées dans sa DPC.

## 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 doit procéder à un contrôle de conformité de cette composante. L'AAI doit également procéder au moins une fois tous les deux ans à un contrôle de conformité de l'ensemble de son IGC.
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 le COFRAC en France (Se reporter au [PROG_ACCRED]) conformément à [QPSCe] et 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'ACR 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.

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.

# IX. Autres problématiques métiers et légales

## IX.1. TARIFS

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

## 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 :

- la DPC de l'ACR et des procédures associées,
- les clés privées de l'ACR et de ses composantes,
- les clés privées des ACF,
- les données d'activation associées aux clés privées d'AC (ACR ou ACF),
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les éléments relatifs à la cérémonie des clés,
- les causes de révocations, sauf accord explicite de l'ACR,
- 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 chapitre § 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.

## 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 »..

### IX.4.2. Informations à caractère personnel

L'AC considère que les informations suivantes sont des informations à caractère personnel :

- Identité des porteurs de secrets ;
- Demande (renseignée) de certificat ;
- Demande (renseignée) de révocation ;
- Motif de révocation.

### 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 restitutions d'informations aux autorités judiciaires et administratives.

### 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, du certificat 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,
- 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,
- respecter les accords ou contrats qui les lient entre elles,
- 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. Autorités de certification

Les AC ont pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour une ACF donnée ;
- Garantir et maintenir la cohérence de sa DPC et sa PC ;
- 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,
- Possibilité de diligenter des audits
- Prévoir la sensibilisation des différents acteurs.

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. 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 politique de certification.

### IX.6.3. Porteurs de certificats

Les porteurs des certificats des ACF ne sont pas concernés par la présente PC.

### IX.6.4. Utilisateurs de certificats

Les utilisateurs de certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Pour chaque utilisateur de certificat de la chaîne de certification, du certificat du porteur jusqu'à 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.6.5. Autres participants

La DPC précisera les exigences des autres participants si nécessaire.

## IX.7. LIMITE DE GARANTIE

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

- L'identification et l'authentification de l'ACR avec son certificat ;
- L'identification et l'authentification des ACF avec les certificats d'AC générés par l'ACR ;
- La gestion des certificats correspondant 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 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

L'ACR garantit qu'elle est conforme à la présente PC ainsi qu'à l'état actuel et stable de l'art.
La responsabilité de l'ACR 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'ACR devant être dûment prouvée ;
- en cas de compromission prouvée, entièrement et directement imputable à l'ACR.

L'ACR 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.

L'ACR 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'ACR 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'ACR 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 qu'INCS pourrait être amenée à versée au titre d'un manquement à ses obligations ne sauraient dépasser le(s) montant(s) prévus à l'article 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'ACR est établie et a causé directement un dommage, INCS indemnisera la personne/entité 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 des ACR doit rester 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 présente PC peut entraîner, en fonction des évolutions demandées, la nécessité pour l'AAI de faire évoluer la PC qu'elle met en œuvre.

En fonction de la nature et de l'importance des évolutions apportées à la présente PC, le délai de mise en conformité sera arrêté par l'AAI.

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 devra 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.

## IX.12. AMENDEMENTS A LA PC

### IX.12.1. Procédures d'amendement

L'AAI révise sa PC et sa DPC à chaque évolution des systèmes de l'IGC et chaque fois qu'une évolution remarquable de l'état de l'art le justifie.
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.

### 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.

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

Les OID des ACR et ACF étant inscrits 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.

## 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 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 chapitre § I.6 ci-dessus.

## IX.16. DISPOSITIONS DIVERSES

### IX.16.1. Accord global

Sans objet

### IX.16.2. Transfert d'activités

Voir chapitre § 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.