Imprimerie Nationale (INCS)

Politique de Certification/ Déclaration des Pratiques de Certification

IGC Document

Programme Plateforme de Gestion des Identités Numériques

Document sécurité

Mode de diffusion	**Publique**
Statut du document	VALIDÉ
Date d'application	**29/11/2024**

HISTORIQUE DES VERSIONS

Version	Date	Auteur	Nature de la révision Paragraphes modifiés
0.1	09/00/2024	Imprimerie Nationale	Version initiale
1.1	23/10/2024	Imprimerie Nationale	Change configuration for a 2 level CA hierarchy
1.2	27/01/2025	Imprimerie Nationale	Change contact mail
1.3	10/03/2025	Imprimerie Nationale	Correction des URL ; correction logo et adresse du siège en bas de page

SOMMAIRE

I. Introduction

I.1. OBJET DU DOCUMENT ET GENERALITES

Le Groupe Imprimerie Nationale a mis en place une Infrastructure de Gestion de clés, baptisée « IGC Document », afin de délivrer des certificats de cachet dans le cadre de signature de QR Code pour différents types de documents officiels de ses clients.
La responsabilité de cette infrastructure de gestion de clés a été confiée à INCS.

INCS offre ainsi des services de certification ayant pour objectif la mise en œuvre de fonctions de scellement (cachet), fonction visant à sceller des données qui seront intégrés dans des QR codes apposés sur les documents produits par l'IN pour le compte de ces clients. En particulier, la présente PC couvre le cas d'usage de la création des QR code au format CEV apposés sur les permis bateau pour son client ANTS. L'IGC a cependant vocation à couvrir potentiellement d'autres types de documents pour d'autres clients. Les pratiques et mesures de sécurité seront cependant communes.

Le présent document constitue la politique de certification (PC) et la déclaration des pratiques de certification (DPC) de l'IGC Document. Elle décrit les différents niveaux de responsabilité, les mesures de sécurité (techniques, audits...) ainsi que les profils des certificats. Elle expose également les engagements des différentes AC de la hiérarchie dans le cadre de la fourniture de ses services de certification électronique pour signature aux usagers.

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

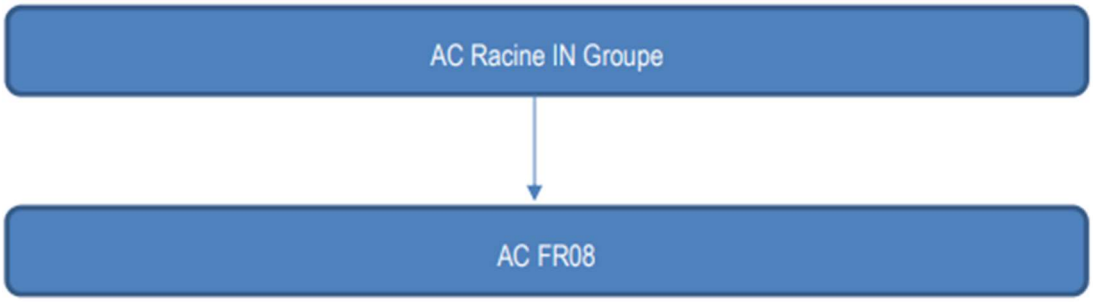
L'IGC Document est composée d'une autorité racine (ACR) baptisée « AC Racine IN Groupe» et, pour cette version de la PC/DPC

- d'autorités finales hiérarchiquement dépendantes de l'ACR, dédiées à un client et fournissant des certificats dédiés à type de document spécifique. La première de celle-ci, dépendante de l'AC ANTS, est baptisée « AC FR08 » et fournit des certificats de cachets dédiés à l'apposition de QR Code sur les permis bateau. L' AC FR08 est incluse dans le domaine de confiance d'INCS puisqu'elles sont rattachées à l' « AC Racine IN Groupe » d'INCS. L' « AC Racine IN Groupe» signe, outre les clés publiques des ACF, les LAR (Liste des Autorités Révoquées).

Chaque ACF est dédiée à un client. Elle peut disposer de plusieurs profils de certificats. Elle signe les clés publiques des porteurs et les LCR.

Il n'existe, dans la version courante de la présente PC/DPC, qu'une seule ACF sous l'AC Racine IN Groupe : il s'agit de l'AC FR08. Cette ACFa elle-même un seul profil de certificat qui est dédiée aux certificats de de scellement de QR code type CEV des permis bateaux produits par l'IN comme le montre la figure suivante.

.



La hiérarchie d'autorité de certification au sein de l'IGC pourra donc être étendue, comme indiquée plus haut :

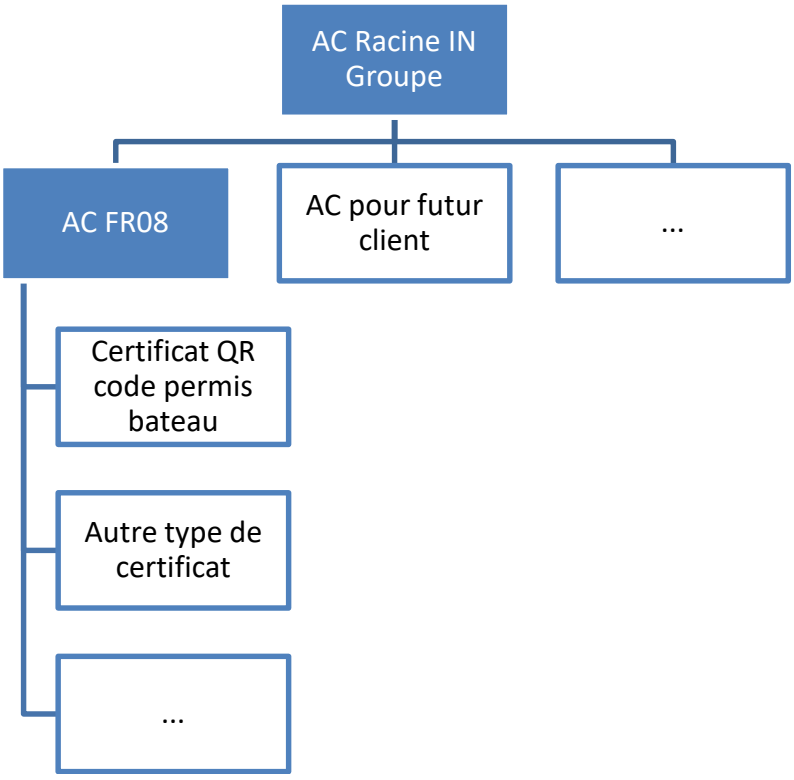


Figure 1 : Hiérarchie des Autorités de Certification

L'ensemble des AC de la hiérarchie étant sous la responsabilité d'INCS, le sigle AC désignera l'autorité morale responsable de cette ACR (AC Racine)des ACF (AC Fille). De façon générale, le document parlera d'ACRet/ou d'ACF, les pratiques étant communes à l'ensemble des clients et documents, sauf mention contraire.

Dans la version courante de la présente PC/DPC, l'ACF délivre un seul type de certificats : des certificat de scellement (cachet)[1].
Dans le cadre de la présente PC/DPC, les certificats cachet pour le scellement des QR code sont exclusivement délivrés au service de création de QR code des ateliers de production de l'IN qui les utilisent (ainsi que les clés privées associées) dans le contexte de la création des documents sur lesquels le QR code est apposé[2].

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

I.2. NOM DU DOCUMENT ET IDENTIFICATION

La présente PC/DPC de l' IGC Document est la propriété INCS
Cette PC/DPC est identifiée dans le tableau suivant par les OID suivants :

	OID associé
Politique de certification de l'AC « Racine IN Groupe »)	1.2.250.1.295.1.2.1.0.2.1.0
Politique de certification de l'AC « FR08 »)	1.2.250.1.295.1.2.1001.0.2.1.0
Certificat cachet pour les permis bateau	1.2.250.1.295.1.2.1001.0.2.107.0

L'OID est composé de la façon suivante (suivant la nomenclature IN Groupe) :

Lettre de l'OID	Désignation	Valeur	Explication
A	Racine	1.2.250.1.295.1	Racine OID
B	Type d'environnement	2	Valeur attribuée à l' IGC Document QR Code
C	Identification de la composante d'AC	1	AC Racine
		2,3,…999	Réservé pour d'autres AC Racines du projet
		1001	AC FR08
		1002, 1003….	Réservé pour de futurs ACF
D	Niveau de sécurité	0	Fixé par convention à 0 pour garder la compatibilité de structure
E	Type de porteur et de certificat	2	Pour équipement. Seuls les équipements sont considérés dans le cadre de cette PC/DPC
F		1	Politique

[1] Les futurs versions de la présente PC/DPC pourront comporter d'autres types de certifciats

[2] Les futures versions pourront considérer d'autres cas d'usage.

	Type de document	2	Déclaration des pratiques
		107	Certificat de cachet
G	Version du document	0	Première version du document

I.3. ENTITES DE L'IGC

La notion d'autorité de certification (AC) telle qu'utilisée dans le présent document est définie au § I.7.1.
L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation) et s'appuie pour cela sur une infrastructure technique dite infrastructure de gestion de clés (IGC). Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.
L'IGC s'appuie sur les services fonctionnels suivants :

- Génération 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/DPC, certificats d'AC, …) ainsi que les résultats des traitements du service de gestion des révocations de certificats (LCR).

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

I.3.1. Autorité de Gestion de la Politique INCS (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.

I.3.2. Les autorités de certification

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

I.3.3. L'autorité d'enregistrement (AE)

L'AE est utilisée pour la mise en œuvre des services d'enregistrement de demandes de certificats, de remise de certificats, de révocation de certificats, de journalisation et d'audit. Dans le cadre de l'AC Permis Bateau, l'AE est directement opérée par l'AC.

I.3.4. Le Service de Publication (SP)

Le SP est utilisé pour la mise en œuvre du service de publication (voir § II).
Le SP agit conformément à la PC/DPC.

I.3.5. Opérateur technique

L'IN est son propre opérateur exploite les clés de l'AC Bateau pour les besoins de génération et révocation de certificats.
L'IN dispose d'une infrastructure matérielle et logicielle lui permettant de générer et émettre des certificats conformément à la présente PC/DPC.
Elle est en charge du bon fonctionnement de l'infrastructure des AC et de la sécurité des moyens informatiques et techniques, de la sécurité des personnels et des locaux.

I.3.6. Porteur de certificat

Est désigné comme « Porteur de certificat », le service de génération de QR code de la chaîne de production de l'IN.
Dans la présente PC/DPC, cette entité (le Porteur) est représenté par une personne physique qui a la responsabilité du Certificat de cachet serveur (RCCS)
La présente PC/DPC impose que la clé privée du Porteur soit stockée exclusivement dans un HSM présent sur la chaîne de production de l'IN.
Le responsable de certificat respecte les conditions qui lui incombent et qui sont définies dans la présente PC/DPC. Ces conditions sont reprises dans les Conditions Générales d'Utilisation qu'il a explicitement acceptées lors de sa demande de certificat.
.

I.3.7. Utilisateurs de certificats (UC)

Un Utilisateur de certificat est une application, utilisé par une personne physique ou morale, visant à vérifier les QR code générés par la chaîne de production. Plus précisément, l'application va lire et décoder le QR code, afin d'extraire la signature électronique qu'il contient et s'appuyer sur les certificats et statuts de révocation pour :

- Vérifier le cachet électronique,
- S'assurer ainsi de l'origine et de l'intégrité des données présentes dans le QR code.

I.3.8. Client Final

Client final pour lequel le document et le QR code est produit, et pour lequel les ACF sont dédiées.

I.4. USAGE DES CERTIFICATS

I.4.1. Domaines d'utilisation applicables

1. Bi-clés et certificats de l'AC

La bi-clé de l'ACF sert à signer les certificats et les listes de certificats révoqués (LCR) qu'elle émet.
L'ACF dispose d'une bi-clé unique pour signer les certificats et les LCR. Cette bi-clé est exclusivement utilisée à cette fin.
Le certificat rattaché à cette bi-clé est signé par l'autorité de niveau supérieur, c'est-à-dire l'ACR.

La chaîne de certification pour l'IGC Document QR code est la suivante :

- Certificat de l'AC Racine (AC hors ligne) : certificat électronique auto-signé,
- Certificat d'une ACF (en ligne) : certificat électronique signé par une ACR,
- Certificat Cachet Porteur : certificat électronique signé par l'ACF.

2. Bi-clés et certificats des Porteurs

La présente PC/DPC traite des bi-clés et certificats émis par l'ACF à destination des catégories de Porteurs identifiées au § I.3.7 (Service de création de QR Code de la chaîne de production de l'IN) afin que ces derniers puisse générer les QRCode à apposer sur les documents officiels du client final.

La vérification du cachet électronique contenue dans un QR code apposé sur le document avec un certificat ACF garantit :

- L'origine des données du QR code : authentification de l'organisme qui a émis/certifié ces données sur le document
- L'intégrité de certaines données du document : le destinataire est assuré que les données lues sur le QR code n'ont pas été modifiées par un tiers et peuvent être comparées à celles présente sur le document pour s'assurer qu'il n'y a pas eu de falsification.

Remarques :

- La vérification du cachet du QR Code avec un certificat émis par l'AC Bateau nécessitant la vérification de la chaîne de certification, cela implique que le certificat de l'AC Bateau soit inclus dans l'outil de lecture de QR Code, ainsi qu'éventuellement toute la chaîne jusqu'à l'AC Racine. Une vérification vis-à-vis d'un certificat de scellement spécifique, attaché par exemple à un type de document, peut aussi être considéré.
- Il est expressément entendu qu'un Porteur de certificat ne peut user de sa clé privée et de son certificat qu'à des fins qu'au fin de la création de QR code pour un document donné dans le cadre d'un contrat avec le client final. 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.

I.4.2. Utilisation interdite des certificats

Les utilisations de certificats émis par l'ACF à d'autres fins que celles prévues par la présente PC/DPC (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/DPC.
L'AC s'engage à faire respecter ces restrictions aux Porteurs et aux Utilisateurs potentiels de ces certificats. À cette fin, l'AC publie à leur destination les Conditions Générales d'Utilisation (CGU). En particulier, la délivrance du certificat à un Porteur est soumise à l'acceptation explicite de ces CGU (mention indiquée dans la demande que le Porteur doit explicitement accepter dans sa demande).

I.5. GESTION ET APPLICATION DE LA PC/DPC

I.5.1. Entité gérant la présente PC/DPC

L'AGP est responsable de la gestion et de la validation de la présente PC/DPC.
Point de contact :

Service SSI
Rue des Frères Beaumont
59128 – Flers-en-Escrebieux
Contact_AC@ingroupe.com

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

I.5.2. Entité déterminant la conformité de la présente PC/DPC

L'AGP à travers son COMITE DE SURVEILLANCE détermine la conformité des pratiques de la PC/DPC. 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.5.3. Procédure d'approbation de la PC/DPC

Les pratiques documentées de la PC/DPC sont approuvées par l'AGP à l'issue d'un processus d'approbation élaboré par l'INCS.
Cette PC/DPC 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/DPC,
- Adapter aux évolutions technologiques.

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

I.6. DOCUMENTS DE REFERENCE

I.6.1. Réglementation

Non applicable

I.6.2. Documents techniques

[RFC 3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[ISO 22376:2023] Sécurité et résilience — Authenticité, intégrité et confiance pour les produits et les documents — Spécifications relatives aux formats de données et l'utilisation du Cachet Électronique Visible (CEV) aux fins d'authentification, de vérification et d'acquisition des données véhiculées par un document ou un objet

I.7. TERMINOLOGIE ET ABREVIATIONS

I.7.1. Terminologie

Audit : Contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures.
Autorité de Certification (AC) : autorité à qui un ou plusieurs Utilisateurs se fient pour créer et attribuer des certificats. [ISO/IEC 9594-8; ITU-T X.509].
Bi-clé : Paire de clés asymétriques, constituée d'une clé publique et de la clé privée correspondante.
Cérémonie de clés : Une procédure par laquelle une bi-clé d'AC est générée et/ou sa clé publique certifiée.
Certificat : clé publique d'une entité, ainsi que d'autres informations, rendues impossibles à contrefaire grâce au chiffrement par la clé privée de l'autorité de certification qui l'a émis [ISO/IEC 9594-8; ITU-T X.509]. 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].
Compromission : violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de la sécurité de cette clé privée.
Confidentialité : La propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus [ISO/IEC 13335-1:2004].

Déclaration des Pratiques de Certification (DPC) : une déclaration des pratiques qu'une entité (agissant en tant qu'Autorité de Certification) applique dans le cadre de fourniture de ses services de certification (demande, émission, renouvellement et révocation de certificats) en conformité avec la PC qu'elle s'est engagée à respecter. [définition PC type RGS].
Disponibilité : La propriété d'être accessible sur demande, à une entité autorisée [ISO/IEC 13335-1:2004].
Données d'activation : Des valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent et qui doivent être protégées (par ex. un PIN, une phrase secrète, …).
Fonction de hachage : fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux trois propriétés suivantes :

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

IGC (Infrastructure de Gestion de Clés) : également appelée Infrastructure à Clé Publique (ICP), c'est l'infrastructure requise pour produire, distribuer, gérer et archiver des clés, des certificats et des Listes de Certificats Révoqués ainsi que la base dans laquelle les certificats et les LCR/LAR doivent être publiés. [2nd DIS ISO/IEC 11770-3 (08/1997)].
Intégrité : fait référence à l'exactitude de l'information, de la source de l'information, et au fonctionnement du système qui la traite.
Liste de Certificats Révoqués (LCR) : liste signée numériquement par une AC et qui contient des identités de certificats déclarés invalides avant leur date de fin de validité (inscrite dans le certificat) ou qui ne sont plus dignes de confiance. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués. Quand la liste contient uniquement des certificats d'AC, le terme Liste des Autorités Révoquées (LAR) est utilisé.
Modules cryptographiques : Un ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé…). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée (FIPS ou critères communs), utilisée pour conserver et mettre en œuvre la clé privée d'AC.
Période de validité d'un certificat : La période de validité d'un certificat est la période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 5280]. En dehors de cette période (avant la date de début de validité et après la date de fin de validité), le certificat est réputé non valide.
Plan de secours (après sinistre) : plan défini par une AC pour remettre en place tout ou partie de ses services d'IGC après qu'ils aient été endommagés ou détruits à la suite d'un sinistre, ceci dans un délai défini dans l'ensemble PC/DPC.
Point de distribution de LCR/LAR : entrée de répertoire ou une autre source de diffusion des LCR ; une LCR diffusée via un point de distribution de LCR peut inclure des entrées de révocation pour un sous-ensemble seulement de l'ensemble des certificats émis par une AC, ou peut contenir des entrées de révocations pour de multiples AC. [ISO/IEC 9594-8; ITU-T X.509].

Politique de Certification (PC) : ensemble de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications possédant des exigences de sécurité communes. [ISO/IEC 9594-8; ITU-T X.509].
Politique de sécurité : ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].
Porteur de secret : personnes qui détient une donnée d'activation liée à la mise en œuvre de la clé privée d'une AC à l'aide d'un module cryptographique.
Qualificateur de politique : Des informations concernant la politique qui accompagnent un identifiant de politique de certification (OID) dans un certificat X.509. [RFC 3647]
Révocation : procédure d'opposition à l'encontre du certificat qui a pour objet de supprimer la garantie d'engagement de l'AC avant la fin de la période de validité. Cette révocation est mise en œuvre à la demande de l'une des parties selon des modalités spécifiques.
RSA : algorithme de cryptographique à clé publique inventé par Rivest, Shamir, et Adleman.
Validation de certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de certification (AC) et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC et la vérification de la chaine de certification. La validation d'un certificat électronique nécessite au préalable d'approuver le certificat de l'autorité Racine (certificat auto-signé).

I.7.2. Abréviations

AGP	Autorité de gestion de la politique
AC	Autorité de Certification
ACF	Autorité de Certification Fille
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'information
DPC	Déclaration des Pratiques de Certification
HSM	*Hardware Security Module*
ICD	*International Code Designator*
IGC	Infrastructure de Gestion de Clés
INCS	Imprimerie Nationale CS (entité juridique du Groupe Imprimerie Nationale responsable de l'IGC Elevée)
IETF	*Internet Engineering Task Force*
ISO	*International Organization for Standardization*
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
OID	*Object Identifier*
PC	Politique de Certification
OCSP	Online Certificate Status Protocol
RCCS	Responsable certificat cachet serveur
RL	Responsable légal
RSA	Rivest Shamir Adleman
SHA-256	*Secure Hash Algorithm 256*
SP	Service de Publication
UC	Utilisateur de certificat

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

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

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

II.2. INFORMATIONS DEVANT ETRE PUBLIEES

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

Informations	Adresse de publication
La présente PC/DPC	https://pc.sikq-ingroupe.com/pc/pc-ac-racine-ingroupe.pdf
Les certificats en cours de validité de l'ACR et de l'ACF	https://sikq-ingroupe.com/cert/ACR-IN-GROUPE.crt https://pc.sikq-ingroupe.com/cert/ac-fr08.crt https://pc.sikq-ingroupe.com/cert/IN01.crt
Les listes d'autorités révoquées (LAR) de l'ACR	http://crl1.sikq-ingroupe.com/crl/ac-racine-in-groupe.crl http://crl2.sikq-ingroupe.com/crl/ac-racine-in-groupe.crl
Les listes des certificats révoqués (LCR) de l'ACF	http://crl1.sikq-ingroupe.com/crl/ac-fr08.crl http://crl2.sikq-ingroupe.com/crl/ac-fr08.crl
L'état de révocation des certificats (serveur OCSP)	http://ocsp.pki.sikq-ingroupe.com

Sauf indications contraires, les autres informations sont réputées confidentielles.
INCS ne publie pas les détails qu'elle juge sensibles voire confidentiels dans sa PC/DPC.
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/DPC applicable
- Les obligations et responsabilités des différentes parties, notamment les exigences relatives à la vérification du statut de révocation d'un certificat pour les Utilisateurs

II.3. DELAIS ET FREQUENCE DE PUBLICATION

Toute nouvelle version de la présente PC/DPC est publiée sur le site du Groupe Imprimerie Nationale dans les 48 heures ouvrées après sa date de mise à jour et sa validation par l'AGP.
Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux § IV.9 et § IV.10
Les certificats d'AC et les informations permettant aux Utilisateurs de certificats de s'assurer de l'origine des certificats émis par l'AC sont diffusés préalablement à toute diffusion de certificats de Porteurs et/ou de LAR/LCR correspondantes.
Les systèmes publiant ces certificats sont accessibles 7j/7 et 24h/24.

II.4. CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées à destination des Utilisateurs de certificats est libre d'accès en lecture et protégé contre les modifications non autorisées.
L'accès en modification aux systèmes de publication des informations d'état des certificats s'effectue au travers d'une authentification (à 2 facteurs).
L'accès en modification aux systèmes de publication des autres informations s'effectue au travers d'une authentification de type ID-Mot de passe basée sur une politique de gestion stricte des mots de passe.

III. Identification et authentification

III.1. NOMMAGE

III.1.1. Type de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.
Dans chaque certificat X.509, l'émetteur (champ « *issuer* ») et le Porteur (champ « *subject* ») sont identifiés par un DN (*Distinguished Name*) de type X.501.

III.1.2. Utilisation de noms explicites

1. Identité de l'AC Racine

Le DN du champ *issuer* du certificat de l'AC Bateau est le suivant :

Attributs du DN	Nom de l'attribut	Valeur
CN	*commonName*	AC RACINE IN GROUPE
OI	*organizationIdentifier*	NTRFR- 352973622
OU	*organizationalUnitName*	0002 352973622
O	*organizationName*	IN GROUPE
C	*countryName*	FR

Remarque :
L' ICD '0002' correspond au Système Informatique pour le Répertoires des Entreprises et des Établissements (SIRENE).
La chaîne de caractère 'NTR' permet d'identifier que la base des immatriculations des entreprises utilisée est le Registre du Commerce.

2. Identité de l'ACF

Attributs du DN	Nom de l'attribut	Valeur	Exemple (pour le premier client et premier document)
CN	*commonName*	<identifiantClient>	FR08
OI	*organizationIdentifier*	NTRFR- 352973622	
OU	*organizationalUnitName*	0002 352973622	
O	*organizationName*	IN GROUPE	
C	*countryName*	FR	

3. Identité du porteur

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

Attributs du DN	Nom de l'attribut	Valeur	Exemple (pour le premier client et le premier document)
CN	*commonName*	<Nom du service de création de QR Code>	IN01
OI	*organizationIdentifier*	NTRFR-352973622	
OU	*organizationalUnitName*	0002 352973622	
OU	*organizationalUnitName*	<description du document>	Permis de conduire - Bateaux de plaisance
O	*organizationName*	IN GROUPE	
C	*countryName*	FR	

Au lancement du service, un seul certificat de cachet sera en place

- CN=IN01
- OU= Permis de conduire - Bateaux de plaisance

Les autres éventuels certificats seront générés sur un modèle similaire.

4. Certificats de test

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

III.1.3. Anonymisation ou pseudonymisation des Porteurs

Sans objet. L'ACF n'émet pas de certificat comportant une identité anonyme ou une identité pseudonyme s'agissant de certificats pour un service de cachet sur une ligne de production.

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'ACF.

III.1.5. Unicité des noms

Les identités portées par l'ACF dans les certificats sont uniques au sein du domaine de certification de l'ACF. L'ACF assure cette unicité par son processus d'enregistrement : un DN attribué à un Porteur ne peut être attribué à un autre Porteur. Du fait du nombre limité de certificats à émettre, cette exigence est réalisée de façon organisationnelle.

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

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

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

III.2. VALIDATION INITIALE DE L'IDENTITE

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

L'opération de génération de la bi-clé du Porteur est réalisée par le porteur. Celui-ci devra fournir une CSR au format PKCS#10.

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

Sans objet, IN Groupe n'émet des certificats que pour son propre usage, c'est-à-dire sa propre ligne de production.

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

La validation initiale d'une personne physique est effectuée dans le cadre de l'enregistrement auprès de l'AE et de la remise de la CSR. L'AE s'assure bien que le responsable de certificat (RC) de la ligne de production est bien le demandeur.

III.2.4. Informations non vérifiées du Porteur

Les certificats émis par l'ACF ne contiennent aucune information non vérifiée.

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.

III.2.6. Certification croisée d'AC

Ce point est sans objet dans la présente PC.

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

L'ACF 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 RCCS
- le responsable légal du client final ou une personne ayant pouvoir.

Une demande de révocation peut être effectuée en prenant contact directement avec l'AC.

IV. Exigences opérationnelles sur le cycle de vie des certificats

IV.1. DEMANDE DE CERTIFICAT

IV.1.1. Origine d'une demande de certificat

La demande de certificat ACF émane du Responsable de Certificat nommé par le responsable de la chaîne de production.
.

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

La demande de certificat se fait au travers d'un outil de demande par ticket interne à IN Groupe.
En premier lieu, le demandeur va demander, via le ticket, à l'équipe SSI de créer une paire de clé sur le HSM de la ligne de production et la CSR associée.
Le ticket devra mentionner :

- Le client final
- Le type de document cible

Une fois la CSR créée, est déposé dans un ticket à destination de la SSI.
Le RCCS devra alors demander l'émission du certificat et accepter explicitement les CGUs du service.

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 RCCS (via l'identité apparaissant dans le ticket – authentification SSO ou équivalent).
- Vérification de la cohérence de la demande avec le contexte du projet (période de renouvellement du certificat, cohérence avec la mise en production d'un nouveau document…)

IV.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande de certificat, l'AE informe le RCCS,

IV.2.3. Durée d'établissement du certificat

La durée maximale de traitement d'une demande de certificat est de 5 jours à partir de la réception et de la validation d'un dossier de demande complet par l'AE.

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 du certificat.

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

L'AC notifie le Porteur et lui transmet le certificat généré.

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 par écrit au travers du suivi du ticket
Il est de la responsabilité du Porteur de vérifier la cohérence des informations portées dans le certificat (par exemple la valeur du CN) avant toute utilisation.
L'acceptation se fait explicitement par une étape sur le ticket. Après installation, et vérification du bon fonctionnement, le ticket sera clos.
En cas de refus explicite du certificat par le RCCS, le certificat sera révoqué.

IV.4.2. Publication du certificat

Les certificats émis par l'ACF dans le cadre de cette PC/DPC ne sont pas rendus publics mais rendu accessible en interne.
Le certificat généré sera publié dans l'outil de gestion de vie des certificats.
Le RCCS et/ou l'équipe projet pourra alors le transmettre au client final pour intégration dans ses applications.

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

Le RCCS est notifié via le ticket de la disponibilité du certificat.
Si le RCCS n'a pas accès à l'outil de gestion des cycles de vie des certification, l'équipe PKI l'ajoute au ticket.
Le processus de notification du client final est à la charge du RCCS et de l'équipe projet.

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

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

L'utilisation de la bi-clé du Porteur et du certificat associé est strictement limitée au service de création de QR Code telle que définie en I.4. L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés : *key Usage* et *Extended Key Usage* (*cf.* VI.1.7 ci-dessous).

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

L'utilisation d'un certificat d'ACF par un UC est limitée aux conditions indiquées dans les extensions *Key Usage* et *Extended Key Usage* du certificat. Plus particulièrement, l'UC vérifiera à l'aide du certificats les données inscrites dans le QR Code.

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/DPC, 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 sont périodiquement renouvelées, selon les recommandations émises par l'ANSSI en matière de cryptanalyse, afin de minimiser les possibilités d'attaques cryptographiques, Ainsi les bi-clés des Porteurs sont renouvelées au minimum tous les 3 ans, durée de validité des certificats délivrés par l'ACF.

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 RC.
Le RCCS est alerté 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

Tout autre renouvellement s'effectue dans les mêmes conditions et selon les mêmes modalités que la demande initiale.

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

Similaire au chapitre IV.3.2.

IV.7.5. Démarche d'acceptation du nouveau certificat

Voir 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/DPC. En cas de modification d'informations, un nouveau certificat doit être délivré avec génération d'une nouvelle bi-clé et révocation de l'ancien certificat.

IV.9. REVOCATION ET SUSPENSION DES CERTIFICATS

IV.9.1. Causes possibles d'une révocation

1. Certificat Porteur

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

- compromission, suspicion de compromission, vol, perte de la clé privée
- 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 service de QR Code de leurs obligations découlant de la PC/DPC
- 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 du Client final) demande la révocation du certificat);
- fin du contrat avec le client final, arrêt de la production de QR Code ;
- révocation du certificat de l'AC

2. Certificat d'une composante de l'IGC

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

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

IV.9.2. Origine d'une demande de révocation

1. Certificat Porteur

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

- Le RCCS
- Le Responsable Légal de l'Entité Cliente pour le compte de laquelle les QR Code sont produits
- L'AC émettrice du certificat ;
- Une composante de l'AC (l'AE) ;

2. Certificat d'une composante de l'IGC

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

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

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

1. Certificat Porteur

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

Une demande de révocation peut être déposée via la création d'un ticket, de façon similaire à la demande initiale.

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 RCCS ainsi que le client final sont informés de la révocation du certificat.

2. Certificat d'une composante de l'IGC

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

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

Le RCCS 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 du client final.

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

1. Certificat Porteur

L'AC traite les demandes de révocation dès que possible suivant sa réception, de préférence immédiatement, et dans un délai inférieur à 48 h jour ouvré. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des Utilisateurs.
La disponibilité du service de révocations est assurée en jour ouvré.
L'AC garantit une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de la fonction de gestion des révocations de 1 jour ouvré et une durée maximale totale d'indisponibilité de 4 jours par mois.

2. Certificat d'une composante de l'IGC

La révocation du certificat d'une composante de l'IGC est effectuée immédiatement dès la détection d'un évènement décrit dans les causes de révocation possibles.
La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR) est effectuée immédiatement en particulier en cas de compromission de la clé privée.

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

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

IV.9.7. Fréquence d'établissement des LCR

La durée de validité de la LCR est de 6 jours.
Une nouvelle LCR est générée et publiée au moins toutes les 12 heures. L'AC ne met en œuvre le mécanisme de delta LCR. En cas de révocation d'un certificat Porteur, la LCR est immédiatement générée et publiée.

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

Après avoir été générée, la LCR est publiée dans un délai maximum de 30 minutes.
Afin d'assurer la durée de 30 minutes depuis la génération de la CRL jusqu'à la publication par IN GROUPE, une CRL générée doit être mise à disposition en pratique dans un délai de 15 minutes

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

L'ACF dispose d'un répondeur OCSP accessible à l'adresse suivante :
http://ocsp.pki.sikq-ingroupe.com
Ce service est mis en place en complément de la publication des LCR en ligne. Ce service répond aux exigences d'intégrité, de disponibilité et de délai de publication décrites dans la présente PC/DPC.

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/DPC.

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

IV.10.1. Caractéristiques opérationnelles

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

IV.10.2. Disponibilité de la fonction

Le service d'information sur l'état des certificats est disponible 24h/24 et 7j/7.

IV.10.3. Dispositifs optionnels

Ce point est sans objet dans la présente PC/DPC.

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

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

IV.12. SEQUESTRE DE CLES ET RECOUVREMENT

Les clés 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/DPC.

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

Ce point est sans objet dans la présente PC/DPC.

V. Mesures de sécurité non techniques

V.1. MESURES DE SECURITE PHYSIQUES

V.1.1. Situation géographique et construction des sites

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

V.1.2. Accès physique

Les moyens et informations de l'IGC utilisés dans le cadre de sa mise en œuvre sont installés dans une salle d'exploitation dont les accès sont contrôlés et réservés aux seules personnes habilitées.
Le système de contrôle des accès permet de garantir la traçabilité des accès aux zones où sont hébergées les IGC.
En dehors des heures ouvrables, la sécurité est 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/DPC. 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/DPC 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 d'application - Le responsable d'application est chargé, de la mise en œuvre de la PC/DPC 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. Dans le cadre de cette IGC, le rôle est assuré par le Responsable Maintien en Condition Opérationnelle d'IN Groupe, qui est responsable de la fourniture de tous les services attendus de la part de la MCO.
- L'ingénieur système - 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 de réseaux de la composante. Dans l'organisation IN Groupe, il s'agit du RSSI
- des officiers de sécurité, en charge, entre autre, de la création des AC et de la configuration de la PKI. Il s'agit, dans l'organisation IN groupe :

  - des administrateurs techniques de la PKI, ils peuvent réaliser les actions d'administration de la PKI (Création d'une AC, de gabarits de certificats, Configuration des CRLs…)
  - des opérateurs PKI réalisant certains actions sensibles sous contrôle du RSSI (révocation, génération de certificat OCSP)
- 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
- 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. Il s'agit ici de l'opérateur de MCO, qui sont les opérateurs IN en charge de la supervision quotidienne du bon fonctionnement de la PKI. Ils ont accès en lecture seul à l'exception du droits de révocation, exercé sur demande en cas d'incapacité de l'officier de sécurité à réaliser l'opération.
- Le contrôleur ou auditeur – Personne autorisée à accéder et en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission. Ce rôle est tenu par le Responsable du dispositif d'analyse récurrente des journaux à des fins d'identification d'anomalies.

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.

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

Sans objet.

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/DPC 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-feu 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,

1. *Informations enregistrées pour chaque évènement*

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

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

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

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

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

2. *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,
- Réception d'une demande de révocation,
- Validation / rejet d'une demande de révocation,

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 certificats des Porteurs,
- Publication et mise à jour des informations liées aux AC (PC/DPC, certificats d'AC, CGU, etc.)
- Génération puis publication des LCR,
- Requêtes et réponses OCSP.

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, …).

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 le contrôleur é 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 selon la politique de journalisation. 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.

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 en cas de soupçon de compromission.

Un test d'intrusion avant la mise en production 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.
Les vulnérabilités détectées à l'occasion de ces contrôles donnent lieu à une analyse pour identifier et évaluer leurs conséquences et impacts éventuels. Selon 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 (PC/DPC),
- Les certificats, LCR et réponses OCSP tels qu'émis ou publiés,
- Les dossiers d'enregistrement (ticket de demande),
- Les journaux d'événements des différentes composantes de l'IGC.

V.5.2. Période de conservation des archives

1. Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable. En l'occurrence, il est archivé pendant au moins cinq ans, comptés au maximum à partir de l'acceptation du certificat par son Porteur.
Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat peut être présenté par l'AC lors de toute sollicitation par les autorités habilitées. Ce dossier, complété par les mentions consignées par l'AE, doit permettre de retrouver l'identité réelle de la personne physique désignée dans le certificat émis par l'AC.

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 5 ans après leur expiration.

3. Réponses OCSP

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

4. Journaux d'événements

Les journaux d'événements tels que traités au § V.4 est selon la politique de journalisation définie.

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/DPC.

V.5.5. Exigences d'horodatage des données

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

V.5.6. Système de collecte des archives

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

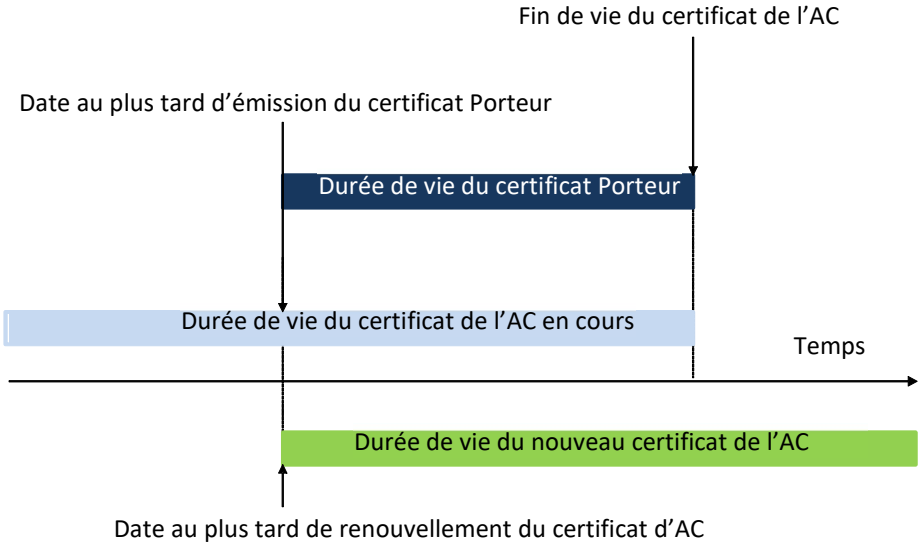
V.5.7. Procédure de récupération et de vérification des archives

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

V.6. CHANGEMENT DE CLE D'AC

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

L'AC ne peut pas générer de certificats dont la durée de vie dépasse la période de validité de son certificat d'AC. C'est pourquoi, la bi-clé de l'AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats émis.
Dès qu'une nouvelle clé privée est générée pour l'AC, seule celle-ci est utilisée pour générer de nouveaux certificats de Porteurs. Le précédent certificat de l'AC reste valable pour valider le chemin de certification des anciens certificats émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats Porteurs émis à l'aide de cette bi-clé.



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

V.7. REPRISE SUITE A COMPROMISSION ET SINISTRE

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

Chaque entité agissant pour le compte de l'IGC met en œuvre des procédures de remontée d'incident et de traitement des incidents. Ceci est réalisé au travers de la sensibilisation et la formation des personnels et au travers de l'analyse des journaux d'événements.
Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui en informe immédiatement l'AC. Le cas de l'incident majeur est impérativement traité dès réception et la publication de l'information de révocation du certificat, s'il y a lieu, est faite dans la plus grande urgence, voire immédiatement, par tout moyen utile ou disponible. Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses Porteurs devient insuffisant pour son utilisation prévue restante, alors l'AC informe tous les Porteurs

et les tiers Utilisateurs de certificats avec lesquels l'AC a passé des accords. De plus tous les certificats concernés sont révoqués.
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/DPC, 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,
- 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/DPC (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

1. Clé de l'AC

La génération des bi-clés associées au certificat d'AC se déroule lors d'une cérémonie de clés à l'aide d'une ressource cryptographique matérielle qualifiée au niveau Standard.
Les cérémonies de clés se déroulent sous le contrôle d'au moins trois personnes ayant des rôles de confiance (maître de cérémonie et témoins dont au moins est externe à l'AC). Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement approuvé par l'AC.
Suite à leur génération, les parts de secrets (données d'activation) sont remises à des Porteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même Porteur ne peut détenir plus d'une part de secret de l'AC à un moment donné. Chaque part de secrets est mise en œuvre par son Porteur.

2. Clés des Porteurs

Les bi-clés des Porteurs sont générées par le porteur dans un module un module cryptographique.

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

Sans objet.

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

La clé publique est transmise au travers de la CSR (voir III.2.1).

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

Les certificats de l'ACR et des ACF sont disponibles aux URL citées au chapitre II.2 de la présente PC/DPC.

VI.1.5. Tailles des clés

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

1. Clés d'AC

ACR
La bi-clé est de type ECDSA P-256 bits
L'algorithme de hashage est SHA-256 dont l'OID est 1.2.840.113549.1.1.13.

ACF
La bi-clé est de type ECDSA P-256 bits
L'algorithme de hashage est SHA-256 a minima

2. Clés Porteurs

Les bi-clés sont de type ECDSA Courbe P-256
L'algorithme de hashage est SHA-256

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

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

VI.1.7. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'ACR et du certificat associé est strictement limitée à la signature de certificats et des LAR.
L'utilisation de la clé privée de l'ACF 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 au service de génération de cachet encodés dans un QR Code dans le cadre de cette version de la PC/DPC.

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

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

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

Le Porteur met en œuvre un module cryptographique qualifié au niveau renforcé.

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

Ce chapitre porte sur le contrôle de la clé privée des 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.2.9 et sa destruction au § VI.2.11.
Le contrôle des clés privées de signature de AC est assuré par du personnel de confiance (Porteurs de secret d'IGC) et met en œuvre un outil de partage des secrets (3 exploitants parmi 5 doivent s'authentifier).

VI.2.4. Séquestre de la clé privée

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

VI.2.5. Copie de secours de la clé privée

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

VI.2.6. Archivage de la clé privée

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

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

1. Clés privées d'AC

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

2. Clés privées des Porteurs

Sans objet.

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

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

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

1. Clés privées d'AC

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

2. Clés privées des Porteurs

L'activation est sous la responsabilité du porteur.

VI.2.10. Méthode de désactivation de la clé privée

1. Clés privées d'AC

Les ressources cryptographiques matérielles dans lesquelles des clés d'AC ont été activées ne sont pas laissées sans surveillance ou accessibles à des personnes non autorisées. Après utilisation, les ressources cryptographiques matérielles sont désactivées. Les ressources cryptographiques sont ensuite stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.
Les ressources cryptographiques de signature de l'AC sont en ligne uniquement afin de signer des certificats Porteurs et des LCR après avoir authentifié la demande de certificat et la demande de révocation.

2. Clés privées des Porteurs

Hors périmètre de l'AC.

VI.2.11. Méthode de destruction des clés privées

1. Clés privées d'AC

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

2. Clés privées des Porteurs

Le porteur devra effacer la clé conformément aux directives du fabriquant de HSM, et supprimer les éventuelles copies de sauvegarde.

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

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

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'ACF est de 9 ans. La durée de vie de la bi-clé correspondante est équivalente, soit 9 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/DPC ont une durée de validité de 2 ans maximum. La durée de vie des bi-clés est équivalente, soit 2 ans également.

VI.4. DONNEES D'ACTIVATION

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

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

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

2. Données d'activation des clés privées des Porteurs

Hors du périmètre de l'AC

VI.4.2. Protection des données d'activation

1. AC

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

2. Porteur

Hors du périmètre de l'AC

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

VII. Profil des certificats et des LCR

VII.1. PROFILE DE L'AC RACINE

VII.1.1. Champs du certificat

Certificat d'AC		
Champs	**Qualification**	**Production**
Version	2 (=version 3	2 (=version 3
SerialNumber	Fourni par le service (unique et généré de manière aléatoire	Fourni par le service (unique et généré de manière aléatoire
SignatureAlgorithm	SHA 256 with ECDSA	SHA 256 with ECDSA
Issuer	CN = AC RACINE IN GROUPE TEST 2.5.4.97 = NTRFR- 352973622 OU = 0002 352973622 O = IN GROUPE C = FR	CN = AC RACINE IN GROUPE 2.5.4.97 = NTRFR- 352973622 OU = 0002 352973622 O = IN GROUPE C = FR
Validity		
NotBefore	Date de la génération de la bi-clé	Date de la génération de la bi-clé
NotAfter	Date de la génération de la bi-clé + 20 ans	Date de la génération de la bi-clé + 20 ans
SubjectPublicKeyInfo	ECC (256 bits)	ECC (256 bits)
Subject	CN = AC RACINE IN GROUPE TEST 2.5.4.97 = NTRFR- 352973622 OU = 0002 352973622 O = IN GROUPE C = FR	CN = AC RACINE IN GROUPE 2.5.4.97 = NTRFR- 352973622 OU = 0002 352973622 O = IN GROUPE C = FR

VII.1.2. Extensions du certificat

Extension	criticité	Qualification	Production
KeyUsage	O	KeyCertSign crlSigning	KeyCertSign crlSigning
Certificate Policies	N		
PolicyIdentifier		anyPolicy	
policyQualifierId		CPS	

Qualifier		https://pc.sikq-ingroupe.com/pc/pc-ac-racine-in-groupe-test.pdf	https://pc.sikq-ingroupe.com/pc/pc-ac-racine-ingroupe.pdf
AuthorityKeyIdentifier	N		
KeyIdentifier		Identifiant de la clé publique de l'AC Racine Permis Bateau	Identifiant de la clé publique de l'AC Racine Permis Bateau
SubjectKeyIdentifier	N		
KeyIdentifier		Identifiant de la clé publique de l'AC Racine Permis Bateau	Identifiant de la clé publique de l'AC Racine Permis Bateau
BasicConstraints	O		
CA		vrai	vrai
pathLenConstraint		1	1

VII.2. PROFILE DE L'AC FRX8

VII.2.1. Champs du certificat

Certificat d'AC		
Champs	**Qualification**	**Production**
Designation de l'AC	**ACFR98**	**ACFR08**
Version	2 (=version 3)	2 (=version 3)
SerialNumber	Alloué automatiquement	Alloué automatiquement
SignatureAlgorithm	SHA 256 with ECDSA	SHA 256 with ECDSA
Issuer	CN = AC RACINE IN GROUPE TEST 2.5.4.97 = NTRFR- 352973622 OU = 0002 352973622 O = IN GROUPE C = FR	CN = AC RACINE IN GROUPE 2.5.4.97 = NTRFR- 352973622 OU = 0002 352973622 O = IN GROUPE C = FR
Validity		
NotBefore	Date de la génération de la bi-clé	Date de la génération de la bi-clé
NotAfter	Date de la génération de la bi-clé + 9 ans	Date de la génération de la bi-clé + 9 ans
Public Key Algorithm	ECDSA_P256	ECDSA_P256
SubjectPublicKeyInfo	ECC (256 bits) Exp = 65537	ECC (256 bits) Exp = 65537
Subject	CN = FR98 OrgID = NTRFR- 352973622 OU = 0002 352973622	CN = FR08 OrgID = NTRFR- 352973622 OU = 0002 352973622

	O = IN GROUPE C = FR	O = IN GROUPE C = FR
SignatureValue	Valeur de la signature	Valeur de la signature

VII.2.2. Extensions du certificat

Extension	criticité	Qualification	Production
KeyUsage	O	KeyCertSign crlSigning	KeyCertSign crlSigning
Certificate Policies	N		
PolicyIdentifier		anyPolicy	anyPolicy
policyQualifierId		CPS	CPS
Qualifier		https://pc.sikq-ongroupe.com/pc/pc-ac-racine-in-groupe-test.pdf	https://pc.sikq-ingroupe.com/pc/pc-ac-racine-in-groupe.pdf
AuthorityKeyIdentifier	N		
KeyIdentifier		hash of IssuerPublicKey hash of IssuerPublicKey	hash of IssuerPublicKey hash of IssuerPublicKey
SubjectKeyIdentifier	N		
KeyIdentifier		hash of SubjectPublicKey	hash of SubjectPublicKey
BasicConstraints	O		
CA		vrai	vrai
pathLenConstraint		0	0
CRLDistributionPoint	N	http://crl1.sikq-ingroupe.com/crl/acr-ingroupe-test.crl http://crl2.sikq-ingroupe.com/crl/acr-ingroupe-test.crl	http://crl1.sikq-ingroupe.com/crl/acr-ingroupe.crl http://crl2.sikq-ingroupe.com/crl/acr-ingroupe.crl
AuthorityInformation Access	N	accessMethod : id-ad-caIssuers accessLocation : https://sikq-ingroupe.com/cert/acr-in-groupe-test.crt	accessMethod : id-ad-caIssuers accessLocation : https://sikq-ingroupe.com/cert/ACR-IN-GROUPE.crt

VII.3. PROFILE DE CERTIFICAT : SIGNATURE DE QR CODE

VII.3.1. Champs du certificat

Certificat d'AC		
Champs	**Qualification**	**Production**
Version	2 (=version 3)	2 (=version 3)
SerialNumber	Alloué automatiquement	Alloué automatiquement
SignatureAlgorithm	SHA 256 with ECDSA	SHA 256 with ECDSA
Validity		
NotBefore	Date de la génération de la bi-clé	Date de la génération de la bi-clé
NotAfter	Date de la génération de la bi-clé + 3 ans	Date de la génération de la bi-clé + 3 ans
Subject	CN = IT01 OrgID = NTRFR- 352973622 OU = 0002 352973622 OU = Permis de conduire - Bateaux de plaisance - POUR QUALIFICATION O = IN GROUPE C = FR	CN = IN01 OrgID = NTRFR- 352973622 OU = 0002 352973622 OU = Permis de conduire - Bateaux de plaisance O = IN GROUPE C = FR
Public Key Algorithm	ECDSA_P256	ECDSA_P256
SubjectPublicKeyInfo	ECC (256 bits)	ECC (256 bits)
SignatureValue	Valeur de la signature	Valeur de la signature

VII.3.2. Extensions du certificat

Extension	criticité	Qualification	Production
KeyUsage	O	nonRepudiation (0x40)	nonRepudiation (0x40)
Certificate Policies	N		
PolicyIdentifier		1.2.250.1.295.1.2.1001.0.2.107.0	1.2.250.1.295.1.2.1001.0.2.107.0
UUID		1ed2780d91334f3bb3efc8f0641347c6	1ed2780d91334f3bb3efc8f0641347c6
policyQualifierId		CPS	CPS
Qualifier		https://pc.sikq-ongroupe.com/pc/pc-ac-racine-in-groupe-test.pdf	https://pc.sikq-ingroupe.com/pc/pc-ac-racine-in-groupe.pdf
AuthorityKeyIdentifier	N		

KeyIdentifier		hash of IssuerPublicKey hash of IssuerPublicKey	hash of IssuerPublicKey hash of IssuerPublicKey
SubjectKeyIdentifier	N		
KeyIdentifier		hash of SubjectPublicKey	hash of SubjectPublicKey
BasicConstraints	O		
CA		vrai	vrai
pathLenConstraint		0	0
CRLDistributionPoint	N	http://crl1.sikq-ingroupe.com/crl/ac-fr98.crl http://crl2.sikq-ingroupe.com/crl/ac-fr98.crl	http://crl1.sikq-ingroupe.com/crl/ac-fr08.crl http://crl2.sikq-ingroupe.com/crl/ac-fr08.crl
AuthorityInformation Access	N	accessMethod : id-ad-caIssuers accessLocation : http://pc.sikq-ingroupe.com/cert/ac-fr98.crt id-ad-ocsp: http://ocsp.ppd.pki.sikqingroupe.com	accessMethod : id-ad-caIssuers accessLocation : http://pc.sikq-ingroupe.com/cert/ac-fr08.crt id-ad-ocsp : http://ocsp.pki.sikq-ingroupe.com

VII.4. FORMAT DES ARL/CRL

Champs	Qualification	Production	Commentaire
Onglet général			
Version	V2	V2	
Signature Algorithm	SHA 256 with ECDSA	SHA 256 with ECDSA	
Issuer	CN= FR98 OU=0002 352973622 O=IN GROUPE C=FR	CN= FR08 OU=0002 352973622 O=IN GROUPE C=FR	
thisUpdate	Date d'émission	Date d'émission	
nextUpdate	Date de la prochaine publication	Date de la prochaine publication	6 jours après la date d'émission pour une LCR d'une AC Déléguée

Extension onglet général			
Authority Key Identifier	Non Critique	Hash of IssuerPublicKey	
CRLnumber Non	Non Critique	Numéro de la CRL	
expiredCertOnCRL	Non Critique	Date à partir de laquelle la CRL inclus les certificats expirés	OID de l'extension : 2.5.29.60 et type GeneralizedTime

Onglet révocation list , : Liste des certificats révoqués			
Serial number	Numéro de série du certificat		
Revocation date	Numéro de série du certificat		
signatureAlgorithm	SHA 256 with ECDSA		
signatureValue	Valeur de la signature numérique		

VII.5. OCSP

IN Groupe met en oeuvre son propre répondeur OCSP sur la PKI Nexus.
Les certificats de signature OCSP seront générés par IN Groupe.

VIII. Audit de conformité et autres évaluations

La présente hiérarchie d'AC ne fait pas l'objet de conformité. Elle est cependant opérée dans le même environnement et avec des pratiques similaires aux AC qualifiées RGS et certifiées ETSI EN 319 411-1 et ETSI EN 319 411-2, et bénéficie, de ce fait, des éventuels améliorations du niveau de sécurité conséquent aux audits sur les autres AC.

VIII.1. FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

Non applicable.

VIII.2. IDENTITES / QUALIFICATIONS DES EVALUATEURS

Non applicable.

VIII.3. RELATIONS ENTRE EVALUATEURS ET ENTITE EVALUEE

Non applicable.

VIII.4. SUJETS COUVERTS PAR LES EVALUATIONS

Non applicable.

VIII.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

Non applicable.

VIII.6. COMMUNICATION DES RESULTATS

Non applicable.

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 production des documents finaux par IN Groupe.

IX.1.2. Tarifs pour accéder aux certificats

Les certificats sont gratuitement accessibles aux Utilisateurs.

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

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

IX.2. RESPONSABILITE FINANCIERE

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

IX.2.1. Couverture par les assurances

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

IX.2.2. Autres ressources

INCS est en capacité financière de remplir sa mission.

IX.2.3. Couverture et garantie concernant les Entités utilisatrices

Les entités utilisatrices doivent être en capacité financière de pouvoir accomplir leur mission.
En cas de dommage pour un client causé par une des AC sous contrôle d'INCS, celle-ci fera appel à son assurance pour couvrir une partie des dommages du client dans la limite de la responsabilité d'INCS définie dans les conditions générales de services INCS et aux présentes.

IX.3. CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

IX.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- les parties non publiques de la PC/DPC de l'AC et les procédures internes associées,

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

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, aux opérateurs d'AE en lien avec l'Entité Cliente de rattachement du Porteur.

IX.4. PROTECTION DES DONNEES PERSONNELLES

IX.4.1. Politique de protection des données personnelles

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

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

IX.4.2. Informations à caractère personnel

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

- Les dossiers d'enregistrement des Porteurs;

- Les demandes de certificat des Porteurs ;
- Les demandes de révocation ;
- Les causes de révocation des certificats des Porteurs.

IX.4.3. Informations à caractère non personnel

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

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

Voir § IX.4.1
L'AC a mis en place et respecte des mesures de protection des données à caractère personnel notamment afin de garantir leur sécurité et ce dans le respect des principes de proportionnalité et de transparence.

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

L'AC s'engage à respecter la finalité de la collecte et de traitement des données à caractère personnel.
Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles identifiées dans cette PC/DPC ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du propriétaire des données), décision judiciaire ou autre autorisation légale.

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

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

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

Sans objet

IX.5. DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

La PC/DPC s'inscrit dans le cadre du respect des droits de propriété intellectuelle et industrielle. INCS conserve tous les droits de propriété intellectuelle et est propriétaire de la présente PC/DPC, 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/DPC et des documents qui en

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

IX.6.1. Autorité de certification

L'AC s'engage à :
- Pouvoir démontrer aux Utilisateurs de ses certificats qu'elle a émis un certificat pour un Porteur donné et que ce dernier a accepté ce certificat conformément au § 4.4 ;
- Garantir et maintenir la cohérence de sa PC/DPC ;
- 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 ;
- Sensibiliser les différents acteurs à la sécurité et aux technologies mises en œuvre.

INCS doit prendre les dispositions nécessaires pour couvrir les responsabilités liées à ses activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente PC/DPC.
De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence dûment prouvée, d'elle-même ou de l'une de ses composantes, qu'elle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération et le détournement des données personnelles des Porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.
Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AC.

IX.6.2. Autorité d'Enregistrement

Les obligations de l'AE sont :
- L'identification et l'authentification du RCCS et l'identification du client final;
- La vérification du dossier d'enregistrement du futur Porteur, la validation et le traitement des demandes de certificats ;
- L'identification de l'émetteur d'une demande de révocation, la validation et le traitement de cette demande ;
- Le respect de la PC/DPC 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 de leurs obligations respectives (parties de la PC/DPC les concernant, lettres d'engagement, etc.) ;

IX.6.3. RCCS et Porteurs de certificats

Les RCCS, représentant les Porteurs des certificats ont pour obligation de :

- Communiquer des informations exactes et à jour lors de la demande de certificat (demande initiale ou renouvellement) ;
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant (décrites dans les CGU et la PC/DPC) ;
- 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, 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/DPC.

IX.7. LIMITE DE GARANTIE

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

- Son identification et authentification grâce à son certificat signé par l'ACR ;
- 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/DPC.

Ces garanties sont exclusives de toute autre garantie de l'AC.
Il est expressément entendu que INCS ne saurait être tenu pour responsable ni d'un dommage résultant d'une faute ou négligence d'un Client et/ou de ses Porteurs ni d'un dommage causé par un fait extérieur ou un cas de force majeur, notamment en cas de :

- Utilisation de la clé privée pour un autre usage que celui défini dans le certificat associé ;
- Utilisation d'un certificat pour une autre application que les Applications autorisées ;
- Utilisation d'un certificat pour garantir un autre objet que l'identité du Porteur ;
- Utilisation d'un certificat révoqué ;
- Mauvais modes de conservation de la clé privée du certificat du Porteur ;
- Utilisation d'un certificat au-delà de sa limite de validité ;
- Non-respect des obligations des autres Intervenants (se reporter au § IX.6.4) ;

- 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/DPC, 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/DPC ainsi que dans tout autre document contractuel applicable associé, en particulier :

- utilisation d'un certificat pour un usage autre que ceux prévus dans la présente PC/DPC
- 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 limite 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/DPC lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1148 du Code civil.

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

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

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

IX.9. INDEMNITES

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

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

IX.10.1. Durée de validité

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

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

IX.10.2. Fin anticipée de validité

En fonction des évolutions demandées ou de la création de nouvelles AC au sein de l'IGC, la nécessité pour l'AGP de faire évoluer la PC/DPC qu'elle met en œuvre peut survenir.
La mise à jour 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/DPC.

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/DPC 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

Sans objet

IX.12. AMENDEMENTS A LA PC

IX.12.1. Procédures d'amendement

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

- à chaque évolution des systèmes de l'IGC ou des procédures internes à l'IGC ayant un impact sur la PC/DPC ;
- à chaque fois qu'une évolution remarquable de l'état de l'art ou d'une législation/réglementation en vigueur le justifie ;
- lors de l'ajout d'un nouveau client ou d'un nouveau type de document

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

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/DPC 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/DPC.
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 changée

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

Toutefois, les Porteurs et Utilisateurs de certificat peuvent facilement identifier et accéder sur le site de publication à la version de la PC/DPC sous laquelle le certificat concerné a été émis par l'AC. Le site diffuse en effet, outre la version courante de la PC/DPC, 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.

IX.13. DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

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

IX.14. JURIDICTION COMPETENTE

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

IX.15. CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

La présente PC/DPC 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'INCS met en place, de façon générale 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'INCS 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'INCS 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/DPC sont, notamment, ceux indiqués au § I.6 ci-dessus.
En l'espèce, l'usage est ici strictement interne IN Groupe, de ce fait, sur ce périmètre précis, la mise en place de mesures d'accessibilité grand public n'est pas applicable.

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/DPC s'avèrerait être non valide au regard de la loi applicable, ceci ne remettrait pas en cause la validité et l'applicabilité des autres clauses.

IX.16.4. Application et renonciation

Sans objet

IX.16.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.
INCS ne saurait être tenu pour responsable et n'assume aucun engagement pour tout retard dans l'exécution ou pour toute inexécution d'obligations résultant de la présente PC/DPC 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/DPC ne formule pas d'exigence spécifique sur le sujet.