IN GROUPE

Politique de Certification

Certificat de Porteur

Document sécurité

Mode de diffusion	**EXTERNE**
Statut du document	**VALIDE**
Date d'application	01/01/2020

HISTORIQUE DES VERSIONS

Version	Date	Auteur	Nature de la révision Paragraphes modifiés
1.0	09/02/2017	Imprimerie Nationale	Version initiale
1.1	23/06/2017	Imprimerie Nationale	Corrections apportées suite à l'audit LSTI
1.2	15/12/2017	Imprimerie Nationale	Modifications suite à audit LSTI
2.0	04/07/2019	Franck Leroy (IN Groupe)	Restructuration

SOMMAIRE

I Introduction

I.1 PRESENTATION GENERALE

I.1.1 Objet du document

IN Groupe a mis en place une Infrastructure de Gestion de Clés (IGC) afin de délivrer des certificats électroniques conformes au *Référentiel Général de Sécurité* (RGS) et à la règlementation européenne eIDAS.

IN Groupe offre ainsi des services d'émission de certificats ayant pour objectif la mise en œuvre des fonctions d'authentification et de Signature. IN Groupe est un PSCE (Prestataire de Service de Certification Électronique).

Le présent document constitue la politique de certification (PC) des AC IN Groupe. Elle décrit les différents niveaux de responsabilité, les mesures de sécurité (techniques, organisationnelles...) ainsi que les profils des certificats. Elle expose également les engagements des AC IN Groupe dans le cadre de la fourniture de ses services de certification électronique pour des porteurs, en conformité avec les exigences des PC type qui ont été rédigées dans le cadre du Référentiel Général de Sécurité.

Ce document incorpore les informations publiques des pratiques de certification. Les détails relatifs aux pratiques sont rédigés dans un document séparé, qui peut être consulté sur demande au point de contact de l'AC (cf. I.6.2), qui communiquera les modalités de consultation.

L'IGC est composée d'une autorité racine (ACR) et de plusieurs autorités hiérarchiquement dépendantes (Autorité de Certification Intermédiaire).

La présente DPC ne couvre que les AC Intermédiaire
- Imprimerie Nationale Substantiel Personnel, et
- Imprimerie Nationale Élevé Personnel.

Ces AC délivrent deux types de certificats :
- Des certificats d'authentification, et
- Des certificats de signature.

Les certificats sont exclusivement délivrés aux personnes physiques qui les utilisent (ainsi que les clés privées associées) dans le contexte de leurs activités en relation avec l'Entité Cliente identifiée dans le certificat et avec laquelle ces personnes physiques ont un lien contractuel (cf. définition du Porteur de certificat au § I.3.7). Les Entités Clientes à laquelle sont rattachées les personnes physiques peuvent appartenir au secteur privé ou au secteur public.

La structure de cette PC est conforme au [RFC3647] « *X.509 Public Key Infrastructure Certificate Policy Certification Practice Statement Framework* » de *l'Internet Engineering Task Force* (IETF) et s'appuie sur la PC-Type [RGS_A_2] (certificats électroniques de personne) du *Référentiel Général de Sécurité* V2.0 élaborée par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) en liaison avec la SGMAP (Secrétariat Général pour la Modernisation de l'Action Publique).

Compte tenu de la complexité de lecture de la PC pour des Porteurs ou des Utilisateurs de Certificats non spécialistes du domaine, IN Groupe publie des Conditions Générales d'Utilisation (*PKI Disclosure Statement)* définis dans la norme ETSI EN 319411-1.

I.1.2 Conventions de rédaction

De manière à mettre en exergue les règles spécifiques à un niveau de sécurité, à un type d'usage ou à un type de porteur, celles-ci seront présentées dans un encadré, le titre du cadre précisant son périmètre d'application (usage du certificat électronique, niveau de sécurité et type de porteur du certificat électronique). La forme est la suivante :

Nom de L'Autorité de Certification	
Usage	Niveau de sécurité

Les exigences qui ne sont pas encadrées s'appliquent de manière identique à toutes les AC IN Groupe.

I.2 IDENTIFICATION DU DOCUMENT

Cette PC est identifiée dans le tableau suivant par les OID suivants :

AC Imprimerie Nationale Substantiel Personnel	
OID	Niveau de sécurité
Authentification : 1.2.250.1.295.1.1.8.6.1.101.1	RGS 1 étoile, ETSI NCP
Signature : 1.2.250.1.295.1.1.8.6.1.102.1	RGS 1 étoile, ETSI QCP-n
Authentification : 1.2.250.1.295.1.1.8.0.1.101.0	RGS 2 étoiles, ETSI NCP+
Signature : 1.2.250.1.295.1.1.8.0.1.102.0	RGS 2 étoiles, ETSI QCP-n+qscd

AC Imprimerie Nationale Elevé Personnel	
OID	Niveau de qualification
Signature : 1.2.250.1.295.1.1.20.7.1.102.1	RGS 1 étoile, ETSI QCP-n
Signature : 1.2.250.1.295.1.1.20.0.1.102.0	RGS 3 étoiles, ETSI QCP-n+qscd

La date d'entrée en application de la présente PC est le 1er Janvier 2020 (01/01/2020).

I.3 DEFINITIONS ET ACRONYMES

I.3.1 Acronymes

AC Autorité de Certification
ACR Autorité de Certification Racine
AE Autorité d'Enregistrement
AGP Autorité de Gestion de la Politique
ANSSI Agence Nationale de la Sécurité des Systèmes d'information
CMS *Credentials Management System*
DPC Déclaration des Pratiques de Certification

HSM	*Hardware Security Module*
ICD	*International Code Designator*
IGC	Infrastructure de Gestion de Clés
IN Groupe	Groupe Imprimerie Nationale
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization*
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
LDAP	*Lightweight Directory Access Protocol*
LRAR	Lettre recommandée avec accusé de réception
MC	Mandataire de Certification
OID	*Object Identifier*
PC	Politique de Certification
OCSP	Online Certificate Status Protocol
OSC	Opérateur de Services de Certification
QSCD	Qualified Signature Creation Device
RL	Responsable légal
RSA	Rivest Shamir Adleman
SHA-256	*Secure Hash Algorithm 256*
SP	Service de Publication
UC	Utilisateur de Certificat

I.3.2 Définitions

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 de Certificats se fient pour créer et attribuer des certificats. [ISO/IEC 9594-8; ITU-T X.509].

Autorité d'Enregistrement (AE) : Cf. chapitre 1.3.1.

Autorité de Gestion de la Politique (AGP) : L'autorité de gestion de la politique IN Groupe (AGP) est composée d'un COMITÉ DE SURVEILLANCE de l'IGC au sein d'IN Groupe. Ce comité est responsable des AC IN Groupe 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, des conditions générales d'utilisation et des procédures mises en œuvre par les composantes de l'IGC. L'AGP valide la PC. Elle s'assure également de la cohérence de la DPC par rapport à la PC. Elle autorise et valide la création et l'utilisation des composantes de l'AC. Elle suit les audits et les contrôles de conformité effectués par les composantes de l'IGC, décide des actions à mener et veille à leur mise en application.

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

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

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

Certificat auto signé : certificat d'AC signé par la clé privée de cette même AC.

Chemin de certification : (ou chaîne de confiance, ou chaîne de certification) chaîne constituée de multiples certificats nécessaires pour valider un certificat.

Clé privée : clé de la bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

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

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

Compromission : violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de la sécurité de cette clé privée.

Confidentialité : La propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus [ISO/IEC 13335-1:2004].

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

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

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

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

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

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

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

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

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

Période de validité d'un certificat : La période de validité d'un certificat est la période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 5280]. En dehors de cette période (avant la date de début de validité et après la date de fin de validité), le certificat est réputé non valide.

Plan de secours (après sinistre) : plan défini par une AC pour remettre en place tout ou partie de ses services d'IGC après qu'ils aient été endommagés ou détruits à la suite d'un sinistre, ceci dans un délai défini dans l'ensemble PC.

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

Politique de Certification (PC) : ensemble de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications possédant des exigences de sécurité communes. [ISO/IEC 9594-8; ITU-T X.509].

Politique de sécurité : ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].

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

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

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

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

Validation de certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de certification (AC) et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC et la vérification de la chaine de certification. La validation d'un certificat électronique nécessite au préalable d'approuver le certificat de l'autorité Racine (certificat auto-signé).

I.4 ENTITES INTERVENANT DANS L'IGC

La notion d'autorité de certification (AC) telle qu'utilisée dans le présent document est définie au § I.3.1.

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

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

- Génération des bi-clés : Ce service génère la bi-clé des futurs Porteurs et remet la clé publique à certifier au service de génération des certificats
- Génération de certificats : Ce service génère les certificats électroniques des futurs Porteurs à partir des informations fournies par l'autorité d'enregistrement.
- Révocation : Ce service traite les demandes de révocation de certificats et détermine les actions à mener dont la génération de la liste des certificats révoqués (LCR ou CRL).
- Publication : Ce service met à disposition des Utilisateurs de Certificats (UC) et des Porteurs ou responsables de certificats les informations nécessaires à l'utilisation des certificats émis par les AC (Conditions Générales d'Utilisation, PC, certificats d'AC, …) ainsi que les résultats des traitements du service de gestion des révocations de certificats (LCR).

La présente PC définit les exigences de sécurité et décrit l'organisation opérationnelle pour toutes les fonctions décrites ci-dessus pour délivrer des certificats aux Porteurs.

I.4.1 Autorités de certification

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

I.4.2 Autorité d'enregistrement

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

L'AE est sous la responsabilité d'IN Groupe.

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

I.4.3 Porteurs de certificats

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

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

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

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

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

I.4.4 Utilisateurs de certificats

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

L'UC utilise un certificat et un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le Porteur du certificat.

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

<u>Un Utilisateur (ou accepteur) de Certificats d'authentification peut être notamment :</u>

- Un service en ligne qui utilise un certificat et un dispositif de vérification d'authentification soit pour valider une demande d'accès faite par le porteur du certificat dans le cadre d'un contrôle d'accès, soit pour authentifier l'origine d'un message ou de données transmises par le porteur du certificat ;
- Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification d'authentification afin d'en authentifier l'origine.

<u>Un Utilisateur (ou accepteur) de Certificats de signature peut être notamment :</u>

- Un service en ligne qui utilise un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le porteur du certificat ;
- Un usager qui signe électroniquement un document ou un message ;
- Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification de signature

afin de vérifier la signature électronique apposée par le porteur du certificat sur ce message ou sur ces données.

I.4.5 Autres participants

I.4.5.1 Composantes de l'IGC

La décomposition en fonctions de l'IGC est présentée au chapitre I.4.1 ci-dessus. Les composantes de l'IGC mettant en œuvre ces fonctions sont présentées dans la DPC de l'AC.

Un opérateur technique est chargé de la mise à disposition et de l'exploitation des clés des ACF pour les besoins de génération et révocation de certificats.

L'opérateur technique dispose d'une infrastructure matérielle et logicielle lui permettant de générer et émettre des certificats, conformément aux PC des ACF.

Il est en charge du bon fonctionnement de l'infrastructure des ACF et de la sécurité des moyens informatiques et techniques, de la sécurité des personnels et des locaux.

L'opérateur technique est tenu de respecter la présente PC.

I.4.5.2 Mandataire de certification

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

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

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

Tout MC doit être formellement désigné par l'un des représentants légaux de l'Entité.

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

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

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

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

I.4.5.3 Le service de publication

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

Le SP agit conformément à la PC.

I.4.5.4 Entité cliente

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

I.5 USAGE DES CERTIFICATS

I.5.1 Domaines d'utilisation applicables

I.5.1.1 Bi-clés et certificats des porteurs

La présente PC traite des bi-clés et certificats émis par l'AC à destination des catégories de Porteurs identifiées au § I.3.7 (personnes physiques) afin que ces dernières puissent s'authentifier ou signer électroniquement des données (documents ou messages) dans le cadre d'échanges dématérialisés avec les catégories d'Utilisateurs de Certificats identifiées au chapitre § I.3.8 ci-dessus. Une telle signature électronique apporte, outre l'authentification du signataire et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

La vérification de la signature d'un document signé avec un certificat de porteur garantit :

- L'origine du document : authentification de la personne qui a créé ou émis le document
- L'intégrité du document : le destinataire est assuré que le contenu du document n'a pas été modifié par un tiers
- Le cas échéant, l'antériorité (existence du document avant une date certaine), si la signature est horodatée : un jeton d'horodatage a été généré par une Autorité d'Horodatage et associé au document en plus de la signature électronique

Remarques :

- Il est expressément entendu qu'un Porteur de certificat ne peut user de sa clé privée et de son certificat qu'à des fins d'authentification ou de signature tel que définis dans l'usage de son certificat. En cas d'usage non autorisé d'une clé privée et de son certificat par son Porteur, la responsabilité de ce dernier pourrait être engagée.
- Il est également expressément entendu que l'Utilisateur du certificat ne peut faire confiance à ce dernier que dans le cadre d'échanges dématérialisés avec le Porteur. La signature électronique apporte, outre des garanties d'authenticité et d'intégrité des données signées, la garantie du consentement du signataire quant au contenu de ces données.

I.5.1.2 Bi-clés et certificats d'AC et de composantes

L'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (hiérarchie d'AC).

La bi-clé de l'AC sert à signer les certificats et les listes de certificats révoqués (LCR) qu'elle émet. Cette bi-clé est exclusivement utilisée à cette fin.

L'IGC dispose de bi-clés et de certificats correspondant supplémentaires, signées par l'AC afin de signer les réponses OCSP

I.5.2 Domaines d'utilisation interdits

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

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

I.6 GESTION DE LA PC

I.6.1 Entité gérant la PC

La présente politique de certification est sous la responsabilité d'IN Groupe.

I.6.2 Point de contact

Point de contact :

IN Groupe
Responsable de l'AC
104, avenue du Président Kennedy
75016 Paris
contact.passin@ingroupe.com

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

I.6.3 Entité déterminant la conformité d'une DPC avec cette PC

L'AGP à travers son COMITE DE SURVEILLANCE détermine la conformité des pratiques de la PC. Elle procède ainsi à des contrôles de conformité et à des audits afin d'autoriser ou non l'émission des certificats. Les audits peuvent être confiés à une société tierce choisie par l'AGP.

I.6.4 Procédures d'approbation de la conformité de la DPC

Les pratiques documentées de la PC sont approuvées par l'AGP à l'issue d'un processus d'approbation élaboré par l'IN Groupe.
Cette PC sera revue régulièrement (au moins une fois par an) par le comité de surveillance qui constitue l'AGP pour :

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

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

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

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

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

II.2 INFORMATIONS DEVANT ETRE PUBLIEES

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

- Les PC en application
- Les CGU
- Les formulaires et PV
- Les certificats d'AC
- Les liste de révocations

Sur le site web : http://www.imprimerienationale.fr/GIN/PC

Sauf indications contraires, les autres informations sont réputées confidentielles.

IN Groupe ne publie pas les détails qu'elle juge sensibles voire confidentiels dans sa PC.

Ces informations sont reportées dans un document confidentiel répertoriant l'ensemble des procédures techniques et non-techniques appliquées au sein de l'IGC.

Les Conditions Générales d'Utilisation décrivent entre autres :

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

II.3 DELAIS ET FREQUENCE DE PUBLICATION

Les délais et les fréquences de publication dépendent des informations concernées :

- Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), l'information est publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.
- Pour les certificats d'AC, ils sont diffusés préalablement à toute émission de certificats et/ou de LCR correspondants sous délai de 24 heures.

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

Les sites web de publication sont accessibles 7j/7 et 24h/24.

II.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

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

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (basé sur une authentification à deux facteurs).

III Identification et authentification

III.1 NOMMAGE

III.1.1 Types de noms

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

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

III.1.2 Nécessité d'utilisation de noms explicites

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

Attributs du DN	Nom de l'attribut	Valeur
C	*countryName*	FR
O	*organizationName*	Nom de l'Entité Cliente à laquelle appartient le Porteur
OU	*organizationalUnitName*	Identifiant de l'Entité Cliente à laquelle appartient le Porteur au format RGS.
OI	*organizationIdentifier*	Identifiant de l'Entité Cliente à laquelle appartient le Porteur au format ETSI.
CN	*commonName*	Premier prénom et Nom de l'état civil du Porteur porté sur le document d'identité présenté lors de son enregistrement.
SN	*surName*	Nom de l'état civil du Porteur
GN	*givenName*	Premier prénom de l'état civil du Porteur
SerialNumber	*SerialNumber*	Contient un numéro permettant de garantir l'unicité du DN et résoudre ainsi les cas d'homonymie.

Note : IN Groupe ne délivre des certificats qu'aux entités de droit français.

Les certificats de test sont identifiables par le fait que leur CN contient le mot « TEST », précédant un prénom et un nom fictifs. Tous les autres champs (*à l'exception des informations d'AC, comme les champs Issuer, AIA, AKI, etc.*) sont susceptibles de différer des profils des certificats porteurs décrits au chapitre VII.1.

III.1.3 Pseudonymisation des porteurs

L'AC n'émet pas de certificat comportant une identité anonyme ou une identité pseudonyme.

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

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

III.1.5 Unicité des noms

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

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

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

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

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

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

III.1.6 Identification, authentification et rôle des marques déposées

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

III.2 VALIDATION INITIALE DE L'IDENTITE

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

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

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

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

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

III.2.3 Validation de l'identité d'un individu

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

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

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

III.2.3.1 Enregistrement d'un RL

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

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

Le dossier d'enregistrement du RL comprend :

- [Optionnel] La demande de certificat écrite, datée de moins de trois mois, signée par le RL
- [Optionnel] Les Conditions Générales d'Utilisation signées par le RL
- La photocopie d'une pièce d'identité officielle du RL en cours de validité

Des informations d'identification de l'Entité Cliente ;

Pour une entreprise :

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

certificat

Pour une administration :

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

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

III.2.3.2 Enregistrement d'un MC

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

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

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

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

III.2.3.3 Enregistrement d'un Porteur via un MC

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

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

- La demande de certificat mentionnant l'identité du Porteur, datée de moins de trois mois, signée par le Porteur.
- Les Conditions Générales d'Utilisation signées par le Porteur
- La photocopie d'une pièce d'identité officielle du Porteur en cours de validité
- Des informations permettant de contacter le Porteur: courriel ou adresse postale, optionnellement n° téléphone

III.2.4 Informations non vérifiées du porteur

Les certificats émis par l'AC ne contiennent aucune information d'identité non vérifiée à l'exception des éléments techniques informatique tels que les UPN et les adresses électroniques.

III.2.5 Validation de l'autorité du demandeur

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

III.2.6 Critères d'interopérabilité

Ce point est sans objet dans la présente PC.

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

L'AC n'émet pas de nouveau certificat pour une bi-clé précédemment émis. Le renouvellement nécessite la génération d'une nouvelle bi-clé et d'une nouvelle demande de certificat (cf. §IV.6).

III.3.1 Identification et validation pour un renouvellement courant

Les vérifications relatives au renouvellement courant sont effectuées conformément à la procédure de demande initiale de certificat (cf. § 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 sont effectuées conformément à la procédure de demande initiale de certificat (cf. § III.2 ci-dessus), ce cas s'apparentant à un renouvellement de la bi-clé avec l'émission d'un nouveau certificat.

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

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

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

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

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

Une demande de révocation peut être effectuée :

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

IV Exigences opérationnelles sur le cycle de vie des certificats

IV.1 DEMANDE DE CERTIFICAT

IV.1.1 Origine d'une demande de certificat

La demande de certificat émane du MC dûment mandaté par le représentant légal de l'Entité Cliente.

Le consentement préalable du futur Porteur est requis.

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

Le dossier de demande de certificat est établi par le RL ou par le MC.

Ce dossier comporte, *a minima*, les informations suivantes :

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

Le dossier contient les éléments décrits en III.2.3.

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

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

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

IV.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

L'AE effectue les traitements suivants :

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

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

IV.2.2 Acceptation ou rejet de la demande

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

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

IV.2.3 Durée d'établissement du certificat

Une fois la demande de certificat validée, le certificat est émis dans les meilleurs délais.

IV.3 DELIVRANCE DU CERTIFICAT

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

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

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

L'AC notifie le Porteur, et le cas échéant le MC, de l'envoi du support (portant la bi-clé et le certificat associé) et de son code d'activation par voie postale, au travers de l'application accessible en ligne. Support et code d'activation sont envoyés séparément. La clé privée du Porteur est protégée lors de son envoi par le code d'activation du support.

Le support est envoyé directement au Porteur ou au MC le cas échéant, par transport express sécurisé suivi, assuré par un prestataire spécialisé.

IV.4 ACCEPTATION DU CERTIFICAT

IV.4.1 Démarche d'acceptation du certificat

L'acceptation du certificat par le Porteur s'effectue de manière explicite sous la forme d'un accord signé. Une fois le dispositif de création de signature qualifié (QSCD) reçu, le Porteur signe un PV d'acceptation du certificat au cours de la phase d'activation de son certificat et le retourne à l'AE qui le conservera.

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

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

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

IV.4.2 Publication du certificat

Les certificats émis par l'AC dans le cadre de cette PC ne sont pas publiés.

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

L'AE est informée de la génération du certificat par l'AC. C'est elle qui est responsable de sa délivrance au Porteur.

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 Porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats.

Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé et du certificat associé sont par ailleurs indiqués dans le certificat lui-même, via les extensions concernant les usages des clés.

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service défini par l'OID de sa politique (cf. chapitre I.4.1.1).

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

Cf. chapitre précédent et chapitre I.4.

Les Utilisateurs de Certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

IV.6 RENOUVELLEMENT D'UN CERTIFICAT

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

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

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

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

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des Porteurs, et les certificats correspondants, seront renouvelés au minimum avant leur fin de vie définie au chapitre 6.3.2.

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

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

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

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

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

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

Le traitement relatif à une demande de nouveau certificat s'effectue dans les mêmes conditions et selon les mêmes modalités que la demande initiale. (cf. § IV.2 ci-dessus).

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

Pour tout renouvellement : l'AC notifie le Porteur, et le cas échéant le MC dans les conditions du chapitre IV.3.2.

IV.7.5 Démarche d'acceptation du nouveau certificat

Tout renouvellement s'effectue dans les conditions du chapitre IV.4.1.

IV.7.6 Publication du nouveau certificat

Voir chapitre IV.4.2.

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

Voir chapitre IV.4.3

IV.8 MODIFICATION DU CERTIFICAT

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

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

IV.9 REVOCATION ET SUSPENSION DES CERTIFICATS

IV.9.1 Causes possibles d'une révocation

IV.9.1.1 Certificats de porteurs

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

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

IV.9.1.2 Certificats d'une composante de l'IGC

Les causes de révocations d'un certificat d'une composante de l'IGC sont les suivantes :

- cessation d'activité de l'entité opérant la composante,
- compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de la composante (perte du secret principal, perte du code d'activation et perte de plus de deux secrets partagés),
- non-respect de la PC de l'AC (détecté lors d'un audit de qualification ou de conformité négatif),
- changement de composante de l'IGC
- obsolescence de la cryptographie au regard des exigences de l'ANSSI (nécessitant renouvellement de la bi-clé de l'AC).

IV.9.2 Origine d'une demande de révocation

IV.9.2.1 Certificats de porteurs

Les personnes autorisées à demander la révocation d'un certificat Porteur sont les suivantes :

- Le Porteur au nom duquel le certificat a été émis
- Le cas échéant, un MC de l'Entité Cliente à laquelle est rattaché le Porteur
- Le Responsable Légal de l'Entité Cliente à laquelle est rattaché le Porteur
- L'AC émettrice du certificat ;

- Une composante de l'AC (l'AE) ;

IV.9.2.2 Certificats d'une composante de l'IGC

La révocation du certificat de l'AC ne peut être décidée que par l'entité responsable de l'AC ou par les autorités judiciaires via une décision de justice.

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

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

IV.9.3.1 Révocation d'un certificat de porteur

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

Une demande de révocation peut être déposée :

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

Les informations suivantes figurent, *a minima*, dans la demande de révocation de certificat :

- Identité du Porteur dont le certificat est à révoquer
- Identité du demandeur
- Information permettant d'identifier de façon univoque le certificat à révoquer (n° série, …)

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

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

IV.9.3.2 Révocation d'un certificat d'une composante de l'IGC

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

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

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

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

IV.9.5.1 Révocation d'un certificat de porteur

L'AC traite les demandes de révocation dès que possible suivant sa réception, de préférence immédiatement, et dans un délai inférieur à 24 h. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des Utilisateurs de Certificat.

IV.9.5.2 Disponibilité du système de traitement des demandes de révocation

La disponibilité du service de révocations est assurée 7 jours sur 7 et 24 heures sur 24.

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

IV.9.5.3 Révocation d'un certificat d'une composante de l'IGC

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

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

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

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

IV.9.7 Fréquence d'établissement et durée de validité des LCR

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

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

IV.9.8 Délai maximum de publication d'une LCR

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

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

Une publication complémentaire suivant le protocole OCSP est disponible.

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

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

Voir § IV.9.6.

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

Sans objet

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

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

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

Une information sera diffusée auprès du point de contact de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) identifié sur le site https://www.ssi.gouv.fr.

IV.9.13 Causes possibles d'une suspension

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

IV.9.14 Origine d'une demande de suspension

Ce point est sans objet dans la présente PC.

IV.9.15 Procédure de traitement d'une demande de suspension

Ce point est sans objet dans la présente PC.

IV.9.16 Limites de la période de suspension d'un certificat

Ce point est sans objet dans la présente PC.

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

IV.10.1 Caractéristiques opérationnelles

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

Les LCR et LAR sont signées par le même certificat d'AC que celui utilisé pour signer les certificats de Porteur.

Les informations d'état de révocation sont disponibles au-delà de la période de validité des certificats. Les LCR contiennent également les numéros de série des certificats arrivés à expiration après leur révocation.

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

Les réponses OCSP sont signées par un certificat de répondeur OCSP émis par le même certificat d'AC que celui utilisé pour signer les certificats de Porteur.

IV.10.2 Disponibilité de la fonction d'information sur l'état des certificats

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

IV.10.3 Dispositifs optionnels

Ce point est sans objet dans la présente PC.

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

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

IV.12 SEQUESTRE DE CLE ET RECOUVREMENT

Les clés privées associées aux certificats d'authentification et de signature des Porteurs ne peuvent pas être séquestrées.

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

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 PHYSIQUE

V.1.1 Situation géographique et construction des sites

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

V.1.2 Accès physique

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

Le système de contrôle des accès permet de garantir la traçabilité des accès aux zones où sont hébergées les IGC. En dehors des heures ouvrables, la sécurité est standard 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.

V.1.3 Alimentation électrique et climatisation

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

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

V.1.4 Vulnérabilité aux dégâts des eaux

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

V.1.5 Prévention et protection incendie

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

V.1.6 Conservation des supports

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

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

V.1.7 Mise hors service des supports

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

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

V.1.8 Sauvegardes hors site

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

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

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

V.2 MESURES DE SECURITE PROCEDURALES

V.2.1 Rôles de confiance

Les personnes ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité. Les personnes ayant un rôle de confiance ne souffrent d'aucun conflit 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 PC 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 à la PC et aux politiques de sécurité de la composante. L'auditeur est désigné par l'AGP.

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

V.2.2 Nombre de personnes requises par tâches

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

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

Les fonctions sensibles (par exemple les cérémonies de clé) sont réparties sur plusieurs personnes pour des questions de sécurité.

V.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC fait 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 conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC est notifiée par écrit. Ce rôle est 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 sont respectées. Les attributions associées à chaque rôle sont conformes à la politique de sécurité de la composante concernée.

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

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

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

V.3.1 Qualifications, compétences et habilitations requises

Chaque personne amenée à travailler au sein de l'AC est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles.

Toute personne intervenant dans les procédures de certification de l'IGC est informée de ses responsabilités relatives aux services de l'IGC et des procédures liées à la sécurité du système et au contrôle du personnel.

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

V.3.2 Procédures de vérification des antécédents

L'AC met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification est basée sur un contrôle des antécédents de la personne (salarié hors période d'essai), il est notamment vérifié que chaque personne n'a pas fait l'objet de condamnation de justice (extrait B3 du casier judiciaire) en contradiction avec leurs attributions.

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

Les personnes ayant un rôle de confiance ne souffrent d'aucun conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

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

V.3.3 Exigences en matière de formation initiale

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

V.3.4 Exigences et fréquences en matière de formation continue

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

V.3.5 Fréquence et séquence de rotation entre différentes attributions

Il n'est pas prévu de fréquence et séquence de rotation entre les différentes attributions.

V.3.6 Sanctions en cas d'actions non autorisées

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

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

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

V.3.8 Documentation fournie au personnel

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

V.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation d'événements consiste à enregistrer les évènements manuellement ou électroniquement par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier et / ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.

V.4.1 Types d'événements à enregistrer

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

- Création / modification / suppression de comptes Utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.),
- Démarrage et arrêt des systèmes informatiques et des applications,
- traces d'activité *(logs)* des pare-feux et des routeurs,
- 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, pannes logicielles et matérielles,
- Connexion / déconnexion des Utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes,

V.4.1.1 Informations enregistrées pour chaque évènement

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

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

Suivant le type d'événement concerné, les champs suivants peuvent être enregistrés :

- Destinataire de l'opération,
- Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande,
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes),
- Cause de l'événement,
- Toute information caractérisant l'événement (par exemple pour la génération d'un certificat, son numéro de série).

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

V.4.1.2 Evènements enregistrés par l'AE

Les évènements enregistrés par l'AE sont les suivants :

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

V.4.1.3 Evènements enregistrés par l'AC

Les évènements enregistrés par l'AC sont les suivants :

- Evénements liés aux clés de signature et aux certificats d'AC (génération, sauvegarde / récupération, destruction, …),

- Génération des bi-clés des Porteurs,
- Génération des certificats des Porteurs,
- Personnalisation des supports et génération des codes d'activation,
- Publication et mise à jour des informations liées aux AC (PC, certificats d'AC, CGU, etc.)
- Génération puis publication des LCR,
- Requêtes et réponses OCSP.

V.4.1.4 Evènements divers

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

- Les accès physiques aux zones sensibles,
- Les actions de maintenance et de changements de la configuration des systèmes,
- Les changements apportés au personnel ayant des rôles de confiance,
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, mots de passe ou code Porteur, …).

V.4.1.5 Imputabilité

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

V.4.2 Fréquence de traitement des journaux d'événements

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

V.4.3 Période de conservation des journaux d'événements

Les journaux d'évènements sont conservés sur site pendant au moins 10 ans. Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous 1 mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

V.4.4 Protection des journaux d'événements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

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

V.4.5 Procédure de sauvegarde des journaux d'événements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système de datation des évènements associe à toutes les archives une date de génération des archives.

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

V.4.6 Système de collecte des journaux d'événements

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

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

Sans objet.

V.4.8 Evaluation des vulnérabilités

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

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

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

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

Par ailleurs, un scan de vulnérabilités est réalisé périodiquement dans le cadre d'une campagne de tests d'intrusion. Le moyen privilégié pour réaliser ces tests d'intrusion repose sur un audit technique réalisé par un prestataire d'audit de la sécurité des systèmes d'information qualifié.

Les vulnérabilités détectées à l'occasion de ces contrôles réguliers ou ponctuels donnent lieu à une analyse pour identifier et évaluer leurs conséquences et impacts éventuels. Selon la criticité de l'impact, un plan d'actions est mis en œuvre pour atténuer ces vulnérabilités.

V.5 ARCHIVAGE DES DONNEES

L'archivage des données permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC. Il permet aussi 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 et déclaration de pratiques de certification,
- Les certificats, LCR et réponses OCSP tels qu'émis ou publiés,
- Les dossiers d'enregistrement des MC,
- Les dossiers de demande de certificats comprenant les justificatifs d'identité des Porteurs, le cas échéant de leur entité de rattachement,
- Les journaux d'événements des différentes composantes de l'IGC.

V.5.2 Période de conservation des archives

V.5.2.1 Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable. En l'occurrence, il est archivé pendant dix ans, comptés à partir de la date de début de validité du certificat Porteur.

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

V.5.2.2 Certificats et LCR émis par l'AC

La période de conservation des certificats et des LCR émis par l'AC, ainsi que celle des certificats d'AC et des LAR est de 10 ans après leur expiration.

V.5.2.3 Réponses OCSP

Les réponses OCSP sont archivées pendant au moins trois mois après leur expiration.

V.5.2.4 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

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

V.5.5 Exigences d'horodatage des données

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

V.5.6 Système de collecte des archives

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

V.5.7 Procédure de récupération et de vérification des archives

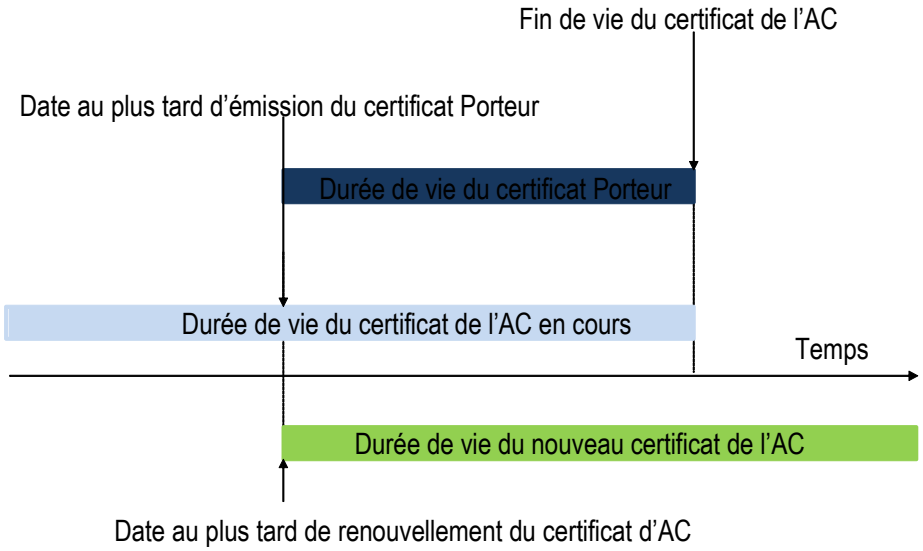
Les archives (papier et électroniques) sont récupérables dans un délai inférieur à 2 jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

V.6 CHANGEMENT DE CLE D'AC

La durée de vie du certificat d'AC est déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment les recommandations des autorités nationale ou internationale compétentes en la matière.

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

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



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

V.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

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

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

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

Conformément aux obligations réglementaires, l'organe de contrôle national (l'ANSSI) sera informé de tout incident de sécurité touchant l'AC et ses services dans les 24 (vingt-quatre) heures.

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

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

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

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

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

Dans le cas de compromission d'une clé d'AC, le certificat correspondant est immédiatement révoqué comme précisé au § IV.9.

De plus, l'AC respecte les engagements suivants :

- Arrêter immédiatement l'utilisation de la clé de la composante compromise,
- Informer sans délai: tous les Porteurs, les Entités Clientes avec lesquelles l'AC a passé des accords et les Utilisateurs de Certificat,
- 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.
- Prévenir l'ANSSI de la compromission,
- Le cas échéant procéder à un dépôt de plainte auprès des autorités compétentes.

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

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

V.8 FIN DE VIE DE L'IGC

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

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

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité. La nouvelle entité garantit un niveau de confiance adéquat, le maintien des garanties financières ainsi qu'une continuité de service (notamment archivage, maintien de la confidentialité, interopérabilité des certificats, etc.).

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée. Ainsi, les certificats émis seront révoqués sans délai et les entités informées de la révocation des certificats.

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

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

En cas de cessation d'activité, l'AC préviendra les Porteurs de certificats sous le délai d'un mois. De même, elle effectuera une information auprès des autorités administratives. En particulier, les contacts auprès de l'ANSSI seront avertis.

VI Mesures de sécurité techniques

VI.1 GENERATION ET INSTALLATION DE BI-CLES

VI.1.1 Génération des bi-clés

VI.1.1.1 Clés d'AC

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

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

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

VI.1.1.2 Clés porteurs générées par l'AC

Les bi-clés des Porteurs sont générées par l'AC dans un environnement sécurisé par un module cryptographique, puis transférées de manière sécurisée dans le QSCD destiné au Porteur sans que l'AC n'en garde aucune copie.

VI.1.1.3 Clés porteurs générées par le porteur

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

VI.1.2 Transmission de la clé privée à son propriétaire

La clé privée est transmise au Porteur de manière sécurisée. Une fois générée par l'AC, elle est importée directement dans le QSCD qui est ensuite transmis par voie postale au Porteur ou, le cas échéant, via le MC de son entité de rattachement.

Une fois remise, la clé privée est maintenue sous le seul contrôle du Porteur.

Si la vérification de l'identité du Porteur en face-à-face n'a pas été effectuée lors de l'enregistrement, elle est effectuée lors de la remise en main propre du support par le MC.

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

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

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

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

La clé publique de l'AC est diffusée dans un certificat signé par l'AC Racine. La clé publique de l'AC Racine est diffusée dans un certificat auto-signé.

Les certificats de l'AC et de l'AC Racine sont disponibles aux URL citées au chapitre II.2 de la présente PC.

VI.1.5 Tailles des clés

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

VI.1.5.1 Clés d'AC

Les bi-clés d'une AC dont la durée de validité est supérieure ou égale à 10 ans sont d'une complexité au moins équivalente à 4096 bits pour l'algorithme RSA.

Les bi-clés AC d'une complexité inférieure à 4096 bits pour l'algorithme RSA, ne sont pas supportées par cette PC.

VI.1.5.2 Clés de porteurs

Les bi-clés des certificats émis sont d'une complexité au moins équivalente à 2048 bits pour l'algorithme RSA et P-256 pour l'algorithme ECDSA-GF(P).

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

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

VI.1.7 Objectifs d'usage de la clé

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

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la fonction de sécurité concernée (cf. chapitres I.5.1.1, IV.5).

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

VI.2.1.1 Modules cryptographiques de l'AC

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

L'AC met en place des procédures pour :

- garantir l'intégrité des modules cryptographiques durant leur stockage et leur transport,
- s'assurer que les modules cryptographiques fonctionnent correctement,
- s'assurer que les opérations sur les modules cryptographiques sont réalisées par au moins deux personnels ayant des rôles de confiance.

VI.2.1.2 Dispositifs de protection des éléments secrets des porteurs

Les dispositifs de protection des éléments secrets des porteurs, pour la mise en œuvre de leurs clés privées de personne, respecte les exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré.

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 du module cryptographique. La génération de la bi-clé est traitée au § VI.1.1, l'activation de la clé privée au § VI.2.8 et sa destruction au § VI.2.10.

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

VI.2.3 Séquestre de la clé privée

Aucunes clés privées associées aux certificats électroniques ne sont séquestrées.

VI.2.4 Copie de secours de la clé privée

Les clés privées des porteurs ne font l'objet d'aucune copie de secours par l'AC.

VI.2.5 Archivage de la clé privée

Les clés privées de l'AC ne sont en aucun cas archivées.

Les clés privées des certificats émis ne sont en aucun cas archivées ni par l'AC ni par aucune des composantes de l'IGC.

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

VI.2.6.1 Clés privées d'AC

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

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

VI.2.6.2 Clés privées des porteurs

Le transfert de la clé privée du Porteur dans le QSCD s'effectue conformément aux exigences du § VI.1.1.2.

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

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

VI.2.8 Méthode d'activation de la clé privée

VI.2.8.1 Clés privées d'AC

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

VI.2.8.2 Clés privées des porteurs

Avant de pouvoir utiliser son support, le Porteur doit procéder à son activation. Cette activation requiert la saisie du code d'activation dans la fonction d'activation accessible en ligne. Le code d'activation est transmis de manière sécurisée au Porteur. La méthode d'activation répond aux exigences définies au §XII.

Le support utilisé est tel que la clé privée du Porteur n'est activable que sur présentation de code d'activation.

Lors d'une opération de signature, après calcul de signature par la carte, cette dernière invalide le statut « code PIN présenté ». Ce mécanisme oblige à saisir le code PIN systématiquement pour chaque signature calculée par la carte.

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

VI.2.9 Méthode de désactivation de la clé privée

VI.2.9.1 Clés privées d'AC

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

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

VI.2.9.2 Clés privées des porteurs

La clé privée stockée sur le support est désactivée après chaque calcul de signature effectué (qu'il y ait mise hors tension ou non). La clé privée reste ainsi sous le contrôle du Porteur.

VI.2.10 Méthode de destruction des clés privées

VI.2.10.1 Clés privées d'AC

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

VI.2.10.2 Clés privées des porteurs

Après délivrance du QSCD, le Porteur est le seul à pouvoir détruire la clé privée (par effacement ou par destruction du QSCD).

VI.2.11 Niveau de qualification du module cryptographique et des dispositifs de protection des éléments secrets

Les modules cryptographiques utilisés par l'AC et l'ACR sont évalués au niveau EAL4+ et qualifiés au niveau renforcé selon les exigences de l'ANSSI.

Les QSCD délivrés par l'AC sont évalués au niveau EAL4+ et sont qualifiés au niveau renforcé selon les exigences de l'ANSSI.

L'AC assure un suivi de la certification du QSCD et s'assure que le produit déployé est toujours conforme à la règlementation.

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

VI.3.1 Archivage des clés publiques

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

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

La durée de validité du certificat de l'AC est de 10 ans. La durée de vie de la bi-clé correspondante est équivalente, soit 10 ans également. La fin de validité du certificat d'AC est postérieure à la fin des certificats Porteurs qu'elle émet.

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

VI.4 DONNEES D'ACTIVATION

VI.4.1 Génération et installation des données d'activation

VI.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'AC

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

VI.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du porteur

Le code d'activation est transmis au Porteur par voie postale, dans un courrier sécurisé (mailer) garantissant l'intégrité et la confidentialité de son contenu. Cet envoi est séparé dans le temps de l'envoi du QSCD au Porteur ou le cas échéant au MC. Les envois du support et du code d'activation peuvent être effectués à des adresses distinctes (respectivement adresse professionnelle et adresse personnelle du Porteur).

VI.4.2 Protection des données d'activation

VI.4.2.1 Protection des données d'activation correspondant à la clé privée de l'AC

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

VI.4.2.2 Protection des données d'activation correspondant aux clés privées des porteurs

Les données d'activation des dispositifs des Porteurs générées par l'AC sont protégées en confidentialité et intégrité jusqu'à leur remise aux Porteurs. Elles ne sont pas sauvegardées par l'AC après leur remise.

Une fois le QSCD activé, le Porteur initialise son code PIN.

Les Porteurs sont responsables de la confidentialité de leurs codes PIN, afin qu'ils soient les seuls à pouvoir utiliser la clé privée. En cas suspicion de perte de confidentialité, les Porteurs s'engagent à modifier ces codes PIN.

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.

VI.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

VI.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Les fonctions suivantes sont fournies par le système d'exploitation, ou par une combinaison du système d'exploitation, de logiciels et de protection physiques.

Un composant d'une IGC comprend les fonctions suivantes :

- Identification et Authentification forte des rôles de confiance (accès physique et logique) ;
- Gestion des droits d'accès basée sur des profils respectant le principe du moindre privilège ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, gestion droits d'accès aux fichiers)
- Interdiction de la réutilisation d'objets ;
- Exige l'utilisation de la cryptographie lors des communications ;
- Assure la séparation rigoureuse des tâches ;
- Protection contre les virus informatiques
- Protection du réseau contre toute intrusion illicite
- Réalise une veille sécurité assurant l'application régulière des correctifs de sécurité des systèmes informatiques, et la prise en compte des vulnérabilités critiques dans un délai de 48 heures.
- Fournit une autoprotection du système d'exploitation.
- Fonction d'audits

VI.5.2 Niveau de qualification des systèmes informatiques

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

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

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

VI.6.1 Mesures de sécurité liées au développement des systèmes

Les développements des systèmes sont contrôlés par les mesures suivantes :

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

VI.6.2 Mesures liées à la gestion de la sécurité

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

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

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

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

Toute évolution significative d'un système d'une composante de l'IGC est testée et validée avant déploiement. Ces opérations sont réalisées par du personnel de confiance.

L'AC informera l'organe de contrôle national (l'ANSSI), selon les modalités décrites sur le site https://www.ssi.gouv.fr, de tout changement significatif d'un système d'une composante de l'IGC avant son déploiement.

VI.7 MESURES DE SECURITE RESEAU

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

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

Le réseau d'administration des systèmes informatiques est logiquement séparé du réseau d'exploitation.

VI.8 HORODATAGE / SYSTEME DE DATATION

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

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

VII Profils 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. Les champs des certificats d'AC et des certificats des Porteurs sont définis par le RFC 5280.

VII.1.1 Profils des certificats des AC IN Groupe

Les principaux champs des certificats des AC sont les suivants :

AC Imprimerie Nationale Substantiel Personnel	
Champs de base	**Valeur**
Version	2 (=version 3)
Serial Number	Défini par l'IGC
Issuer	C = FR

	O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Racine
Validity	10 ans
Subject	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Substantiel Personnel
Subject Public Key Info	4096 bits
Unique Identifiers	Non utilisé

AC Imprimerie Nationale Elevé Personnel	
Champs de base	**Valeur**
Version	2 (=version 3)
Serial Number	Défini par l'IGC
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Racine
Validity	10 ans
Subject	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Elevé Personnel
Subject Public Key Info	4096 bits
Unique Identifiers	Non utilisé

Ainsi que les extensions suivantes :

Extensions	Criticité	Valeur
Authority Key Identifier	N	Identifiant de la clé publique de l'AC Racine
Basic Constraints	O	Contraintes de base : SubjectType=CertAuthority PathLengthConstraint=0
Certificate Policies	N	Stratégies de certificat : Toutes les stratégies d'émission

		http://www.imprimerienationale.fr/GIN/PC
CRL Distribution Points	N	Point de distribution de la LAR : URL=http://www.imprimerienationale.fr/GIN/CRL/ACR.crl URL=http://crl.imprimerienationale.fr/GIN/ACR.crl
Key Usage	O	Signature de certificat Signature de la liste de révocation hors connexion Signature de la liste de révocation
Subject Key Identifier	N	Identifiant de la clé publique de l'AC

VII.1.2 Profils des certificats de Porteurs

Les principaux champs des certificats Porteur sont les suivants :

AC Imprimerie Nationale Substantiel Personnel	
Champs de base	**Valeur**
Version	2 (=version 3)
Serial Number	Défini par l'IGC
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Substantiel Personnel
Validity	3 ans
Subject	Voir chapitre 7.2
Subject Public Key Info	Cf. chapitre 5 sur les exigences en matière d'algorithmes et de longueurs de clés.
Unique Identifiers	Non utilisé.

AC Imprimerie Nationale Elevé Personnel	
Champs de base	**Valeur**
Version	2 (=version 3)
Serial Number	Défini par l'IGC
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Elevé Personnel
Validity	3 ans
Subject	Voir chapitre 7.2
Subject Public Key Info	Cf. chapitre 5 sur les exigences en matière d'algorithmes et de

	longueurs de clés.
Unique Identifiers	Non utilisé.

VII.1.2.1 Extensions des certificats de Porteurs sur QSCD

Extensions	Criticité	Valeur	
Authority Key Identifier	N	Contient l'identifiant de clé de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice). Méthode 1 définie dans la RFC 5280 chapitre 4.2.1.2.	
Basic Constraints	N	Contraintes de base : SubjectType=EndEntity PathLengthConstraint=aucun	
Certificate Policies	N	A minima, l'OID de la PC de l'AC émettrice	
Subject Alternative Name	N	Autre nom de l'objet : Nom RFC822 Nom Principal (UPN) [Valeur optionnelle]	
Issuer Alternative Name	N	Non utilisée	
Subject Directory Attributes		Non utilisée	
CRL Distribution Points	N	Points de distribution vers la CRL de l'AC émettrice.	
Authority Information Access	N	Point de distribution vers l'OCSP de l'AC émettrice	
Freshest CRL	N	Non utilisée	
Subject Key Identifier	N	Identifiant de la clé publique du Porteur	
		Certificats d'Authentification	**Certificats de Signature**
Key Usage	O	digitalSignature	nonRepudiation
Extended Key Usage	N	id-kp-clientAuth id-ms-smartcardlogon	id-kp-emailProtection
Qc Compliance	N	Non utilisée	id-etsi-qcs 1
QcSSCD	N	Non utilisée	id-etsi-qcs 4
QcType	N	Non utilisée	id-etsi-qct-esign
QcPDS	N	Non utilisée	URL vers les CGU

Note : Le bit nonRepudiation est désormais nommé contentCommitment.

VII.1.2.2 Extensions des certificats de Porteurs sur SCD

Extensions	Criticité	Valeur
Authority Key Identifier	N	Contient l'identifiant de clé de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice).

		Méthode 1 définie dans la RFC 5280 chapitre 4.2.1.2.	
Basic Constraints	N	Contraintes de base : SubjectType=EndEntity PathLengthConstraint=aucun	
Certificate Policies	N	A minima, l'OID de la PC de l'AC émettrice	
Subject Alternative Name	N	Autre nom de l'objet : Nom RFC822 Nom Principal (UPN) [Valeur optionnelle]	
Issuer Alternative Name	N	Non utilisée	
Subject Directory Attributes		Non utilisée	
CRL Distribution Points	N	Points de distribution vers la CRL de l'AC émettrice.	
Authority Information Access	N	Point de distribution vers l'OCSP de l'AC émettrice	
Freshest CRL	N	Non utilisée	
Subject Key Identifier	N	Identifiant de la clé publique du Porteur	
		Certificats d'Authentification	**Certificats de Signature**
Key Usage	O	digitalSignature	nonRepudiation
Extended Key Usage	N	id-kp-clientAuth id-ms-smartcardlogon	id-kp-emailProtection
Qc Compliance	N	Non utilisée	id-etsi-qcs 1
QcSSCD	N	Non utilisée	Non utilisée
QcType	N	Non utilisée	id-etsi-qct-esign
QcPDS	N	Non utilisée	URL vers les CGU

Note : Le bit nonRepudiation est désormais nommé contentCommitment.

VII.1.3 Identifiant d'algorithme

Les identifiants des algorithmes utilisés sont :

- Sha-256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}.
- Sha-384WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha384WithRSAEncryption(12)}.
- Sha-512WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}.

VII.1.4 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.1.5 Identifiant d'objet (OID) de la PC

Les certificats Porteurs contiennent l'OID du modèle de certificat (voir & **Erreur ! Source du renvoi introuvable.**).

VII.1.6 Extensions propres à l'usage de la politique

Sans objet

VII.1.7 Syntaxe et sémantique des qualifiants de politique

Sans objet

VII.1.8 Interprétation sémantique de l'extension critique « Certificate Policies »

Pas d'exigence formulée

VII.2 PROFILS DE LCR

Les AC IN Groupe émettent des LCR dont les caractéristiques sont :

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

Les principaux champs de la LCR sont :

AC Imprimerie Nationale Substantiel Personnel	
Champs de base	**Valeur**
Version	1 (=version 2)
Serial Number	Défini par l'IGC
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Substantiel Personnel
This Update	Date de génération de la LCR
Next Update	Date limite d'émission de la prochaine LCR.
Revoked certificates	Liste des numéros de série des certificats Porteurs révoqués

AC Imprimerie Nationale Elevé Personnel	
Champs de base	**Valeur**
Version	1 (=version 2)

Serial Number	Défini par l'IGC
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Elevé Personnel
This Update	Date de génération de la LCR
Next Update	Date limite d'émission de la prochaine LCR.
Revoked certificates	Liste des numéros de série des certificats Porteurs révoqués

Plus les extensions suivantes :

Extensions	Criticité	Description
Authority Key Identifier	N	Contient l'identifiant de clé de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice). Méthode 1 définie dans la RFC 5280 chapitre 4.2.1.2.
CRL Number	N	Numéro de série de la LCR
ExpiredCertsOnCRL	N	Indique que la LCR contient également les numéros de série des certificats arrivés à expiration après leur révocation.

VII.3 PROFIL OCSP

Un répondeur OCSP est mis en place pour vérifier en ligne l'état des certificats émis par les AC IN Groupe. Les réponses OCSP sont signées par le répondeur OCSP dont le certificat est émis par l'AC émettrice du certificat vérifié (cf. rfc6960).

Afin d'assurer la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat, les réponses OCSP contiennent l'extension « *id-pkix-ocsp-archive-cutoff* » conformément à la RFC 6960 contenant la date de début de validité de l'AC émettrice.

AC Imprimerie Nationale Substantiel Personnel	
Champs de base	**Valeur**
Version	2 (=version 3)
Serial Number	Défini par l'IGC
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Substantiel Personnel
Subject DN	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496

	CN = [Nom du service OCSP]
Durée de vie	1 an

AC Imprimerie Nationale Elevé Personnel	
Champs de base	**Valeur**
Version	2 (=version 3)
Serial Number	Défini par l'IGC
Issuer	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = AC Imprimerie Nationale Elevé Personnel
Subject DN	C = FR O = Groupe Imprimerie Nationale OU = 0002 410494496 OI = NTRFR-410494496 CN = [Nom du service OCSP]
Durée de vie	1 an

Plus les extensions suivantes :

Extensions	Criticité	Valeur
Authority Key Identifier	N	Contient l'identifiant de clé de la clé publique de l'AC émettrice (même valeur que le champ "Subject Key Identifier" du certificat de cette AC émettrice). Méthode 1 définie dans la RFC 5280 chapitre 4.2.1.2.
Basic Constraints	N	Contraintes de base : SubjectType=EndEntity PathLengthConstraint=aucun
Certificate Policies	N	A minima, l'OID de la PC de l'AC émettrice
Key Usage	O	digitalSignature
Subject Key Identifier	N	Identifiant de la clé publique du répondeur OCSP
Extended Key Usage	N	OCSP Signing
OCSP No Check	N	Null

VIII Audit de conformité et autres évaluations

Les audits et les évaluations concernent :

- d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification selon le schéma de qualification des prestataires de service de confiance conformément au décret RGS et au Règlement eIDAS,

- et d'autre part, ceux que doit réaliser, ou faire réaliser l'AGP afin de s'assurer que l'ensemble de son IGC, et le cas échéant l'ensemble des MC, respecte les engagements affichés dans cette PC.

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

VIII.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AGP procède à un contrôle de conformité de cette composante. L'AGP procède également :

- une fois par an à un contrôle de conformité de l'ensemble de son IGC dans le cadre de la qualification RGS de l'AC,
- une fois tous les 2 ans un contrôle de conformité à la norme ETSI EN 319 411-1 et ETSI EN 319 411-2.

Un contrôle de conformité de l'AC a été effectué avant la première mise en service pour l'obtention de la qualification RGS et d'une qualification au sens eIDAS.

VIII.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

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

VIII.3 RELATIONS ENTRE EVALUATEURS ET ENTITE EVALUEE

L'équipe d'audit n'appartient en aucun cas à l'entité opérant la composante de l'IGC contrôlée, quelle que soit cette composante, et est 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 (procédures opérationnelles, ressources mises en œuvre, etc.) définies dans la PC de l'AC.

VIII.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AGP, 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'AGP 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'AGP et doit respecter ses politiques de sécurité internes.
- En cas de résultat "à confirmer", l'AGP 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'AGP confirme à la composante contrôlée la conformité aux exigences de la PC.

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'AGP. Ils incluent les mesures correctives de la composante déjà prises ou en cours.

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

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

IX Autres problématiques métiers et légales

IX.1 TARIFS

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

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

IX.1.2 Tarifs pour accéder aux certificats

Les certificats sont gratuitement accessibles aux Utilisateurs de Certificat.

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

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

IX.1.4 Tarifs pour d'autres services

Aucune exigence particulière.

IX.1.5 Politique de remboursement

Aucune exigence particulière.

IX.2 RESPONSABILITE FINANCIERE

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

IX.2.1 Couverture par les assurances

IN Groupe 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

IN Groupe 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'IN Groupe, celle-ci fera appel à son assurance pour couvrir une partie des dommages du client dans la limite de la responsabilité d'IN Groupe définie dans les conditions générales de services IN Groupe et aux présentes.

IX.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

IX.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- les parties non publiques de la PC de l'AC et les procédures internes associées,
- les clés privées de l'AC, de ses composantes et des Porteurs de certificats
- les données d'activation associées aux clés privées d'AC ainsi quelle celles associées aux clés privées des Porteurs (avant que ces données soient transmises aux Porteurs),
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les éléments relatifs à la cérémonie des clés, comprenant l'identité des Porteurs de secrets
- les causes de révocations, sauf accord explicite du Porteur,
- les dossiers d'enregistrement des Porteurs,
- les rapports des audits.

Seules les personnes habilitées peuvent y accéder.

IX.3.2 Informations hors périmètre des informations confidentielles

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

IX.3.3 Responsabilité en termes de protection des informations confidentielles

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

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

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

IX.4 PROTECTION DES DONNEES A CARACTERE PERSONNEL

IX.4.1 Politique de protection des données à caractère personnel

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

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

IX.4.2 Données à caractère personnel

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

- Les dossiers d'enregistrement des Porteurs, des MC ;
- Les demandes de certificat des Porteurs ;
- Les demandes de révocation ;
- Les causes de révocation des certificats des Porteurs.

IX.4.3 Données 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 à caractère personnel

Voir § **Erreur ! Source du renvoi introuvable.**

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 à caractère personnel

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 n'être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du propriétaire des données), décision judiciaire ou autre autorisation légale.

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

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

IX.4.7 Autres circonstances de divulgation de données à caractère personnel

Sans objet

IX.5 DROITS DE PROPRIETE INTELLECTUELLE

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

IX.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

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

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ainsi que des éventuelles données

d'activation ;
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par cette PC et des documents qui en découlent ;
- respecter et appliquer la partie de la PC 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'AGP et l'organisme de qualification ;
- mettre en œuvre les mesures adaptées pour la correction des écarts détectés lors de ces contrôles de conformité ;
- respecter les accords ou contrats qui les lient entre elles ou aux Porteurs ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques, organisationnels et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité ;
- mettre en œuvre des actions de sensibilisation et de formation ;
- mettre en place une documentation de la responsabilité de chacun des acteurs concernés.

IX.6.1 Autorité de Certification

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

IN Groupe 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 PC.

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 Service d'enregistrement

Les obligations de l'AE sont :
- L'identification et l'authentification du Porteur, le cas échéant au travers du MC, et l'identification de son Entité Cliente ;
- La vérification du dossier d'enregistrement du futur Porteur, la validation et le traitement des demandes de certificats ;
- La vérification du dossier d'enregistrement des futurs MC ;
- La délivrance du support personnalisé au Porteur, le cas échéant via le MC ;
- L'envoi sécurisé des données d'activation au Porteur ;
- L'identification de l'émetteur d'une demande de révocation, la validation et le traitement de cette demande ;
- Le respect de la PC de l'AC ;

- L'assurance de la connaissance et de l'acceptation par le Porteur de ses obligations (reprises dans les Conditions Générales d'Utilisation) ;
- L'assurance du respect par les opérateurs d'AE et les MC de leurs obligations respectives (parties de la PC les concernant, lettres d'engagement, etc.) ;

IX.6.3 Porteurs de certificats

Les Porteurs ont pour obligation de :

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

IX.6.4 Utilisateurs de certificats

Les Utilisateurs de Certificats doivent :

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

IX.6.5 Autres participants

Sans objet.

IX.7 LIMITE DE GARANTIE

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

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

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

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

- Utilisation de la clé privée pour un autre usage que celui défini dans le certificat associé ;
- Utilisation d'un certificat pour une autre application que les Applications autorisées ;
- Utilisation d'un certificat pour garantir un autre objet que l'identité du Porteur ;
- Utilisation d'un certificat révoqué ;
- Mauvais modes de conservation de la clé privée du certificat du Porteur ;
- Utilisation d'un certificat au-delà de sa limite de validité ;
- Non-respect des obligations des autres Intervenants (se reporter au § IX.6.4) ;
- Faits extérieurs à l'émission du certificat tel qu'une défaillance de l'application pour laquelle il peut être utilisé ;
- Cas de force majeur tels que définis par les tribunaux français.

IX.8 LIMITE DE RESPONSABILITE

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

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

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

- utilisation d'un certificat pour un usage autre que l'authentification du Porteur ou la protection de la messagerie électronique ;
- utilisation d'un certificat pour garantir un autre objet que l'identité du Porteur pour lequel il a été émis ;
- utilisation d'un certificat révoqué ;
- utilisation d'un certificat au-delà de sa limité de validité.

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

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

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

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

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

IX.9 INDEMNITES

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

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

IX.10.1 Durée de validité

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

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

IX.10.2 Fin anticipée de validité

La publication d'une nouvelle version de la PC type « certificats électroniques de personne » [RGS_A_2], rédigée par l'ANSSI en liaison avec la SGMAP et dont la présente PC vise la conformité, peut entraîner, en fonction des évolutions demandées, la

nécessité pour l'AGP de faire évoluer la PC qu'elle met en œuvre. Le délai de mise en conformité des Autorités qualifiées est arrêté conformément aux modalités prévues par la réglementation en vigueur.

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'AGP s'engage :

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

L'AGP s'engage à adresser à l'ANSSI une synthèse de l'ensemble des modifications apportées à la fourniture de ses services de confiance qualifiés à une fréquence annuelle.

IX.12 AMENDEMENTS A LA PC

IX.12.1 Procédures d'amendement

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

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

Ces amendements sont toutefois effectués en restant conforme aux exigences de la PC type « certificats électroniques de personne » et des éventuels documents complémentaires du RGS.

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

En cas de modification majeure de la PC, l'AGP procède à une vérification de la conformité de la PC par rapport aux PC type « certificats électroniques de personne », et de la conformité des pratiques avec cette nouvelle version de la PC. La PC n'est applicable qu'après validation de l'AGP.

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

L'AGP 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.

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

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

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

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

L'AC informera l'organe de contrôle national (l'ANSSI) dans les meilleurs délais, selon les modalités décrites sur le site https://www.ssi.gouv.fr, de tout changement d'OID avant sa diffusion.

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

IX.13 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

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

IX.14 JURIDICTIONS COMPETENTES

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

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 politiques et les procédures, en fonction desquelles l'AC fonctionne, sont non-discriminatoires.

L'IN Groupe met en place, à chaque fois que cela est possible, des moyens pour faciliter l'accès de ses services aux personnes en situation de handicap.

Par ailleurs, l'IN Groupe délivre des certificats aux administrations et aux entités elles-mêmes déjà soumises à des obligations réglementaires relatives à l'accessibilité. De ce fait, l'utilisation des services proposés par l'IN Groupe au sein de ces établissements est embarquée par les dispositifs d'accessibilité mis en place par ces mêmes entités.

Les textes législatifs et réglementaires applicables à la PC sont, notamment, ceux indiqués au § **Erreur ! Source du renvoi introuvable.** ci-dessus.

IX.16 DISPOSITIONS DIVERSES

IX.16.1 Accord global

Sans objet.

IX.16.2 Transfert d'activités

Voir § V.8

IX.16.3 Conséquences d'une clause non valide

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

IX.16.4 Application et renonciation

Sans objet

IX.16.5 Force majeure

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

IN Groupe 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 PC 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.

X Annexe 1 : Documents cités en référence

X.1 REGLEMENTATION

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 ; https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460
Directive 1999/93/CE du Parlement Européen et du Conseil en date du 13 Décembre 1999 sur un cadre communautaire pour les signatures électroniques.
[Règlement eIDAS] Règlement (UE) No 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (dit « Règlement eIDAS »)
[ORDONNANCE] Ordonnance n°2005-1516 du 8 Décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&dateTexte=vig
Article 801-1 du code de procédure pénale

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

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

X.2 DOCUMENTS TECHNIQUES

[RGS] Référentiel général de sécurité – version 2.0 https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/
[RGS_A_2] Politique de Certification Type « certificats électroniques de personne » - Version 3.0
[RFC 3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[ETSI] ETSI EN 319401 v2.1.1 : General Policy Requirements for Trust Service Providers ETSI EN 319411 : Policy & Security Requirements for TSPs Issuing Certificates ETSI EN 319412 : Certificate Profiles

XI Annexe 2 : Exigences de sécurité du module cryptographique de l'AC

XI.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR et, éventuellement, des réponses OCSP), ainsi que, le cas échéant, générer les bi-clés des certificats émis, doit répondre aux exigences de sécurité suivantes :

- si les bi-clés des certificats émis sont générées par ce module, garantir que ces générations sont réalisées exclusivement

par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- si les bi-clés des certificats émis sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif cryptographique du Porteur et assurer leur destruction sûre après ce transfert ;
- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- si une fonction de sauvegarde et de restauration des clés privée de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

Le module cryptographique de l'AC détecte les tentatives d'altérations physiques et entre dans un état sûr quand une tentative d'altération est détectée

XI.2 EXIGENCES SUR LA QUALIFICATION

Le module cryptographique utilisé par l'AC fait l'objet d'une qualification, au niveau renforcé selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 11.1 ci-dessus.

XII Annexe 3 : Exigences de sécurité du dispositif de protection des éléments secrets

XII.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le dispositif cryptographique, utilisé par le Porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes:
- si la bi-clé du certificat émis est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer un cachet ou une authentification qui ne peut être falsifiée sans la connaissance de la clé privée.

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques doivent être mises en place afin de :
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

XII.2 EXIGENCES SUR LA QUALIFICATION

L'AC fournit un dispositif de protection des éléments secrets au porteur, qualifié au niveau renforcé, selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 12.1 ci-dessus.