MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

ANFSI

IGC DES FORCES DE SÉCURITÉ INTÉRIEURE

Mesures de sécurité communes

1.2.250.1.668.1.1.1.8.1

Direction générale de la Gendarmerie nationale
4 rue Claude Bernard
CS 60003
92136 Issy les Moulineaux CEDEX

HISTORIQUE DES MODIFICATIONS

Version	Date	Objet de la modification	Auteur	Statut
0.1	12/2023	Version initiale	Sealweb	projet
0.2	03/2024	Compléments	CNE MRQ	projet
1	22/05/24	Validation par autorité administrative	ANFSI	Validé

Table des matières

A. Introduction

A.1. Objet du document

L'ANFSI a mis en place et exploite une IGC, disposant d'une autorité de certification (AC) racine et d'AC subordonnées. L'IGC de l'ANFSI est notée « IGC/FSI » dans ce document.

Le présent document présente les mesures organisationnelles, les mesures techniques et non-techniques mises en œuvre par les AC de l'ANFSI pour la délivrance de certificats aux entités finales (personnes physiques et machines). Ce document est complémentaire des politiques de certification des AC émettrices et fait intégralement partie de ces politiques.

A.2. Numérotation

Afin de distinguer les sections des politiques de certification et celles du présent document, ces dernières sont numérotées alphabétiquement (A, B, C…) ; les chapitres des PC sont numérotées en chiffres romains (I, II, III…).

B. Gestion des PC

Toutes les PC de l'IGC/FSI sont gérées de la même façon, et par une entité commune. La DPC est commune aux différentes AC.

B.1. Entité gérant les PC

Les PC et les DPC afférentes sont élaborées et maintenues par l'Autorité Administrative (AA), représentée par le Chef de la direction de la sécurité et de l'architecture (DSA).

B.2. Point de contact

Pour toute remarque ou question relative aux PC, le point de contact est :

Direction Générale de la Gendarmerie Nationale
Agence du numérique des forces de sécurité intérieure
Direction de la sécurité et de l'architecture
4 rue Claude Bernard
CS 60003
92136 Issy les Moulineaux Cedex
FRANCE

B.3. Entité déterminant la conformité d'une DPC avec une PC

Les personnes habilitées à déterminer la conformité de la DPC avec les PC sont nommées par l'AA. Il s'agit des personnels de la SGI. Un contrôle est également effectué par le BASSI et la société externe lors des audits internes.

B.4. Procédures d'approbation de la conformité de la DPC

L'AA dispose d'un processus de gestion (mise à jour, révisions) de la DPC et d'approbation de sa conformité avec la PC. La validation finale de la DPC est annoncée en COPIL.

Toute nouvelle version de la PC est publiée, conformément aux exigences du chapitre C, sans délai.

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

C.1. Entités chargées de la mise à disposition des informations

Les AC, objet de cette PC, disposent d'une fonction de publication et d'une fonction d'information sur l'état des certificats.

Les documents sont publiés à destination des porteurs et des utilisateurs de certificats à l'adresse suivante :

http://igc.gendarmerie.fr

https://www.gendarmerie.interieur.gouv.fr/igc/pc

La publication de ces éléments se fait manuellement. Elle est de la responsabilité de l'AA.

Les informations d'état des certificats sont publiées sous forme de liste de certificats révoqués (LCR) aux adresses suivantes :

- http://crl.gendarmerie.fr

Des réplications sont faites sur les adresses suivantes :

http://crl.gendarmerie.interieur.gouv.fr

http://crl.gendarmerie.interieur.ader.gouv.fr

La publication de ces éléments est automatisée pour les CRL signées par les AC subordonnées. Elle est manuelle pour la LAR de l'AC Racine FSI. Elle est de la responsabilité de l'ACR (qui est également ACD).

L'ensemble des certificats tant révoqués que expirés sont présents dans la CRL.

Un script mis en place au groupe de sécurité opérationnelle (GSOP STIG) automatise la surveillance des publications de CRL, vérifie la signature de l'AC, et vérifie la persistance des numéros de série des certificats (révoqués et expirés) au fil des CRL et remonte une alarme en cas de détection d'anomalie.

Aucun service OCSP n'est disponible.

C.2. Informations devant être publiées

Les informations publiées sont :

Sur Internet :

- les politiques de certification et le présent document ;
- les certificats de la chaîne de certification des AC en cours de validité pour les certificats de signature ;
- les listes des certificats révoqués (LCR) délivrées et signées par les AC subordonnées ;
- les conditions générales d'utilisation applicables aux services de certification ;

Sur intranet :

- les politiques de certification et le présent document ;
- les certificats de la chaîne de certification des AC en cours de validité ;
- les listes des certificats révoqués (LCR) délivrées et signées par les AC subordonnées ;
- les conditions générales d'utilisation applicables aux services de certification ;

Les documents sont rédigés en français.

C.3. Délais et fréquences de publication

Les informations sont publiées dans les meilleurs délais après la disponibilité d'une nouvelle version.

En particulier,

- les informations liées à l'IGC (PC, conditions générales…) sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC ;
- les certificats d'AC sont diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants ;
- les délais et fréquences de publication des informations d'état des certificats sont décrits aux chapitres IV.9 et IV.10.

Les informations ont une disponibilité de 24h/24 et 7j/7, des contraintes de disponibilité particulières étant définies pour les informations d'état des certificats aux chapitres IV.9 et IV.10.

C.4. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC. La publication est lancée automatiquement par l'IGC dès lors qu'une nouvelle CRL est générée.

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées de l'IGC. La publication est gérée par la SGI qui transmet les informations à publier au G2CM ANFSI via un ticket de changement.

Le GSOP exécute un script de contrôle de l'intégrité. Il est mis en copie du ticket de changement de toutes les demandes de publication afin de mettre à jour les informations d'intégrité (*hash*).

D. Mesures de sécurité non techniques

D.1. Mesures de sécurité physique

D.1.1. Situation géographique et construction des sites

Les sites d'hébergement des composantes de l'IGC/FSI se trouvent sur le territoire national dans les deux centres de données du Service de Traitement de l'Information Gendarmerie (STIG).

D.1.2. Accès physique

La plate-forme de certification de l'IGC/FSI est hébergée et utilisée dans une zone protégée, au sens des articles 413-7, et R. 413-1 à R. 413-5 du Code pénal.

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. La sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. Toute personne entrant dans ces zones physiquement sécurisées n'est jamais laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

D.1.3. Alimentation électrique et climatisation

La prévention physique contre des incidents matériels, y compris concernant l'alimentation électrique et climatisation, est effectuée conformément aux normes s'appliquant aux établissements et aux locaux hébergeant une ou plusieurs composantes de l'infrastructure.

Ces dispositions garantissent les engagements de disponibilité des différents services pris dans cette PC.

De plus, la plate-forme de l'IGC/FSI est protégée contre les signaux parasites compromettants lors de la mise en œuvre des fonctions et informations dont le besoin de confidentialité est élevé.

D.1.4. Vulnérabilité aux dégâts des eaux

La plate-forme de l'IGC/FSI est hébergée dans des locaux protégés contre les dégâts des eaux, de façon à garantir les engagements de disponibilité des différents services pris dans cette PC.

D.1.5. Prévention et protection incendie

La prévention physique contre des incidents matériels, y compris concernant la prévention et la protection incendie, est effectuée conformément aux normes s'appliquant aux établissements et aux locaux hébergeant une ou plusieurs composantes de l'infrastructure.

Ces dispositions garantissent les engagements de disponibilité des différents services pris dans cette PC.

Les consignes de sécurité incendie sont vérifiées et connues des utilisateurs de la plate-forme de l'IGC/FSI.

D.1.6. Conservation des supports

La conservation des informations sensibles ou classifiées de défense, sur quelque medium que ce soit, est effectué conformément à la réglementation pour les documents sensibles ou classifiés de défense.

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. L'AC met en place des mesures pour éviter la compromission et le vol de ces informations.

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils sont manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion protège ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

D.1.7. Mise hors service des supports

La destruction des articles contrôlés de la sécurité des systèmes d'information (ACSSI) et des supports d'informations sensibles sera réalisée conformément à la réglementation en vigueur pour les documents sensibles ou classifiés de défense.

Ainsi les disques durs seront démagnétisés puis déchiquetés.

D.1.8. Sauvegardes hors site

Dans le cadre d'un plan anti-sinistre, l'ARA a mis en place des politiques et procédures qui permettent de rétablir les opérations dès que possible en cas d'accident, y compris la compromission des clés de signature privées des AC. Ces mesurent garantissent une disponibilité des fonctions de l'IGC conforme aux engagements pris dans cette PC. Le rétablissement des opérations se fait dans le respect des exigences de sécurité exposées dans cette PC.

Le responsable du plan anti-sinistre est chef du STIG.

Les modalités de déclenchement du plan anti-sinistre sont définies par l'ARA.

D.2. Mesures de sécurité procédurales

D.2.1. Rôles de confiance

Les rôles définis pour les AC subordonnées sont :

- **Autorité :** personne physique ayant un rôle de responsabilité dans l'IGC. Ce rôle est défini à la section II, III et IV de [GESTION_ROLES].
- **Responsable d'AC subordonnée** : la personne physique responsable d'une AC subordonnée, notamment de l'utilisation de son certificat et de sa bi-clé correspondante. Ce rôle est défini à la section V de [GESTION_ROLES].
- **Administrateur** : responsable du bon fonctionnement de l'ensemble des services rendus par l'autorité de certification, notamment de l'organisation et du bon déroulement des séances nécessitant la mise en œuvre d'un outil cryptographique par un opérateur. Il est responsable de l'ensemble des services rendus par l'AC. Responsable également de la préparation des documentations relatives à :

l'installation de l'application, l'initialisation des ressources cryptos, la cérémonie des clés, les scripts additionnels (génération des CRLs, supervision, …), configuration initiale d'EJBCA avant coupure/limitation des accès aux personnes physiques, supervision des services rendus par le STIG (CRL-eyes). Ce rôle est défini à la section VII, VIII, XVIII et XIX de [GESTION_ROLES].

- **Auditeur** : personne désignée par l'AC de l'ANFSI et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre de la politique de certification et des services effectivement fournis par l'AC. Responsable de la vérification de la conformité des procédures, vérification de l'application des procédures, vérification de la configuration des éléments de l'IGC, vérification du suivi de l'IGC (COPIL, indicateurs). Ce rôle est défini aux sections XV, XVI et XX de [GESTION_ROLES].
- **Ingénieur système** : il est chargé de la mise en route, de la configuration et de la maintenance technique de la plate-forme informatique hébergeant l'AC. Il assure l'administration de l'ensemble des composants nécessaires à la plate-forme (Machines virtuelles, SGBD, réseaux, supervision). Ce rôle est défini aux sections VI, IX, X, XI, XII, XIII, XIV et XXVI de [GESTION_ROLES].
- **Opérateur** : l'opérateur de l'AC réalise l'exploitation des services offerts par l'autorité, dans le cadre de ses attributions. Il est chargé de lancer l'exécution des fonctions cryptographiques. Ce rôle est défini à la section XXI de [GESTION_ROLES].
- **Opérateur de certification (OC)** : l'opérateur de certification est un organisme fournissant le service de certification de clés publiques émetteurs, distribution de certificats aux émetteurs et de prise en compte des révocations de certificats, sur la base des informations détenues par l'autorité d'enregistrement. Il s'agit d'AGeC@PE.
- **Responsable de sécurité de l'AC** : il est responsable de l'application de la politique de sécurité physique et fonctionnelle de l'AC. Il gère les contrôles d'accès physiques à la plate-forme informatique et est chargé de mettre en œuvre la politique de sécurité. Ce rôle est défini à la section XXII de [GESTION_ROLES].
- **Responsable de publication** : il est responsable de la publication des documents de l'IGC sur le site de publication. Ce rôle est défini à la section XXIV de [GESTION_ROLES].
- **Porteur de secret** : il est responsable de la conservation d'une part du secret des AC, soit en tant que commandant d'une unité détentrice, soit en tant que représentant temporaire du porteur.. Ce rôle est défini à la section XVII et XXV de [GESTION_ROLES].

Le nom et la fonction de tous les personnels amenés à travailler au sein de composantes de l'IGC/FSI sont explicitement précisés dans le document [GESTION_ROLES]

Les personnes ayant un rôle de confiance sont habilitées. Les personnels ont connaissance et comprennent les implications des opérations dont ils ont la responsabilité.

D.2.2. Nombre de personnes requises par tâches

Selon le type d'opérations effectuées, le nombre et le type de rôles et de personnes devant nécessairement être présentes (en tant qu'acteurs ou témoins) peuvent être différents. L'annexe « Rôles par opération » de la DPC permet de définir un nombre d'exploitants minimum nécessaires par type d'opérations.

D.2.3. Identification et authentification pour chaque rôle

L'identification et l'authentification des personnes commandant une action en fonction d'un rôle ayant trait à la gestion d'un certificat s'appuient sur des mesures organisationnelles.

Chaque composante met en place une gestion des droits d'accès selon les besoins et les autorisations définies par la présente PC qui respecte la séparation des rôles.

La déclaration des pratiques de certification décrit les actions effectuées.

D.2.4. Rôles exigeant une séparation des attributions

L'attribution des rôles aux différentes personnes se fait en évitant au maximum le cumul des attributions.

Les rôles incompatibles entre eux sont définis dans le document [GESTION_ROLES]

D.3. Mesures de sécurité vis-à-vis du personnel

D.3.1. Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité vis-à-vis de leur employeur. Dans le cas des agents d'autorités administratives, ceux-ci sont soumis à leur devoir de réserve.

Chaque entité opérant une composante de l'IGC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.

Les AC de l'IGC/FSI informent toute personne intervenant dans des rôles de confiance de l'IGC/FSI :

- de ses responsabilités relatives aux services de l'IGC/FSI,
- des procédures liées à la sécurité du système et au contrôle du personnel.

En particulier, les personnes intervenant dans des rôles de confiance doivent y être formellement affectées par l'encadrement supérieur chargé de la sécurité.

D.3.2. Procédures de vérification des antécédents

Afin de s'assurer de l'honnêteté et de la capacité d'une personne à tenir son rôle dans l'infrastructure de gestion des clés, l'ANFSI effectue des vérifications.

Ces procédures sont décrites dans la déclaration des pratiques de certification.

D.3.3. Exigences en matière de formation initiale

Le personnel exécutant est formé aux logiciels, matériels et procédures internes de fonctionnement de la composante pour laquelle il opère.

D.3.4. Exigences et fréquence en matière de formation continue

Tout nouvel exploitant doit suivre une formation initiale au système, aux politiques de sécurité, au plan de secours, aux logiciels et opérations qu'il doit mettre en œuvre. Chaque employé devra assister à une formation après toute évolution importante du système.

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

L'AC n'établit aucune de règle concernant cette partie.

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

L'AA en concertation avec l'ARA décide des sanctions à appliquer lorsqu'un acteur abuse de ses droits ou effectue une opération non conforme à ses attributions.

D.3.7. Exigences vis-à-vis du personnel des prestataires externes

Les personnels contractants doivent respecter les mêmes conditions que celles énoncées dans les rubriques D.3.1, D.3.2, D.3.3, D.3.4.

D.3.8. Documentation fournie au personnel

Les documents dont doit disposer le personnel, en fonction de son besoin d'en connaître pour l'exécution de sa mission, sont les suivants :

- PC de l'IGC/FSI ;
- DPC de l'IGC/FSI ;
- documents constructeurs des matériels et logiciels utilisés ;
- procédures internes de fonctionnement.

Les AC et l'AE veillent à ce que leur personnel respectif (comme défini dans la DPC) possède bien les documents identifiés ci-dessus en fonction de leur besoin d'en connaître comme le précise la DPC.

D.4. Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer de façon manuelle ou automatique. Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

D.4.1. Type d'événements à enregistrer

Les entités opérant une composante de l'IGC journalisent au minimum les événements suivants :

- événements physiques dont la trace n'est pas fournie automatiquement par le système,
  - registre des accès physiques aux postes de travail de l'IGC/FSI ;
  - autres registres dépendants de la configuration du site physique, à préciser dans la DPC tels que :
    - journaux des accès des personnes,
    - changements concernant les personnes,
    - changement de configuration du système,
    - opérations menées sur les postes informatiques de l'IGC/FSI et relatives aux opérations rendues par l'IGC/FSI ;
    - opérations menées sur les postes informatiques et matériels du réseau de l'AC subordonnée ;
  - actions menées en cérémonie de clés, consignées dans les procès-verbaux de cérémonie, comme :
    - initialisation de secrets,
    - affectation de secrets à des porteurs de secrets,
    - utilisation de secrets,
    - destruction de secrets.
  - publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- événements généraux tracés par le système ou une application :
  - démarrage et arrêt des applications,
  - connexion / déconnexion des utilisateurs ayant des rôles de confiance
  - modification de paramètres de configuration,
  - installation et désinstallation d'un logiciel ou périphérique matériel,
  - messages d'alerte de l'application, du système d'exploitation ou du réseau ;
  - création de nouveaux comptes.
  - modification ou suppression de comptes utilisateurs
  - changements de mots de passe,

- modifications de droits d'accès,
- événements métiers tracés par les applications :
  - enregistrement :
    - enregistrement d'un nouvel utilisateur (dans la base de données interne),
    - éventuellement demande de renouvellement ;
  - génération de certificat :
    - génération des certificats des porteurs ;
    - génération des données de création et de vérification de l'AC ;
    - remise de la carte au porteur.
  - révocation de certificat :
    - demande de révocation,
    - révocation de certificat,
    - génération d'une LCR,
    - publication d'une LCR.
  - génération de clés cryptographiques (enregistrement les données propres à cette opération conformément aux PC d'applications utilisées)
    - demande de génération
    - transmission
    - destruction ;
  - séquestre et recouvrement
    - Séquestre d'une clé privée de porteur,
    - Réception d'une demande de recouvrement,
    - Recouvrement d'une clé privée,
    - Destruction d'une clé privée séquestrée ;
  - communications avec le service de publication ;
- remise à zéro du journal d'audit,

Pour tout événement, les informations minimales enregistrées sont :
- date et heure de l'opération,
- nom de l'exécutant,
- type de l'opération,
- résultat de l'événement

En fonction du type de l'événement, d'autres informations peuvent être ajoutées :
- organisme destinataire de l'opération,
- nom des personnes présentes,
- nom du représentant de l'ARA et des AC subordonnées,
- cause de l'événement,
- autre information caractérisant l'événement (un identifiant par exemple).

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

L'analyse du contenu des journaux d'événements est effectuée de manière régulière par l'AC de l'IGC/FSI, au minimum une fois par semaine. Un traitement particulier pour les alertes est décrit dans la DPC.

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

Les journaux sont conservés 1 mois sur site et archivés jusqu'à la fin de vie de l'IGC/FSI sur le site de rétention des archives.

D.4.4. Protection des journaux d'événements

Les journaux d'événements sont protégés en intégrité et confidentialité conformément aux réglementations.

D.4.5. Procédure de sauvegarde des journaux d'événements

Chaque entité opérant une composante de l'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC.

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

Les journaux d'événements sont centralisés dans un outils de collecte.

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

La notification de l'enregistrement des événements est réalisée lors de la signature des CGU.

D.4.8. Évaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée. Les journaux d'évènements sont contrôlés une fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec. Ils sont analysés dans leur totalité au moins une fois par semaine.

Cette analyse donne lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'événements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) est effectué une fois par mois, ceci afin de vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.

D.5. Archivage des données

D.5.1. Types de données à archiver

L'AC prend des dispositions en matière d'archivage pour assurer la pérennité des informations ou données produites, en particulier les journaux constitués par les différentes composantes de l'IGC.

L'archivage permet la conservation des preuves liées aux opérations de certification (dossiers de demande, signature des CGU des certificats…), que ces documents se trouvent sous forme papier ou électronique. Il assure leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les conditions générales d'utilisation ;
- les accords contractuels avec d'autres AC ;
- les certificats, LCR tels qu'émis et publiés ;
- les dossiers de demande et les CGU des certificats
- les justificatifs d'identité des porteurs ;
- les journaux d'événements des différentes entités de l'IGC ;
- les procès-verbaux de cérémonies de clés.

II.1.1. Période de conservation des archives

Dossiers de demande de certificat
Tout dossier de demande de certificat accepté est archivé jusqu'à la fin de vie de l'IGC/FSI, et au minimum 10 ans à compter de la demande du certificat, sur le site de rétention des archives.

Certificats, LCR émis par l'AC
Les certificats de clés de porteurs et d'AC, ainsi que les LCR / LAR produites sont archivés jusqu'à la fin de vie de l'IGC/FSI, et au minimum 10 ans à compter de leur génération, sur le site de rétention des archives.

Journaux d'événements
Les journaux d'événements traités en section D.4 seront archivés jusqu'à la fin de vie de l'IGC/FSI, et au minimum 10 ans après leur génération. Des mesures de contrôles d'accès, de redondance et de contrôle des conditions de stockage assurent leur intégrité.

Autres journaux
La DPC précise les moyens mis en œuvre pour archiver les autres journaux.

D.5.2. Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, sont :
- protégées en intégrité ;
- accessibles uniquement aux personnes autorisées ;
- disponible pour pouvoir être relues et exploitées.

La DPC précise les moyens mis en œuvre pour archiver les pièces en toute sécurité.

D.5.3. Procédure de sauvegarde des archives

La DPC décrit la procédure de sauvegarde des archives.

D.5.4. Exigences d'horodatage des données

Voir section D.4 pour la datation des journaux d'événements.

Voir section E.8 précise les exigences en matière de datation / horodatage.

D.5.5. Système de collecte des archives

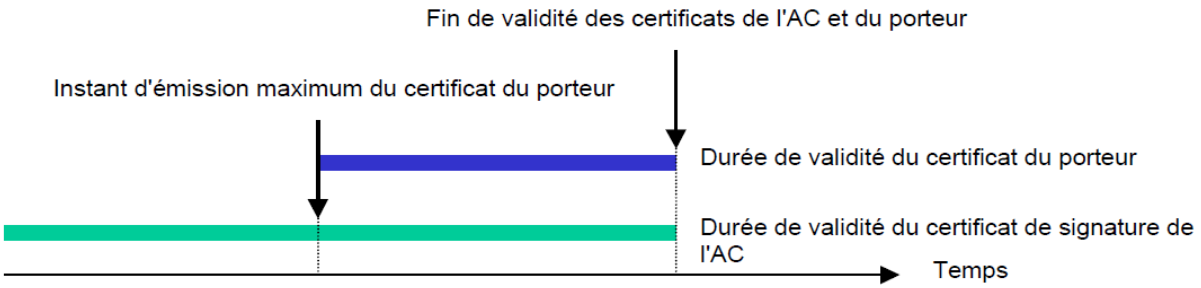
Le système de collecte des archives est interne à l'IGC et respecte les exigences de protection des archives concernées.

D.5.6. Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) peuvent être récupérées dans un délai inférieur à deux (2) jours ouvrés.

D.6. Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.



Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée doit être utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

D.7. Reprise suite à compromission et sinistre

D.7.1. Procédures de remontée et de traitement des incidents et des compromissions

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens permettent de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

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'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur est traité dès détection 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 et disponible. L'AC doit également prévenir directement et sans délai le point de contact identifié sur le site www.cyber.gouv.fr doit être immédiatement informé.

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. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- révoque tout certificat concerné.

D.7.2. Procédures 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 permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan est testé au minimum 1 fois tous les 2 ans.

D.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante

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

Dans le cas de compromission d'une clé d'AC, le certificat correspondant est immédiatement révoqué (voir IV.9 dans la PC).

En outre, l'AC respecte au minimum les engagements suivants :

- informer les entités suivantes de la compromission : tous les porteurs, et les tiers utilisateurs et d'autres AC ;
- indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

D.7.4. Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC.

D.8. Fin de vie de l'IGC

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

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La 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.

D.8.1. Transfert d'activité ou cessation d'activité[1] affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC:

1) Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats, archivage de séquestre le cas échéant).
2) Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication de l'état des certificats), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC.

L'AC avisera les porteurs et les utilisateurs de certificats aussitôt que nécessaire, sous un délai d'un mois au minium. L'AC établira un plan d'action circonstancié et le communiquera à l'ANSSI afin de minimiser les impacts de tous ordres de cet événement. L'AC tiendra informée l'ANSSI de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus.

D.8.2. Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité sera progressive

1 Cessation d'activité d'une composante autre que l'AC

de telle sorte que seules les obligations ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans le document [Cessation d'activité].

La DPC stipule les dispositions prises en cas de cessation de service, en particulier :

- la notification des entités affectées ;
- le transfert de ses obligations à d'autres parties ;
- la gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC doit :

1) s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
1) prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
2) révoquer son certificat ;
3) révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
4) informer (par exemple par récépissé) tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre III.2.3 de la PC).

E. Mesures de sécurité techniques

E.1. Génération et installation de bi-clés

E.1.1. Génération des bi-clés

E.1.1.1 Clés d'AC

Les clés de signature d'AC sont générées dans un environnement sécurisé (*cf.* chapitre D).

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique qualifié au niveau renforcé.

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. D.2.1), dans le cadre de cérémonies de clés. Ces cérémonies se déroulent suivant des scripts préalablement définis.

Le script de « Cérémonie des clés » indique :

- L'ensemble des rôles des participants de la cérémonie. Au moins deux personnes ayant des rôles de confiance et un témoin externe à l'AC et impartial participent à la cérémonie.
- Les fonctions de chacun de ces rôles et les phases auxquelles ils interviennent
- Leurs responsabilités durant la cérémonie et à l'issue de celle-ci
- Les preuves qui seront recueillis durant la cérémonie.

La cérémonie fait l'objet d'un PV signé des participants attestant qu'elle s'est déroulée conformément à la procédure prévue et démontrant que l'intégrité et la confidentialité de la génération de la paire de clé a été assurée.

La cérémonie peut inclure la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC. Les parts de secrets sont remis pendant la cérémonie à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Le PV de cérémonie liste les parts de secrets générés ou utilisés et leurs détenteurs respectifs.

E.1.1.2 Clés porteurs générées par l'AC

La génération des clés d'authentification et de chiffrement des porteurs est effectuée par l'AC dans un environnement sécurisé (*cf.* chapitre D).

Ces bi-clés sont générés dans un module cryptographique qualifié au niveau renforcé, puis transférées de manière sécurisée dans la carte du porteur. Un séquestre de la bi-clé de confidentialité est réalisé.

E.1.1.3 Clés porteurs générées par le porteur

Se référer à la PC.

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

Se référer à la PC.

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

Les requêtes de demande de certificat du porteur sont transmises à l'AC au format PKCS#10, dont l'intégrité et l'origine sont authentifiées par l'AC.

E.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 via le certificat de l'AC publié conformément aux dispositions du chapitre C.

E.1.5. Tailles des clés

Les clés d'AC sont des clés RSA 4096 bits.

Les clés des porteurs sont des clés RSA 2048 bits pour les certificats contenus dans les cartes JCOP3 P60, ou RSA 3072 bits pour les autres supports.

Ces caractéristiques sont conformes à l'état de l'art et respectent les exigences de sécurité du RGS.

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

Toutes les clés sont générées dans des composants qualifiés. Il peut s'agir des puces des cartes ou des HSM. La qualité des bi-clés et leurs paramètres de génération dépendant des équipements utilisés et ces derniers étant qualifiés dans ce cadre, elles sont réputées conformes à l'état de l'art tant que la qualification est maintenue.

E.1.7. Objectifs d'usage de la clé

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

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la fonction de sécurité concernée.

E.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

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

E.2.1.1 Modules cryptographiques de l'AC

Les modules cryptographiques utilisés par l'AC, pour ses clés de signature et celles des porteurs, sont des modules cryptographiques qualifiés au niveau renforcé.

E.2.1.2 Dispositifs de protection des éléments secrets des porteurs

Se référer à la PC.

E.2.2. Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets.

E.2.3. Séquestre de la clé privée

Se référer à la PC, le cas échéant.

E.2.4. Copie de secours de la clé privée

Hormis pour les clés privées de confidentialité, les clés privées des porteurs ne font l'objet d'aucune copie de secours.

Les clés privées d'AC font l'objet de copies de secours dans des fichiers chiffrés, générés par le mécanisme natif du module cryptographique. Ce chiffrement offre un niveau de sécurité équivalent au stockage au sein du module cryptographique.

Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne sont à aucun moment en clair en dehors du module cryptographique.

E.2.5. Archivage de la clé privée

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

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

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

Concernant les clés des porteurs, se référer à la PC.

Pour les clés privées d'AC, tout transfert (sauvegarde, restauration) se fait sous forme chiffrée, conformément aux exigences de la section E.2.4.

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

Les clés privées d'AC sont stockées dans un module cryptographique qualifié au niveau renforcé, excepté leurs sauvegardes qui respectent des exigences du E.2.4.

L'AC garantit, en tout état de cause, que les clés privées d'AC ne sont pas compromises pendant leur stockage ou leur transport.

E.2.8. Méthode d'activation de la clé privée

E.2.8.1 Clés privées d'AC

L'activation des clés privées d'AC dans le module cryptographique est contrôlée via des données d'activation (*cf.* E.4) et fait intervenir au moins deux personnes dans des rôles de confiance (des porteurs de secrets).

E.2.8.2 Clés privées des porteurs

Se référer à la PC.

E.2.9. Méthode de désactivation de la clé privée

E.2.9.1 Clés privées d'AC

La désactivation des clés privées d'AC dans le module cryptographique est automatique dès qu'il est arrêté, mis à jour au niveau de sa configuration logicielle ou technique.

E.2.9.2 Clés privées des porteurs

Se référer à la PC.

E.2.10. Méthode de destruction des clés privées

E.2.10.1 Clés privées d'AC

La destruction des clés privées d'AC dans le matériel cryptographique est réalisée par une fonction nominale du matériel qui garantit un effacement sécurisée. La destruction des sauvegardes est réalisée conformément à des directives précises d'effacement sécurisé des supports (effacement et écrasements successifs).

E.2.10.2 Clés privées des porteurs

Se référer à la PC.

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

Le module cryptographique de l'AC sont qualifiées par l'ANSSI au niveau renforcé.

Concernant les dispositifs des porteurs, se référer à la PC.

E.3. Autres aspects de la gestion des bi-clés

E.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.

E.3.2. Durées de vie des bi-clés et des certificats

Concernant les dispositifs des porteurs, se référer à la PC.

L'AC s'interdit d'émettre des certificats dont la durée de vie dépasse celle du certificat de l'AC.

E.4. Données d'activation

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

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

La génération et l'installation des données d'activation du module cryptographique de l'AC se font lors de la phase d'initialisation et de personnalisation de ce module, dans le cadre d'une cérémonie de clés. Les porteurs de ces données en sont les détenteurs exclusifs, ils les reçoivent directement en main propre et sont responsables de leur confidentialité et de leur intégrité.

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

Se référer à la PC.

E.4.2. Protection des données d'activation

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

Cf. §E.4.1.1.

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

Se référer à la PC.

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

Il n'y a pas d'autres aspects lié aux données d'activation.

E.5. Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques répondent à une politique de sécurité interne de l'ANFSI, qui couvre les objectifs de sécurité de l'IGC.

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

La DPC décrit un ensemble de mesures permettant de répondre aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique),
- gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non- autorisés et mises à jour des logiciels,
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- protection du réseau contre toute intrusion d'une personne non autorisée,
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- fonctions d'audits (non-répudiation et nature des actions effectuées),
- éventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés privées séquestrées des porteurs, des clés secrètes ou privées des composantes de l'infrastructure font l'objet de mesures particulières de sécurité.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système sont mises en place.

E.5.2. Niveau de qualification des systèmes informatiques

Le module cryptographique de l'AC et les puces des cartes des porteurs sont qualifiées par l'ANSSI au niveau renforcé.

E.6. Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité décrites dans la DPC garantissent le maintien du niveau de sécurité durant toute la durée de vie de l'IGC, donc pour le cycle de vie complet des biens sensibles.

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

L'implémentation de l'infrastructure de l'IGC est documentée. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau sont documentées et contrôlées.

Cette implémentation répond aux objectifs de sécurité définis en amont pour l'IGC et utilise des systèmes et des produits fiables qui sont protégés contre toute modification.

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

Les processus internes de gestion de configuration de l'AC garantissent l'évaluation et la documentation de toute évolution significative, afin de maintenir le niveau de sécurité et l'emploi des matériels qualifiés dans l'environnement préconisé.

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

La DPC décrit les processus d'évaluation.

E.7. Mesures de sécurité réseau

L'IGC n'est pas interconnectée avec des réseaux publics, excepté pour la publication des informations sur un site internet. Cet accès est protégé par contrôles d'accès et une restriction aux seuls protocoles nécessaires.

Les composants du réseau sont sécurisés et leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC. Les modules cryptographiques sont maintenus dans un environnement dédié physiquement sécurisé.

E.8. Horodatage / Système de datation

Les événements consignés dans les différents journaux de l'IGC sont horodatés par l'horloge des serveurs sur lesquels ils sont générés. Tous les serveurs en ligne sont synchronisés sur une source fiable de temps UTC, au minimum à la seconde près. L'heure des serveurs hors ligne est corrigée si besoin avant la réalisation d'une opération de l'IGC.

F. Audit de conformité et autres évaluations

La suite du présent chapitre concerne les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC (et non ceux de qualification RGS).

F.1. Fréquences et / ou circonstances des évaluations

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

L'AC procède également régulièrement à un contrôle de conformité de l'ensemble de son IGC, 1 fois tous les 2 ans.

F.2. Identités / qualifications des évaluateurs

Le contrôle d'une composante est assigné par l'AC à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

F.3. Relations entre évaluateurs et entités évaluées

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

F.4. Sujets couverts par les évaluations

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

L'AC est en mesure de justifier qu'il a pris les mesures nécessaires pour assurer la protection des échanges d'information entre les différentes composantes de l'IGC. Elle vérifie périodiquement les mesures de sécurité prises dans ce cadre, par exemple au moyen d'audits techniques.

F.5. Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : "réussite", "échec", "à confirmer".

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.
- En cas de résultat "à confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

F.6. Communication des résultats

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

G.Autres problématiques métiers et légales

G.1. Tarifs

Sans objet, les services de l'IGC/FSI n'étant pas facturés aux AC subordonnées ni aux entités finales (personne physique).

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

Sans objet.

G.1.2. Tarifs pour accéder aux certificats

Sans objet.

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

Sans objet.

G.1.4. Tarifs pour d'autres services

Sans objet.

G.1.5. Politique de remboursement

Sans objet.

G.1.6. Couverture par les assurances

L'état étant sont propre assureur, tous les frais seront couvert par le ministère de l'intérieur.

G.1.7. Autres ressources

Sans objet

G.2. Responsabilité financière

L'état étant sont propre assureur, tous les frais dont la responsabilité serait imputés à la gendarmerie seront couvert par le ministère de l'intérieur.

G.2.1. Couverture et garantie concernant les entités utilisatrices

Tout usage non explicitement permis est interdit et engage la responsabilité du porteur.

G.3. Confidentialité des données professionnelles

G.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- la DPC de l'AC,
- les clés privées de l'AC, des composantes et des porteurs de certificats,
- les clés privées séquestrées des porteurs,
- les données d'activation associées aux clés privées d'AC et des porteurs,
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- les dossiers d'enregistrement des porteurs,
- les causes de révocations, sauf accord explicite du porteur.

G.3.2. Informations hors du périmètre des informations confidentielles

Les informations publiques sont les politiques de certification, les certificats d'AC ainsi que les CRL.

G.3.3. Responsabilités en termes de protection des informations confidentielles

L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre G.3, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

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

L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français. 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 l'accès à ces informations au porteur.

G.4. Protection des données à caractère personnel

G.4.1. Politique de protection des données à caractère personnel

Il est entendu que toute collecte et tout usage de données à caractère personnel par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi [CNIL].

G.4.2. Données à caractère personnel

Les données considérées comme personnelles sont au moins les suivantes :

- les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur) ;
- le dossier d'enregistrement du porteur.

G.4.3. Données à caractère non personnel

Sans objet.

G.4.4. Responsabilité en termes de protection des données à caractère personnel

Cf. G.15.

G.4.5. Notification et consentement d'utilisation des données à caractère personnel

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne sont ni divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

Cf. G.15.

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

Sans objet.

G.5. Droits de propriété intellectuelle

L'ensemble des moyens de l'infrastructure de gestion des clés respecte et applique la législation et la réglementation en vigueur sur le territoire français.

G.6. Interprétations contractuelles et garanties

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

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre F) et l'organisme de qualification,
- 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 et humains) nécessaires à la réalisation des
- prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

G.6.1. Autorités de Certification

L'AC a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences du chapitre IV.4 de la PC.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant de leurs droits et obligations 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 par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC est responsable de la conformité de sa Politique de Certification avec les exigences émises dans la présente PC. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la présente PC, par elle-même ou l'une de ses composantes. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou 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.

En cas de non-respect ponctuel des obligations décrites dans la présente PC, l'Administration se réserve le droit de refuser temporairement ou définitivement les certificats de l'AC conformément à la réglementation en vigueur.

G.6.2. Service d'enregistrement

Cf. les obligations pertinentes du G.6.1.

G.6.3. Porteurs de certificats

Le porteur a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- protéger sa clé privée par des moyens appropriés à son environnement ;
- protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- protéger l'accès à sa base de certificats ;
- respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- informer l'AC de toute modification concernant les informations contenues dans son certificat ;
- faire, sans délai, une demande de révocation de son certificat auprès de l'AE, du MC de son entreprise ou de l'AC en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activation).

La relation entre le porteur et l'AC ou ses composantes est formalisée par un engagement du porteur visant à certifier l'exactitude des renseignements et des documents fournis.

G.6.4. Responsable de certificat (RC)

Le RC a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- protéger la clé privée du service applicatif dont il a la responsabilité par des moyens appropriés à son environnement ;
- protéger les données d'activation de cette clé privée et, le cas échéant, les mettre en oeuvre ;
- protéger l'accès à la base de certificats du service applicatif ;
- respecter les conditions d'utilisation de la clé privée du service applicatif et du certificat correspondant ;
- informer l'AC de toute modification concernant les informations contenues dans le certificat électronique ;
- faire, sans délai, une demande de révocation du certificat électronique dont il est responsable auprès de l'AC en cas de compromission ou de suspicion de compromission de la clé privée correspondante (ou de ses données d'activation).

La relation entre le RC et l'AC ou ses composantes est formalisée par un engagement du RC visant à certifier l'exactitude des renseignements et des documents fournis.

G.6.5. Utilisateurs de certificats

Les utilisateurs utilisant les 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'à l'AC Racine, vérifier la signature numérique 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 exprimées dans la présente PC ;

- contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application qu'ils utilisent.

G.6.6. Autres participants

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

G.7. Limite de garantie

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

G.8. Limite de responsabilité

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

G.9. Indemnités

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

G.10. Durée et fin anticipée de validité de la PC

G.10.1. Durée de validité

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

G.10.2. Fin anticipée de validité

La présente PC peut être remplacée par une version plus récente. La présente PC peut par exemple évoluer suite à la publication d'une nouvelle version de la PC Type du RGS.

Une évolution de la PC n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

G.10.3. Effets de la fin de validité et clauses restant applicables

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

G.11. Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra :

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

G.12. Amendements à la PC

G.12.1. Procédures d'amendements

L'AC contrôle que tout projet de modification de sa PC reste conforme aux exigences de la PC Type du RGS et des éventuels documents complémentaires du [RGS]. En cas de changement important, l'AC fait appel à une expertise technique pour en contrôler l'impact.

G.12.2. Mécanisme et période d'information sur les amendements

Les nouvelles politiques de certification seront proposées au comité de pilotage qui en validera les modifications. Après validation, elles seront publiées dans le mois suivant et rentreront en application dès leur publication.

Les changements majeurs modifiant la relation avec le porteur feront l'objet d'un nouvel OID qui ne s'appliquera qu'aux nouveaux certificats.

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

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux 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.

En particulier, l'OID de la PC de l'AC doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC) intervient dans les exigences de la présente PC applicable à la famille de certificats considérée.

G.13. Dispositions concernant la résolution de conflits

Les Politiques de Certification des AC sont soumises au droit français.

Toute réclamation doit être adressée à l'inspection générale de l'ANFSI.

L'adresse courriel de l'ANFSI est : anfsi@gendarmerie.interieur.gouv.fr

G.14. Juridictions compétentes

Application de la législation et de la réglementation en vigueur sur le territoire français.

G.15. Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre I.1 ci-dessous.

L'AC est notamment soumise aux dispositions prévues par l'article 31 de la [LSQ] concernant la remise des clés privées des porteurs, si celles-ci sont séquestrées par l'AC.

G.16. Dispositions diverses

G.16.1. Accord global

Sans objet.

G.16.2. Transfert d'activités

Voir D.8.

G.16.3. Conséquences d'une clause non valide

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

G.16.4. Application et renonciation

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

G.17. Autres dispositions

L'AC n'a pas d'autres dispositions que celles exposées précédemment

G.17.1. 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.

H. Annexe 1 : Documents cités en référence

H.1. Réglementation

[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005
[LSQ]	Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

H.2. Documents techniques

[Cessation d'activité]	Procédure_cessation_activité
[ETSI EN 319 412]	EN 319 412 Certificate Profiles - 319 412-1 v1.1.1: Overview and common data structures - 319 412-2 v2.1.1: Certificate profile for certificates issued to natural persons - 319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons - 319 412-4 v1.1.1: Certificate profile for web site certificates issued to organisations - 319 412-5 v2.1.1: QCStatements
[GESTION_ROLES]	Rôles et responsabilités de l'IGC de l'ANFSI
[MESURES_IGC]	Mesures de sécurité communes aux AC de l'IGC de l'ANFSI
[PC_AC_RACINE]	Politique de certification de l'AC Racine de l'ANFSI
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[RGS_A1]	RGS - Fonction de sécurité « xxxx » - Version 3.0
[RGS_A4]	RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 3.0
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 2.03
[RGS]	Référentiel Général de Sécurité - Version 2.0

[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version d'août 2005 (complétée par les correctifs techniques Corrigendum 1 de janvier 2007et Corrigendum 2 de novembre 2008)

I. Annexe 1 : Documents cités en référence

I.1. Réglementation

[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005
[LSQ]	Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

I.2. Documents techniques

[RGS]	Référentiel Général de Sécurité - Version 2.0
[RGS_A1]	RGS - Fonction de sécurité « xxxx » - Version 3.0
[RGS_A4]	RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 3.0
[RGS_B_1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 2.03
[ETSI EN 319 412]	EN 319 412 Certificate Profiles - 319 412-1 v1.1.1: Overview and common data structures - 319 412-2 v2.1.1: Certificate profile for certificates issued to natural persons - 319 412-3 v1.1.1: Certificate profile for certificates issued to legal persons - 319 412-4 v1.1.1: Certificate profile for web site certificates issued to organisations - 319 412-5 v2.1.1: QCStatements
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version d'août 2005 (complétée par les correctifs techniques Corrigendum 1 de janvier 2007et Corrigendum 2 de novembre 2008)
[PC_AC_RACINE]	Politique de certification de l'AC Racine FSI

[GESTION_ROLES]	Rôles et responsabilités de l'IGC de l'ANFSI
[Cessation d'activité]	Procédure_cessation_activité