POLITIQUE DE CERTIFICATION – AC PERSONNES 4

OID du document :	1.2.250.1.120.4.2.1.1 1.2.250.1.120.4.3.1.1	**Nombre total de pages :**	88
Statut du document :	☐ Projet	☒ Version finale	

Rédaction

Nom	Fonction
Franck YVELIN	Département "Évaluation et projets de modernisation" du service de l'expertise et de la modernisation
Andréana JANNIN	Département "Évaluation et projets de modernisation" du service de l'expertise et de la modernisation

Validation

Nom	Fonction	Signature
Emmanuelle WACHENHEIM	Cheffe de service de l'expertise et de la modernisation	le 5/1/2021
Roland FRIEH	Fonctionnaire de sécurité des systèmes d'information – MJ	le 06/1/2021

Approbation

Nom	Fonction	Signature
Catherine PIGNON	Haut fonctionnaire défense et sécurité, Secrétaire général – MJ	le 07/01/2021

REVISION DOCUMENTAIRE

Historique

Date	Version	Commentaires
26/03/10	0.1	Création du document
13/04/10	0.2	Mise à jour du document
07/04/10	0.4	Version de travail diffusée au MJ
13/05/10	0.7	Version de travail diffusée au MJ
20/05/10	0.8	Version de travail diffusée au MJ
01/06/10	1.0	Version de référence
23/01/11	1.1	Prise en compte commentaires MJ/SG changement du nom de l'AC ordre judiciaire → AC personnes pour couvrir l'ensemble du ministère
15/10/11	1.6	Version pour relecture finale
25/11/11	2.0	Version pour signature
24/01/11	2.0.1	Prise en compte des fiches d'audit
12/06/11	2.1	Ajout de précisions sur les rôles de confiance
31/07/12	2.1.1	Prise en compte des évolutions 2011 et mise à jour des noms des intervenants
16/07/13	3.0	Mise à jour du document en cohérence par rapport aux évolutions apportées dans la DPC Mise à jour des modalités de changement de clés d'AC
25/06/16	4.0	Mise à jour du document en cohérence par rapport aux évolutions apportées dans la DPC Prise en compte des remarques audit interne, audit externe, analyse de risques
15/08/2018	5	Prise en compte des remarques des audits interne et externe Prise en compte des modifications de l'ASSCAP 4.9.3
19/12/2019	5.1	Prise en compte des remarques des audits interne et externe
20/01/2020	6	Mise à jour pour prendre en compte la mise en production de PGCA en remplacement de l'ASSCAP
05/10/2020	7.t	Version de travail pour intégrer la migration de responsabilités de l'ANTS vers l'IN G
06/12/2020	7.3	Prise en compte des écarts de l'audits externe 11067-1428

SOMMAIRE

1 INTRODUCTION

1.1 Généralités

Le ministère de la justice (MJ) met en place une Infrastructure de Gestion de Clés (IGC) afin de gérer les certificats de clés publiques de ses personnels.

La Politique de Certification (PC) définit un cadre d'utilisation de ces clés publiques. Dans le cadre de cette PC, les certificats mis à disposition des porteurs sont au nombre de deux :

- Un certificat à usage d'authentification au niveau (***) du RGS, et
- Un certificat à usage de signature électronique au niveau (***) du RGS, permettant une signature « présumée fiable » au sens de l'article 1367 du Code civil.

Un certificat de chiffrement est prévu ultérieurement, sans exigence RGS et hors du champ strict de cette PC.

Ces certificats d'utilisateurs sont émis par une Autorité de Certification (AC) dite « en ligne » appelée « AC Personnes ». L'AC Personnes 4 est placée hiérarchiquement sous une AC supérieure appelée « Autorité de certification Justice 2 ».

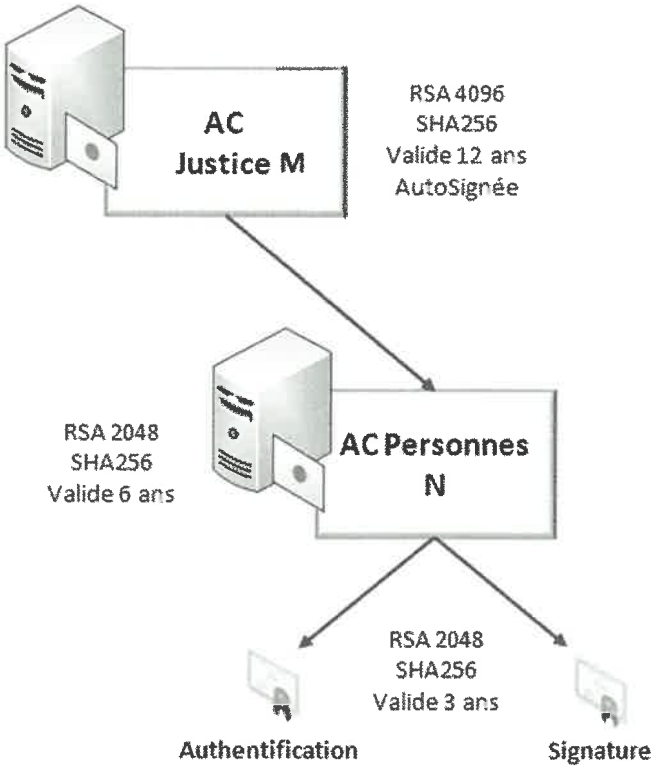


Figure 1 : Représentation IGC Justice[1]

L'AC Justice génère un certificat auto-signé qui peut être utilisé comme racine de confiance pour vérifier la validité d'un chemin de certification. Ce certificat a pour vocation d'être référencé dans la trusted list européenne (TSL)

[1] Se référer au § 3.1.1.

La présente politique de certification (PC) a pour objet de décrire la gestion du cycle de vie des certificats des porteurs et des bi-clés associées.

La présente Politique de Certification est élaborée conformément :

- au RFC 3647 « X.509 Public Key Infrastructure Certificate Policy Certification Practise Statement Framework » de l'Internet Engineering Task Force (IETF) ;
- au document « RGS - Politique de Certification Type - certificats électroniques de personne », version 3.0 du Référentiel Général de Sécurité v2.0 ;
- au règlement n°910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS ».

L'AC fournit au porteur un dispositif sécurisé de création de signature, qui contient les clés privées et les certificats. Ces dispositifs sécurisés sont qualifiés au niveau renforcé, selon le processus décrit dans le [RGS], et sont conformes aux exigences du chapitre XII.1 de la Politique de Certification Type « certificats électroniques de personne ».

L'utilisation d'un certificat à usage de signature électronique au niveau (***) du RGS, associé à l'usage d'un dispositif sécurisé de signature électronique et d'un logiciel permettant de générer des signatures sécurisées permet d'obtenir une signature électronique « présumée fiable » jusqu'à preuve du contraire, au sens de l'article 1367 du code civil.

De manière à faciliter l'identification des différences entre les certificats destinés à l'authentification et ceux destinés à la signature, les exigences spécifiques à un certificat sont encadrées, le titre du cadre précisant le type de certificat auquel l'exigence s'applique. Les exigences qui ne sont pas encadrées s'appliquent de manière identique pour les deux types de certificats.

La finalité de ces présentes PC et des DPC associées est d'obtenir la qualification RGS*** ainsi que eIDAS au niveau « élevé » afin de pouvoir avoir l'inscription à la TSL (liste des certificats de confiance européenne).

Nota : La gestion du certificat de l'AC Personnes et de la bi-clé associée est décrite dans la PC AC Racine Justice.

1.2 Nom du document et identification

La présente PC appelée : « PC Personnes 4 » est la propriété du ministère de la Justice.

Ce document couvre deux politiques de certification :

- La politique de certification pour les certificats d'authentification de l'AC Personnes 4, identifiée par le numéro d'identifiant d'objet (OID) 1.2.250.1.120.4.2.1.1;
- La politique de certification pour les certificats de signature de l'AC Personnes 4, identifiée par le numéro d'identifiant d'objet (OID) 1.2.250.1.120.4.3.1.1.

Des éléments plus explicites comme le nom, le numéro de version, la date de mise à jour, permettent d'identifier la présente PC, néanmoins les seuls identifiants de la version applicable des PC sont les OID.

La finalité de ces présentes PC et des DPC associées est d'obtenir la qualification RGS*** ainsi que eIDAS au niveau « élevé » afin de pouvoir avoir l'inscription à la TSL (liste des certificats de confiance européenne).

Nota : La gestion du certificat de l'AC Personnes et de la bi-clé associée est décrite dans la PC AC Racine Justice.

1.3 Définitions et Acronymes

1.3.1 Acronymes

AA	Autorité Administrative
AC	Autorité de Certification
ACR	Autorité de Certification Racine
AE	Autorité d'Enregistrement
AEC	Autorité d'Enregistrement Centrale
AED	Autorité d'Enregistrement Déléguée
AEx	Toute autorité d'enregistrement (regroupe AE, AEC, AED et OC dans certains cas)
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANTS	Agence Nationale des Titres Sécurisés
ARL ou LAR	Authority Revocation List ou Liste des Autorités Révoquées
CA	Cour d'Appel
CGU	Conditions Générales d'Utilisation
COFRAC	Comité français d'accréditation
CPS	Centre de Personnalisation des Supports
CRL ou LCR	Certificate Revocation List (Liste des Certificats Révoqués)
DAP	Direction de l'administration pénitentiaire
DICOM	Délégation à l'information et à la communication
DITP	Direction Interministérielle de la Transformation Publique
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
DPJJ	Direction de la Protection judiciaire de la Jeunesse
DSJ	Direction des Services Judiciaires
ENAP	École Nationale de l'Administration Pénitentiaire
ENG	École Nationale des Greffes
ENM	École Nationale de la Magistrature
ENPJJ	École Nationale de Protection Judiciaire de la Jeunesse
EPELFI	Établissement Public d'Exploitation du Livre Foncier Informatisé
FSSI	Fonctionnaire de la Sécurité des Systèmes d'Information
HFDS	Haut Fonctionnaire de Défense et de Sécurité

HSM	Hardware Security Module ou RCM
IETF	Internet Engineering Task Force (normes européennes)
IGC	Infrastructure de Gestion de Clés
INGroupe	Imprimerie Nationale Groupe
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LAR ou ARL	Liste des Autorités Révoquées ou (Authority Revocation List)
LCR ou CRL	Liste des Certificats Révoqués ou (Certificate Revocation List)
MJ	Ministère de la justice
NTP	Network Time Protocol
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier (norme de nommage des documents de sécurité)
OSC	Opérateur de Service de Certification
PC	Politique de certification
PMDS	Politique Ministérielle de Défense et Sécurité
PSCE	Prestataire de Services de Certification Électronique
PSCO	Prestataire de Services de Confiance
RCM	Ressource Cryptographique Matérielle ou HSM
RCSSI	Responsable Central de la Sécurité des Systèmes d'information
RFID	Radio Frequency IDentification
RGRH	Responsable de gestion des ressources humaines
RGS	Règlement Général de Sécurité
RH	Ressources Humaines
RSA	Rivest Shamir Adleman (algorithme de chiffrement)
RSSI	Responsable de la Sécurité des Systèmes d'information
SAR	Service administratif régional
SG	Secrétariat Général
SHA	Secure Hash Algorithm
SNum	Service du Numérique (ex. SSIC)
SP	Service de Publication
SPIP	Services Pénitentiaire d'Insertion et de Probation

SSIC	Service des systèmes d'Information et de communications (SNum)
SSL	Secure Socket Layer
TJ	Tribunal Judiciaire
TProx	Tribunal de Proximité
UC	Utilisateur de Certificats
URL	Uniform Resource Locator

1.3.2 Définitions

Autorité Administrative : administration de l'État, collectivité territoriale, établissement public à caractère administratif, organisme gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L. 223-16 et L. 351-21 du code du travail ou organisme chargé de la gestion d'un service public administratif [Ordonnance].

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) : entité responsable de garantir le lien (infalsifiable et univoque) entre l'identifiant d'un porteur et une bi-clé cryptographique pour un usage donné. Cette garantie est apportée par des certificats de clé publique qui sont signés par la clé privée de l'AC.
Dans cette PC l'AC est le ministère de la Justice

Autorité d'Enregistrement (AE) : entité responsable de la délivrance des supports de clés et des certificats aux porteurs lors d'un face-à-face. L'AE effectue en outre, les opérations de demandes de certificat à la vue des données fournies par différents systèmes d'information. L'AE peut intervenir pour la révocation d'un certificat.
Dans cette PC l'AC est un personnel du ministère de la Justice

Critères Communs : ensemble d'exigences de sécurité qui sont décrites suivant un formalisme internationalement reconnu. Les produits et logiciels sont évalués par un laboratoire afin de s'assurer qu'ils possèdent des mécanismes qui permettent de mettent en œuvre les exigences de sécurité sélectionnées pour le produit ou le logiciel évalué.

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

Certificat électronique : fichier électronique attestant qu'une clé publique appartient à la personne physique ou morale identifiée dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identifiant de la personne physique ou morale et la bi-clé. Le certificat est valide uniquement s'il est utilisé pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente PC, le terme "certificat électronique" désigne un certificat délivré à une personne physique et portant sur une bi-clé d'authentification ou de signature, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, ...).

Certificat d'AC : certificat pour une AC émis par une autre AC. [ISO/IEC 9594-8 ; ITU-T X.509].

Certificat d'AC 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 plusieurs certificats nécessaires pour valider un certificat vis-à-vis d'un certificat d'AC auto-signé.

Clé privée : clé de la bi-clé asymétrique d'une entité qui ne doit être conservée pour l'la connaissance et l'usage unique du porteur [ISO/IEC 9798-1].

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

Composante : ensemble de composants physiques (des ordinateurs, des équipements cryptographiques logiciels ou matériel), des procédures humaines, de logiciels, humains, infrastructures, etc. jouant un rôle dans la mise en œuvre d'au moins une fonction de l'IGC.

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 cette clé privée.

Confidentialité : propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes, des entités ou des processus non autorisés.

Déclaration des Pratiques de Certification (DPC) : document qui identifie et référence les pratiques (organisation, procédures opérationnelles, moyens techniques et humains, etc.) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Demande de certificat : message transmis par l'AE à l'AC pour obtenir l'émission d'un certificat d'AC.

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

Dispositif de création de signature : Un dispositif de création de signature électronique est un matériel ou logiciel destiné à mettre en application les données de création de signature électronique.

Données d'activation : 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 deux 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] ;

Infrastructure de gestion de clés (IGC) : ensemble de composantes dédiées à la gestion de clés cryptographiques utilisés par des services de confiance. C'est l'infrastructure requise pour produire, distribuer, gérer des clés publiques et privées, des certificats, des Listes de Certificats Révoqués et des Listes des Autorités Révoquées.

Intégrité : fait référence à l'exactitude et la non-altération de l'information, de la source de l'information, et au fonctionnement du système qui la traite. Désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation. L'intégrité des données comprend quatre éléments : l'intégralité, la précision, l'exactitude/authenticité et la validité.

Interopérabilité : implique que le matériel et les procédures utilisés par deux entités ou plus sont compatibles ; et qu'en conséquence il leur est possible d'entreprendre des activités communes ou associées.

Liste de Certificats Révoqués (LCR) : liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides. 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.

Modules cryptographiques : ensemble de composants logiciels et matériels utilisés pour 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), utilisé pour conserver et mettre en œuvre la clé privée AC.

Période de validité d'un certificat : période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 2459].

PKCS #10 : (Public-Key Cryptography Standard #10) mis au point par RSA Security Inc., qui définit une structure pour une Requête de Signature de Certificat (en anglais : Certificate Signing Request: CSR).

Plan de reprise d'activité (PRA) : plan défini 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. Le PRA du ministère de la justice est défini par une AC, et le délai est défini dans l'ensemble PC/DPC.

Point de distribution de LCR *:* 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, identifié par un nom (OID), définissant (a) les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes (b) les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

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 : personne physique travaillant pour le ministère de la justice (interne ou externe), qui dispose d'une carte à microcircuit comportant deux couples clé privée/certificat, l'un à usage d'authentification et l'autre à usage de signature électronique. Un porteur possède nécessairement un dossier administratif (interne) ou un dossier d'habilitation (externe).

Porteur de secret : personne 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.

Prestataire de services de confiance (PSCO) : personne offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique entre les usagers et les autorités administratives et entre les autorités administratives].

Prestataire de services de certification électronique (PSCE) : un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE est un type de PSCO particulier.

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

Qualification d'un prestataire de services de certification électronique : le [Décret RGS] décrit la procédure de qualification des PSCO. La qualification d'un PSCE est un acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC Type pour un niveau de sécurité donné et correspondant au service rendu par les certificats.

Qualification d'un produit de sécurité : acte par lequel l'ANS (au niveau français l'ANSSI) atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS]. La procédure de qualification des produits de sécurité est décrite dans le [Décret RGS].

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

Unité d'Horodatage : Ensemble de matériel et de logiciel en charge de la création de contremarques de temps caractérisé par un identifiant de l'unité d'horodatage accordé par une AC, et une clé unique de signature de contremarques de temps.

Utilisateur de Certificats (UC) : application, personne physique ou morale, organisme administratif ou système informatique matériel qui utilise un certificat de porteur conformément à la politique de sécurité du ministère de la justice dans le cadre d'une authentification ou d'une signature électronique.

Validation d'un certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de certification (AC) et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC et la vérification de la signature électronique de l'ensemble des AC contenues dans le chemin de certification. Elle inclue également la validation du certificat de l'ensemble des AC du chemin de certification. La validation d'un certificat électronique nécessite au préalable de choisir le certificat qui sera pris comme référence (dans le cas du ministère de la justice il s'agit d'un certificat auto-signé).

1.4 Entités intervenant dans l'IGC

L'AC s'appuie sur les composantes et sous-composantes suivantes :

- Service d'enregistrement : Ce service, aussi appelé « Autorité d'Enregistrement » (AE), est assuré par le personnel du ministère de la justice qui utilise, en amont, un annuaire référençant l'ensemble des informations relatives à l'identité des personnels (interne ou externe) du MJ. Les personnes affectées à ce service génèrent des demandes de certificat en se connectant sur un portail dédié.
- Service de génération des certificats : dans le cadre du ministère de la justice, ce service est assuré par un Prestataire de Services de Certification Électronique (PSCE) qui génère les certificats électroniques des porteurs à partir des informations transmises par le service d'enregistrement qui ont été préalablement vérifiées et validées par ledit service.
- Service de génération des éléments secrets du porteur : Ce service permet de personnaliser électriquement (génération de bi-clés) les supports de bi-clé(s) cryptographique(s) en utilisant les données fournies par le service de génération de certificats. Ce service permet également de générer et d'insérer une donnée d'activation dans les supports de clés privées. Cette donnée d'activation consiste en un code d'activation qui permettra au porteur de créer deux codes personnels, appelés « Personal Identification Number » (PIN) afin de protéger/activer chacune des deux clés privées cryptographiques. Le code d'activation et les supports de clés privées sont communiqués aux porteurs en utilisant deux chemins différents. Les données d'activation sont communiquées au porteur au moyen d'un courrier postal sécurisé (enveloppe scellée opaque).
- Service de remise au porteur : Ce service va remettre au porteur une carte à puce (également appelé un support » comportant deux certificats, un d'authentification et un de signature. Au ministère de la justice, la remise de la carte est effectuée par une autorité d'enregistrement. Les données d'activation sont adressées au porteur au moyen d'un courrier sécurisé.
- Service de publication : Ce service met à disposition sur un Intranet et sur Internet les informations nécessaires à l'utilisation des certificats émis par l'AC (conditions générales, politiques de certification, certificats d'AC, ...),et tout autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors information d'état des certificats ;
- Service de gestion des révocations : Ce service traite de la prise en compte des demandes de révocation des certificats des porteurs Les résultats des traitements sont diffusés via le service d'information sur l'état des certificats ;

- Service d'information sur l'état des certificats : Cette fonction fournit des informations sur l'état des certificats. Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers sous la forme de Listes de Certificats Révoqués (LCR) et d'OCSP.
- Service de journalisation : Ce service utilise les données de l'ensemble des composantes techniques de l'IGC. Pour le ministère de la justice, il est assuré par le PSCE II permet de collecter l'ensemble des données utilisées et/ou générées dans le cadre de la mise en œuvre des services d'IGC afin d'obtenir des traces d'audits consultables. La DPC apporte plus de précisions sur cet aspect.
- Service d'exploitation des journaux : ce service permet de détecter toute tentative de violation de l'intégrité des données, par le biais d'une analyse des journaux pour détecter les anomalies et falsifications constatées.
- Service d'audit : Ce service est assuré par le FSSI du MJ, et consiste à organiser, coordonner et surveiller les prestations d'audit ayant pour but de vérifier que les procédures mises en place par le ministère de la justice couvrent les exigences des référentiels de sécurité visés.
- Service d'assistance aux utilisateurs : Ce service est assuré par le ministère de la justice, et accompagne les utilisateurs durant tout le cycle de vie de leur carte.

La présente PC définit les exigences de sécurité pour tous les services décrits ci-dessus afin de délivrer des certificats aux porteurs. La Déclaration des Pratiques de Certification (DPC) apporte des détails sur les pratiques de l'IGC dans cette perspective.

Les composantes de l'IGC mettent en œuvre leurs services conformément à la présente PC et la DPC associée.

1.4.1 Ministère de la justice (AC – AE – SP)

1.4.1.1 Autorité de Certification (AC)

Le ministère de la justice a le rôle d'Autorité de Certification.

L'AC 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 (CGU) et de la DPC associée. L'AC valide le référentiel de sécurité. Elle autorise et valide la création et l'utilisation des composantes des AC. Elle suit les audits et/ou contrôle de conformités effectués sur les composantes de l'IGC, décide des actions à mener et veille à leur mise en application.

RGS : « L'AC doit mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse ».

L'AC a pour responsabilité de garantir le lien (infalsifiable et univoque) entre l'identifiant d'un porteur et une bi-clé cryptographique pour un usage donné. Cette garantie est apportée par des certificats de clé publique qui sont signés par la clé privée de l'AC.

En tant qu'autorité, l'AC :

- Définit et valide l'organisation de l'IGC ;
- Définit et contrôle la présente PC, les CGU et la DPC associée ;
- Contrôle la mise en œuvre de la DPC ;
- Arbitre les litiges.

L'AC peut déléguer tout ou partie de ces fonctions.

Dans le cadre de l'AC Personnes 4, elle délègue ses services de la façon suivante :

- Au Service du Numérique (SNum) du ministère de la justice : la tenue d'un annuaire où figurent tous leurs agents de l'État et le personnel extérieur sous contrat avec l'État ;
- Au secrétariat général (SG) et aux directions (direction des services judiciaires (DSJ), direction de l'administration pénitentiaire (DAP), etc.) du ministère de la justice, l'habilitation des agents de l'État du ministère de la justice ayant un rôle à jouer dans le cadre de l'enregistrement des utilisateurs au niveau AE, AEC, AED, OC.
- À l'ANTS au titre de Prestataire de Service de Certification Électronique (PSCE) : la génération des certificats et leur renouvellement, la gestion des révocations et les systèmes informatiques utilisés par les AE, AEC ; AED pour l'enregistrement.
- Au CPS : la génération des éléments secrets du porteur ainsi que des données d'activation temporaires, l'acheminent des cartes et des codes d'activation.
- Au Service du Numérique (SNum) du ministère de la justice : la publication des PC, CGU et des certificats d'AC ainsi que l'information sur l'état des certificats.

1.4.1.2 Autorité d'Enregistrement (AE)

Le ministère de la justice a le rôle d'Autorité d'Enregistrement.

L'AE est responsable de la délivrance des supports de clés et des certificats aux porteurs lors d'un face-à-face.

L'AE effectue en outre, les opérations de demandes de certificat à la vue des données fournies par différents systèmes d'information. L'AE peut intervenir pour la révocation d'un certificat octroyé à toute personne située dans la hiérarchie de l'AE (AEC, AED ou OC).

L'Autorité d'Enregistrement du ministère de la justice est structurée sur la base d'un système hiérarchique à quatre niveaux.

- Le niveau inférieur est celui des Opérateurs de Certification (OC). Ce sont eux qui ont un contact en face-à-face avec les porteurs lors de la remise du support cryptographique. Les Opérateurs de Certification (OC) peuvent être désignés par des personnes ayant le rôle d'Autorité d'Enregistrement Déléguée (AED) ou d'Autorité d'Enregistrement Centrale (AEC).
- Les personnes ayant le rôle d'Autorité d'Enregistrement Déléguée (AED) sont désignées par des personnes ayant le rôle d'Autorité d'Enregistrement Centrale (AEC). Les personnes ayant le rôle d'AED assurent la validation des demandes de certificat initiées par les Opérateurs de Certification (OC). Chacune des personnes ayant le rôle d'AED peut désigner d'autres AED pour l'assister dans son travail.
- Les personnes ayant le rôle le rôle d'Autorité d'Enregistrement Centrale (AEC) sont désignées par des personnes ayant le rôle d'Autorité d'Enregistrement (AE). L'AEC est chargée de désigner les AED (ou les OC) et d'assurer le suivi de ces acteurs. Une AEC ne peut pas nommer une AEC *alter ego*. Si l'AEC désire avoir une autre AEC alter ego, il doit en faire la demande à l'AE.
- Le rôle d'Autorité d'Enregistrement (AE) est tenu par le Secrétaire Général. Les personnes ayant le rôle d'Autorité d'Enregistrement (AE) sont initialement désignées, sur demande du Secrétariat Général du ministère de la justice, par l'administrateur technique de l'annuaire du MJ.

Nota : Dans la suite du document, les tâches menées par les AED ou les OC peuvent être effectuées, par défaut, par toute AE ou AEC. Aucune AEx (AE, AEC, AED) ne peut faire ni remise ni commande (création ou remplacement) pour elle-même.

Les personnes ayant le rôle d'Autorité d'Enregistrement (AE), d'Autorité d'Enregistrement Centrale (AEC), d'Autorité d'Enregistrement Déléguée (AED) ou d'Opérateur de Certification (OC) sont dotées de certificats de clé publiques et de supports de clés (cartes agent).

Le SNum du ministère de la justice tient à jour un annuaire où figurent tous les agents du MJ ayant un rôle à jouer dans le cadre de l'enregistrement des utilisateurs. Chaque agent dispose d'un profil qui définit le périmètre des actions qu'il peut effectuer dans le cadre de l'un des rôles décrits ci-dessus. Ce profil permet de gérer leur site de rattachement et leurs habilitations. Le détail des habilitations figure dans la DPC.

L'enregistrement utilise des informations externes à l'IGC, disponibles sur des systèmes d'information existants. Ces systèmes d'information sont de confiance (informations détenues par les services de l'État, fichier des ressources humaines d'un organisme, etc.).

Pour l'AC Personnes 4, l'AE est organisée selon le schéma suivant :

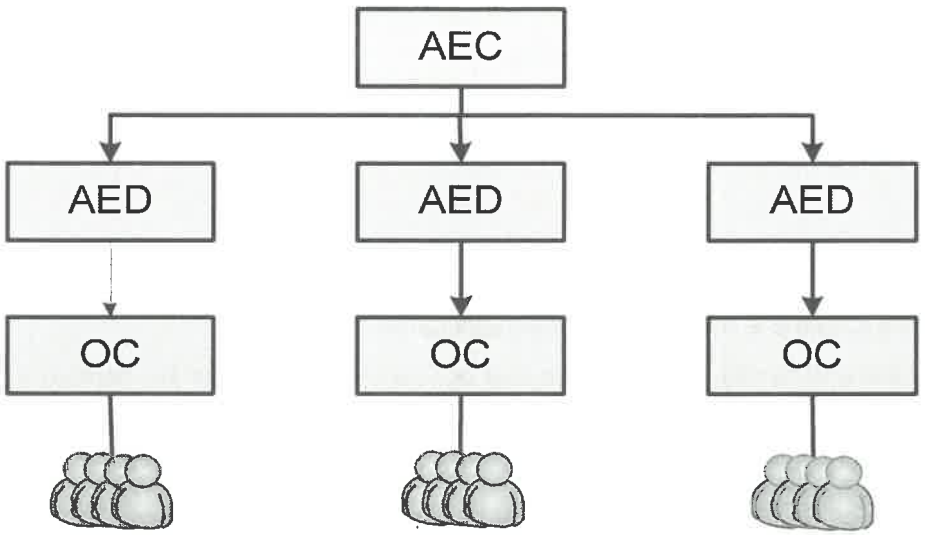


Figure 2 : Représentation générale de la chaîne de confiance

Nota : L'organisation des rôles de confiance de la présente PC est détaillée dans la DPC correspondante.

1.4.1.3 Autorité d'Enregistrement Centralisée (AEC)

Les personnes ayant le rôle d'AEC sont désignées par l'AE. Une fois désignées, elles sont en mesure d'obtenir un certificat et un support de clés. Lors de leur désignation, il leur est attribué un profil d'habilitation qui limite les juridictions situées dans leur domaine de responsabilité.
Dans cette PC l'AEC est un personnel du ministère de la Justice

1.4.1.4 Autorité d'Enregistrement Déléguée (AED)

Les personnes ayant le rôle d'AED sont désignées par l'AEC ou mandatés par l'AED. Une fois désignées, elles sont en mesure d'obtenir un certificat et un support de clés. Lors de leur désignation, il leur est attribué un profil d'habilitation qui limite les juridictions et/ou les sites situées dans leur domaine de responsabilité.
Dans cette PC l'AED est un personnel du ministère de la Justice.

1.4.1.5 Opérateur de Certification (OC)

Les opérateurs de certification (OC) sont désignés par une AED ou une AEC. Une fois désignés, ils sont en mesure d'obtenir un certificat et un support de clés. Lors de leur désignation, il leur est attribué un profil d'habilitation qui limite les juridictions et/ou les sites situés dans leur domaine de responsabilité.

L'OC ont un rôle de mandataire. À ce titre, il effectue les opérations de demandes de certificat, à partir des données fournies par les différents systèmes d'information, qui doivent ensuite être validées par une personne ayant le rôle d'AED. Une fois validées les demandes sont transmises à l'AC.

La remise des cartes est effectuée par l'OC qui s'assure de l'identité du porteur au cours d'un face-à-face. L'OC est aussi en mesure d'effectuer des demandes de révocation pour le compte d'un porteur.

Pour les dossiers de demande, l'OC remonte les justificatifs au niveau de l'AED dont il dépend. L'OC ne peut pas valider un dossier de demande.
Dans cette PC l'OC est un personnel du ministère de la Justice

1.4.2 Service de Publication (SP)

Le ministère de la justice a le rôle de Service de Publication.

Le SP est une entité qui met à disposition des utilisateurs de certificat (UC) au moyen d'un Intranet et de l'Internet les informations nécessaires à l'utilisation des certificats émis par l'AC Personnes (conditions générales, politiques de certification publiées par l'AC, certificats d'AC Personnes, LCR, ...).

Ce service met aussi à disposition des utilisateurs de certificat (UC) les informations de validité des certificats issues des traitements du service de gestion des révocations (LCR, avis d'information, ...). Le SP s'appuie sur les moyens du ministère de la justice et du PSCE afin de réaliser ces services.

1.4.3 Autres participants

1.4.3.1 Management de l'IGC

Le Garde des sceaux (GDS) a nommé le département de l'évaluation et projet de modernisation (DEPM) responsable des services d'IGC et lui a donné autorité sur les autres participants.

1.4.3.2 Centre de Personnalisation des Supports (CPS)

L'Imprimerie Nationale Groupe (INGroupe) assure le rôle de Centre de Personnalisation des Supports pour l'AC.

Le CPS dispose d'une plate-forme pour mettre en œuvre le service de personnalisation et de gestion des supports de bi-clé et la fourniture aux porteurs d'un code d'activation. Le CPS met en œuvre un plan de continuité d'activité sur lequel s'appuie l'AC pour la continuité des services d'IGC.

Il dispose en outre d'un service de journalisation et d'audit conformément à la présente PC et à la DPC applicable.

Nota : La distinction entre le CPS et PSCE est précisée dans la DPC applicable.

1.4.4 Prestataire de Services de Certification Électronique (PSCE)

L'AC délègue à l'Agence Nationale des Titres Sécurisés (ANTS) conjointement avec l'INGroupe, le rôle de Prestataire de Services de Certification Électronique (PSCE).

Le PSCE assure des prestations techniques, en particulier des opérations cryptographiques, nécessaires au processus de certification, conformément à la présente PC et à la DPC associée. Le PSCE est techniquement dépositaire de la clé privée de l'ACR 2 utilisée pour la signature des certificats des porteurs. Sa responsabilité se limite au respect des procédures que l'AC définit afin de répondre aux exigences de la présente PC.

Le PSCE possède un plan de continuité d'activité sur lequel s'appuie l'AC pour la continuité des services d'IGC. Une analyse de risques et ce plan de continuité couvrent le seul périmètre de le PSCE en tant qu'hébergeur de moyens qui permettent à l'AC de mettre en œuvre ses services d'IGC.

Le PSCE met en place un service de journalisation et d'audit pour les composantes techniques qu'il opère.

Dans la présente PC, le rôle et les obligations du PSCE ne sont pas toujours distingués de ceux de l'AC. Cette distinction est précisée dans la DPC.

1.4.5 Porteur de certificats

Un porteur de certificats est une personne physique qui travaille pour le ministère de la justice. Ces personnes peuvent être :

- Interne au ministère de la justice en tant qu'agent de l'État ;
- Externe au ministère de la justice en tant que personnel d'un autre ministère ou prestataire d'une société.

Nota : Tout porteur possède un dossier administratif (Pour les internes au MJ) ou un dossier d'habilitation (Pour les externes au MJ). Des précisions sont apportées dans la DPC rattachée à la présente PC.

Un porteur de certificat dispose d'une carte à microcircuit qui comporte deux couples clé privée/certificat, l'un à usage d'authentification et l'autre à usage de signature électronique :

- « Certificat d'Authentification Personnes » : certificat généré par l'AC Personnes 4 dont les conditions de recevabilité sont décrites dans la Politique de Certification AC Personnes 4 ;
- « Certificat de Signature Personnes » : certificat généré par l'AC Personnes 4 dont les conditions de recevabilité sont décrites dans la Politique de Certification AC Personnes 4.

Chaque couple est activable / déverrouillable par l'usage d'un code PIN (Personal Identification Number) dédié.

Le porteur respecte les conditions qui lui incombent définies dans la présente PC.

1.4.6 Utilisateur de Certificats (UC)

L'UC est une application, une personne physique ou morale, un organisme administratif ou un système informatique matériel qui utilise un certificat de porteur conformément à la politique de sécurité du ministère de la justice, dans le cadre d'une authentification ou d'une signature électronique.

Dans le cadre de la présente PC, un UC, pour s'assurer de la validité d'un certificat d'un porteur, doit construire et valider un chemin de certification depuis le certificat du porteur jusqu'à la racine de confiance auto-signée qui est celle du MJ, et doit en outre contrôler les informations de révocation pour chaque élément du chemin de certification (LCR pour le certificat du porteur et LAR pour les certificats d'AC).

1.5 Usage des certificats

1.5.1 Utilisation appropriée des certificats

1.5.2 Certificats de porteur

Le porteur dispose de deux certificats :

- Le certificat d'authentification sert à authentifier le porteur, typiquement lors d'une authentification du type « client SSL » ;
- Le certificat de signature sert signer un document à l'aide d'une signature électronique sécurisée pour en garantir l'origine.

Ces certificats ne sont utilisables que dans le cadre des activités professionnelles, uniquement sur des postes de travail du ministère de la justice et uniquement sur les applications professionnelles supportant les cartes à microcircuit qui sont mises à disposition des porteurs par le MJ.

Ces certificats sont utilisés par des applications pour lesquelles les besoins de sécurité sont très forts eu égard aux risques très élevés qui les menacent.

Les certificats ne peuvent être utilisés que conformément aux lois en vigueur et à la règlementation applicable à la profession.

1.5.3 Certificat de l'AC

La bi-clé de l'AC sert à signer des certificats de porteurs et les Listes de Certificats Révoqués (LCR).

Pour cette AC, les chaînes de certificats issues de l'IGC Personnes possèdent la structure suivante :

- Certificat d'ACR 2 (« AC Justice 2 ») : certificat électronique auto-signé d'une AC racine ;
- Certificat de l'AC « Personnes 4 » : certificat électronique délivré à l'AC Personnes par l'AC Justice 2 ;
- Certificat de porteur : certificat électronique délivré à un porteur par l'AC Personnes 4.

1.5.4 Certificats de test

Pour des besoins de tests ou de vérification de plans (PRA, PCA, etc.) des cartes de test peuvent être créées avec des identités affichant clairement le mot « TEST ». Ainsi les anciennes identités avaient pour noms : TESTSGxxxx. (Où xxxx est un n° d'ordre unique.)

Depuis la réorganisation du SG les noms sont devenus « TEST-NNNxxx » où « NNN » représente l'abréviation ou l'acronyme du projet (Par exemple CAJ pour Carte agent justice) et où xxx est un n° d'ordre unique.

Ces cartes sont systématiquement créées dans l'environnement TEST1 qui a été spécialement crée à cet effet dans le Système de Référence Justice (SRJ).

1.5.5 Utilisation interdite des certificats

Les utilisations de certificats émis par l'AC Personnes 4 à d'autres fins que celles prévues au paragraphe ci-dessus et par la présente PC ne sont pas autorisées. Le détail des utilisations du certificat de chiffrement sera précisé dans la mise à jour de cette PC lors de la mise en œuvre de ce certificat.

Dans le cas où cette interdiction serait outrepassée, l'AC ne peut être en aucun cas être tenue pour responsable d'une utilisation des certificats qu'elle émet.

1.6 Gestion de la PC

1.6.1 Entité gérant la PC

Le ministère de la justice est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC. À cette fin, il met en œuvre et coordonne une organisation dédiée, qui statue à échéances régulières, sur la nécessité d'apporter des modifications à la PC.

1.6.2 Point de contact

La personne responsable est le Haut Fonctionnaire de Défense et de Sécurité (HFDS, Secrétaire Général du ministère de la justice) joignable au 01 44 77 60 60.

1.6.3 Entité déterminant la conformité d'un DPC avec cette PC

Le ministère de la justice procède à des analyses/contrôles de conformité et/ou des audits qui aboutissent à l'autorisation ou non pour l'AC Personnes 4 d'émettre des certificats.

1.6.4 Procédures d'approbation de la conformité de la DPC

Les personnes ou les sociétés habilitées à déterminer la conformité de la DPC avec la présente PC sont choisies par le ministère de la justice sur la base, en particulier, de leur capacité à réaliser des évaluations de sécurité. Ces personnes ou ces sociétés sont des personnes indépendantes du MJ.

Le ministère de la justice s'assure de la conformité de la DPC avec la présente PC pour la mise en œuvre opérationnelle des composantes de l'IGC Personnes. Toute demande de mise à jour de la DPC doit suivre le processus d'approbation mis en place.

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1 Entités chargées de la mise à disposition des informations

Le service de publication est le service en charge de la publication du présent document et des autres documents ou informations dont la publication est nécessaire afin d'assurer la bonne utilisation des certificats délivrés au titre de la présente PC.

Le SP est chargé de mettre à disposition les informations, citées ci-après, au niveau de l'Intranet du ministère de la justice et au niveau d'internet. La DPC précise les différentes interfaces du SP en fonction des informations à publier.

2.2 Informations devant être publiées

L'AC s'assure que les termes et conditions applicables à l'usage des certificats qu'elle délivre sont mis à la disposition des porteurs et des UC.

Les informations sont accessibles depuis le site suivant : http://www.justice.gouv.fr/igc/ants

L'AC, via le SP, rend disponibles les informations les informations suivantes :

- La présente PC ;
- La PC de l'AC Racine 2 ;
- Les certificats de l'AC Racine 2 et AC Personnes 4 ;
- Les Conditions Générales d'Utilisation (CGU) des certificats ;
- Les LAR et les LCR[2] ;
- Les formulaires d'acceptation d'un rôle de confiance ;
- L'empreinte SHA-256 du certificat racine (*SHA-256 avant 9 juin 2016 et SHA-512 après.*).

2.3 Délais et fréquences de publication

La présente PC et les documentations relatives aux demandes de certificat et de révocation sont accessibles 24h/24 7j/7.

Le certificat de l'AC Racine 2 à laquelle est rattachée l'AC Personnes 4 et le certificat de l'AC personnes 4 sont publiés préalablement à toute diffusion de certificats porteurs ou de LCR avec une disponibilité de 24h/24 7j/7.

Le certificat de l'AC Personnes 4 est renouvelé et publié à la moitié de la durée de vie, soit tous les trois ans.

Les LCR sont publiées toutes les 24h. Chaque nouvelle version des LCR est mise à disposition des utilisateurs dans un délai de 30 minutes qui suivent leur création.

Nota : La Politique de Certification, la Déclaration des Pratiques de Certification et les conditions générales d'utilisation sont actualisées en tant que de besoin, après la validation du ministère de la justice. À terme, la révision semestrielle est ciblée.

2.4 Contrôle d'accès aux informations publiées

Le SP s'assure que les informations sont disponibles, protégées en intégrité contre les modifications non autorisées et sont accessibles en lecture uniquement pour les porteurs et les utilisateurs de certificats (UC).

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

L'AC s'assure que toute information conservée dans une base documentaire de son IGC et dont la diffusion est publique ou la modification n'est pas autorisée est protégée.

Nota : La DPC apporte des précisions concernant l'accès par authentification forte aux systèmes de publication.

[2] Chaque certificat comporte l'adresse du point de distribution de la LCR le concernant.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Les identifiants utilisés dans un certificat sont conformes à la norme X.501. Dans chaque certificat X 509, le fournisseur (Issuer) et le porteur (Subject) sont identifiés par un nom distinctif, en anglais « Distinguished Name » (DN).

3.1.2 Certificat d'AC

L'identifiant inclus dans le certificat de l'AC est conforme aux exigences de la PC AC Racine 2 du ministère de la justice. L'identité de l'AC dans le certificat est la suivante :

Champ de base	Valeur
Issuer DN	C = FR
	O = Ministère de la Justice
	OU = 0002 <espace > 110010014
	CN = Autorité de certification Justice 2
Subject DN	C = FR
	O = Ministère de la Justice
	OU = 0002 <espace > 110010014
	CN = Autorité de certification personnes 4

Nota : à compter du premier renouvellement de clés de l'AC Personnes, les changements de la valeur du « CN » dans le champ « Subject DN » sont les suivants :

- Pour la première clé cette valeur est « Autorité de certification personnes 4 » ;
- Pour les clés suivantes, cette valeur est « Autorité de Certification Personnes N » où N est un entier incrémenté par pas de 1 à chaque changement de clé d'AC, à partir de la valeur « 5 » pour le premier changement (le deuxième jeu de clés).

3.1.3 Certificat de porteur

L'identifiant unique du CN permet de faire le lien entre le certificat attribué au porteur et les données du porteur contenues dans l'annuaire qui a été utilisé à l'origine pour créer le porteur.

L'identité du porteur dans le certificat du porteur est la suivante :

Champ de base	Valeur
Issuer DN	C = FR O = Ministère de la Justice OU = 0002 <espace > 110010014 OU = POUR QUALIFICATION UNIQUEMENT* CN = Autorité de certification personnes 4
Subject DN	C = FR O = Ministère de la Justice OU = 0002 <espace > 110010014 OU = POUR QUALIFICATION UNIQUEMENT* CN = premier prénom de l'état civil <espace> nom de l'état civil <espace> identifiant unique.

* A AJOUTER SI ENVIRONNEMENT DE QUALIFICATION

Nota : à compter du premier renouvellement de l'AC Personnes 4, la valeur « CN » du champ « Issuer » des certificats porteurs prend la valeur « CN » du champ « Subject » du certificat d'AC ayant servi à les signer.

3.1.4 Nécessité d'utilisation de noms explicites

Les identités incluses dans les certificats émis conformément à la présente PC sont toujours explicites et nominatives. Le nom de famille ou le nom d'usage et prénoms du porteur sont ceux qui correspondent à l'identité du porteur (personne) à l'état civil conformément au contenu de l'annuaire du ministère de la justice.

Nota : L'identité des porteurs (personnes) à l'état civil peut être consultée par l'autorité d'enregistrement ou les OC à partir du dossier administratif ou du dossier d'habilitation. Des précisions seront apportées dans la DPC rattachée à la présente PC.

3.1.5 Pseudonymisation des porteurs

L'identité utilisée dans les certificats de porteurs n'est ni un pseudonyme ni un nom anonyme (Voir § 3.1.4).

3.1.6 Règles d'interprétations des différentes formes de noms

Les UC (applications, réseaux, machines, organisme extérieurs, ...) peuvent se servir des certificats d'AC et de porteurs pour mettre en œuvre et valider des fonctions de sécurité, en vérifiant entre autres les identifiants (DN) des porteurs et des AC contenues respectivement dans les certificats de porteur et d'AC.

3.1.7 Unicité des noms

Les DN des certificats porteurs sont uniques au sein du domaine de certification de l'AC qui émet le certificat. L'identifiant unique qui fait partie intégrante du DN assure à lui seul l'unicité des DN, indépendamment du contenu du prénom et du nom. Cet identifiant unique peut être utilisé pour rechercher dans l'annuaire d'origine des propriétés ou des attributs liés au porteur. Durant toute la durée de vie de l'AC, un DN attribué à un porteur ne peut être attribué à un autre porteur.

3.1.8 Identification, authentification et rôle des marques déposées

Sans objet.

3.2 Vérification initiale d'identité

Pour être un futur porteur, il est nécessaire d'avoir été préalablement enregistré dans l'un des annuaires utilisés comme référentiel. Les OC sont en mesure de connaitre les demandes de certificats pour les sites dont ils sont responsables.

La validation initiale de l'identité consiste pour l'AED à :

1. Vérifier l'éligibilité du porteur en vérifiant sa présence dans l'application « Pages Blanches »
2. Vérifier que le futur porteur appartient bien au site ou bien à un site rattaché,
3. Valider la demande une fois ces vérifications effectuées,
4. Pour les OC : transmettre la demande à l'AED dont il dépend.

Dans le cadre de l'AC Personnes 4, tous les futurs porteurs sont déclarés dans l'annuaire du ministère de la justice. L'identification de la personne physique a donc été préalablement effectuée.

3.2.1 Méthode pour prouver la possession de la clé privée

Les clés privées initiales sont générées par l'AC. Seule la personne possédant à la fois le support des clés (une carte à microcircuit) et les codes d'activation initiaux est en mesure d'utiliser les clés privées.

Lors d'un premier renouvellement des clés privées, les bi-clés sont générées par le support de clés. Il est alors vérifié que les clés privées ont bien été générées dans le support initialement en possession du porteur. De ce fait, seul le porteur original est en mesure d'utiliser les nouvelles clés privées.

3.2.2 Validation de l'identité d'un organisme

Sans objet.

3.2.3 Validation de l'identité des porteurs

Le dossier d'enregistrement déposé auprès de l'AE comprend :

- Le nom de famille ou d'usage et prénoms ;
- L'identifiant unique ministère de la justice, appelé aussi identifiant « Pages Blanches » ;
- Une adresse de messagerie permettant de contacter le porteur.
- Une adresse pour l'expédition de la carte. ;
- Une adresse postale pour l'expédition du code d'activation,

NB : Ces informations sont obtenues par interrogation de l'annuaire ;

L'authentification d'un porteur est réalisée lors d'un face-à-face physique entre le futur porteur et l'OC. Cette disposition permet d'être conforme au niveau (***). Le face-à-face physique est réalisé lors de la remise au porteur du support de clés (i.e. la carte à microcircuit) qui contient à la fois les clés privées et les certificats.

L'AE ou l'OC s'assure de l'identité de la personne en :

- Demandant au porteur de présenter une pièce d'identité en cours de validité comportant une photographie ; par exemple, la carte professionnelle, une carte d'identité ou un passeport ;
- S'assurant que la personne est bien en possession de son code d'activation.

Une copie d'un document officiel d'identité est présente dans tout dossier administratif, ou dossier d'habilitation, des porteurs. Ce dossier est constitué en amont de la procédure d'enregistrement, et peut être consulté à tout moment par toute AE (ou OC en fonction des cas).

Nota : Pour pouvoir emporter la carte, le futur porteur doit présenter le code d'activation et définir deux codes PIN, l'un pour la fonction authentification, l'autre pour la fonction signature. Si la procédure n'est pas effectuée avec succès, l'OC ou l'AED en est averti et la carte est alors restituée à l'OC (ou AED) par le futur porteur.

3.2.4 Informations non vérifiées du porteur

Aucune information non vérifiée n'est introduite dans les certificats.

3.2.5 Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l'identité de la personne physique (directement par l'AEx).

3.2.6 Certification croisée d'AC

L'AC Personnes 4 est uniquement rattachée à l'AC Justice. Tout autre rattachement n'est pas autorisé.

3.3 Identification et validation d'une demande de renouvellement des clés

Le renouvellement d'un certificat s'accompagne toujours d'un renouvellement de la bi-clé.

3.3.1 Identification et validation pour un renouvellement courant

On distingue deux types de renouvellement : le renouvellement de certificats (sans changement de carte) et le remplacement de carte (avec changement de certificats).

Le premier renouvellement est un renouvellement de certificats. Lors de ce premier renouvellement, le porteur est invité par un courriel à se connecter à un portail qui lui permet de renouveler à la fois ses deux clés privées et ses certificats. Dans ce cas, la bi-clé est générée par la carte.

Avant l'envoi du courriel, l'AC s'assure que les informations du dossier d'enregistrement initial sont toujours valides et que le certificat à renouveler existe, et est toujours valide. Cette disposition permet d'être conforme au niveau (***). L'AE s'assure également que le certificat à renouveler existe et peut également vérifier que le renouvellement est nécessaire.

Le renouvellement suivant (le remplacement de la carte) suit le même processus que celui de la première demande de carte : le porteur reçoit un courrier postal contenant un code d'activation et qui l'invite à retirer sa carte auprès de l'AEx de rattachement. Dans ce cas, la bi-clé est générée par l'AC.

Si lors du premier renouvellement l'un des certificats à renouveler a été révoqué, alors les conditions du § 3.2 s'appliquent.

3.3.2 Identification et validation pour un renouvellement après révocation

Les vérifications aux fins de renouvellement de clés après révocation du certificat sont identiques à celles prévues par la procédure initiale (Voir § 3.23).

3.4 Identification et validation d'une demande de révocation

Un certificat porteur peut être révoqué par :

- Le porteur au nom duquel le certificat a été émis ;
- Le personnel appartenant au service qui lui a remis la carte (AED), ou à défaut sa hiérarchie fonctionnelle (AEC ou AE).

Si la demande de révocation est faite par le porteur via un service en ligne (serveur web), le demandeur est formellement authentifié sur la base d'un mot de passe connu uniquement par le porteur et d'une série de trois questions[3]. Cette disposition permet d'être conforme au niveau (***).

Si le porteur n'est pas en mesure de présenter les quatre bonnes réponses, il doit alors s'adresser au personnel appartenant au service qui lui a remis la carte, ou à défaut sa hiérarchie fonctionnelle (AED, AEC ou AE). Ces personnes, après s'être authentifiées à l'aide d'une carte à microcircuit, sont en mesure de révoquer les certificats de toute personne appartenant au site ou bien à un site rattaché.

La révocation par téléphone doit être dûment authentifiée et vérifiée : en cas de doute sur l'authenticité de la demande, il reste possible de se servir du dossier de proximité pour s'assurer de l'identité de l'appelant. En dernier ressort si l'authentification formelle n'a pu être faite, l'autorité d'enregistrement préférera révoquer une carte légitime que de laisser valide un certificat corrompu.

[3] Ce mot de passe et ces questions/réponses ont été choisis par le porteur.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

L'AEx est à l'origine d'une demande de certificat. En fonction de l'avancement des projets de dématérialisation, l'AE, l'AEC, l'OC ou l'AED effectue des demandes de certificats pour le compte des futurs porteurs qui ont besoin d'une carte.

Vis-à-vis de l'AC, l'AEx est à l'origine des demandes de certificats des porteurs pour le ministère de la justice.

4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

Le dossier de demande de certificat d'un simple porteur ou futur porteur est composé des informations suivantes (voir § 3.2.3), extraites du référentiel des identités du ministère de la justice :

- Le nom d'état civil et les prénoms indiqués dans l'annuaire justice,
- L'identifiant unique MJ,
- Une adresse de messagerie professionnelle,
- Une adresse postale professionnelle pour l'expédition de la carte,
- Une adresse postale professionnelle pour l'expédition du code d'activation,
- Une identification de l'opération : génération de certificat ou renouvellement de certificat.

Pour les porteurs, l'autorité d'enregistrement déléguée établit le dossier de demande ou de renouvellement ou valide celui préparé par l'OC.

Si des informations supplémentaires sont requises pour la constitution du dossier de demande de certificat, alors elles sont décrites dans la DPC.

La demande de certificat est validée par une AEx Elle est alors immédiatement transmise à la fonction de génération des certificats pour y être traitée.

4.2 Traitement d'une demande de certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

L'AEx établit la demande de certificat qui est ensuite transmise le cas échéant à l'AED qui contrôle et valide le dossier d'enregistrement fourni (voir § 0).

La référence de la pièce d'identité présentée lors de la remise est enregistrée dans le système de gestion des cartes lors de la remise de la carte au porteur.

4.2.2 Acceptation ou rejet de la demande

Si l'AEx accepte la demande de certificat initiée par l'OC, alors la demande de certificat peut être traitée. L'AED émet alors la demande de génération de la bi-clé et du certificat vers le service adéquat de l'AC. L'AC conserve une trace de la demande de certificat.

Le porteur n'étant pas à l'origine d'une demande de création, il n'est pas informé en cas de rejet.
En revanche dans le cas d'une demande de renouvellement de support (carte) il sera averti par PGCA en cas de rejet de sa demande.

4.2.3 Durée d'établissement du certificat

Lorsque la demande de certificat de porteur est validée par l'AED, son traitement est immédiat. La durée du traitement d'une demande de certificat est précisée dans la DPC.

4.3 Délivrance d'un certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération de la carte, des certificats du porteur et des codes d'activation. Les conditions de génération des bi-clés et des certificats et les mesures de sécurité sont précisées aux § 5 et 6.

4.3.2 Notification par l'AC de la délivrance du certificat au porteur

Le ministère de la justice confie à son PSCE la génération de la première bi-clé du porteur et le PSCE s'assure que le certificat du futur porteur est bien associé à la clé privée présente dans la carte à puce.

Le porteur reçoit ensuite un courriel automatique lui indiquant que la carte a été commandée.

La carte du futur porteur est envoyée à son autorité d'enregistrement sous pli sécurisé, dans une enveloppe sécurisée.

Le code d'activation est envoyé directement au porteur par courrier sécurisé.

Le futur porteur est convoqué par son autorité d'enregistrement ou son OC.pour la remise de sa carte

Conformément à la PC Type du RGS au niveau (***), Le ministère de la Justice peut s'assurer que le certificat est bien associé, dans l'environnement du porteur, à la clé privée correspondante (par exemple, par la mise à disposition par le PSCE d'une application en ligne permettant de réaliser une authentification de test). Il s'agit notamment du cas où le certificat est associé à une clé privée stockée sur une carte à puce non fournie par l'AC : le certificat doit alors être téléchargé sur la bonne carte à puce.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Pour la remise de sa carte, le futur porteur est tenu de s'authentifier. L'authentification du porteur se fait lors d'un face-à-face au moment de la remise du support (cf. § 3.2). Après vérification de son identité au moyen d'un titre comportant une photographie (carte professionnelle, carte d'identité, passeport, ...), l'OC ou l'AED remet le support au porteur.

Le porteur peut contrôler l'identifiant qui figure dans ses certificats et définir deux codes PIN, l'un pour la fonction d'authentification l'autre pour la fonction de signature. Pour cela, il utilise son code d'activation et choisit ensuite ses codes PIN, puis signe les Conditions Générales d'Utilisation (CGU) au moyen de sa clé privée de signature. L'AED contresigne l'attestation d'acceptation. Après quoi, le porteur est autorisé à repartir avec son support de clés. L'AC garde une trace de l'acception du certificat par le porteur. Ces dispositions permettent d'être conforme au niveau (***).

4.4.2 Publication du certificat

Après l'acceptation des certificats par le porteur, ceux-ci sont publiés dans l'annuaire du MJ et dans la base de données de l'IGC.

Nota : les certificats des porteurs ne sont pas publiés par le SP.

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

L'ensemble des composantes de l'IGC, à l'exception du SP, est informé de la délivrance du certificat.

4.4.4 Recouvrement

Sans objet : le recouvrement n'est possible que pour le certificat de chiffrement, qui n'est pas utilisé par le ministère de la justice.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisations de la clé privée et du certificat par le porteur

Les usages autorisés des bi-clés et des certificats sont définis au § 1.5 ci-dessus.

Le porteur dispose de deux clés privées :

- La clé privée d'authentification sert à signer numériquement des données permettant d'authentifier le porteur, typiquement lors d'une authentification du type « client SSL ».
- La clé privée de signature sert à signer numériquement des données permettant de vérifier qu'un document a été effectivement signé à l'aide d'une signature électronique qualifiée.

L'usage d'une bi-clé et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés (voir § 6.1.7).

Certificats d'authentification

Les bi-clés et les certificats générés dans le cadre de la PC pour les certificats d'authentification sont uniquement destinés à l'authentification des porteurs.

Certificats de signature

Les bi-clés et les certificats générés dans le cadre de la PC pour les certificats de signature sont uniquement destinés à la mise en place de signatures électroniques qualifiées.

Cet usage est également explicité dans les conditions générales d'utilisation qui sont fournies au porteur lors de la remise du support. Le porteur est tenu de les respecter.

4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Un utilisateur de certificats doit utiliser des logiciels qui sont à même de vérifier que le certificat d'un porteur est effectivement utilisé selon l'usage prescrit dans le certificat (authentification ou signature). Pour cela, il doit soit utiliser les logiciels mis à sa disposition par le ministère de la justice, soit sous sa propre responsabilité utiliser des logiciels donnant les mêmes garanties. Dans le cas contraire, sa responsabilité pourrait être engagée.

Un utilisateur de certificat (ex. : une application utilisatrice de certificats) doit utiliser un logiciel qui vérifie que le certificat est valide. La vérification que doit effectuer le logiciel est différente selon qu'il s'agit de la vérification en temps-réel d'un échange d'authentification ou la vérification en temps différé d'une signature électronique.

Pour la vérification en temps-réel d'un échange d'authentification, le logiciel doit construire un chemin de certification entre le certificat du porteur et le certificat auto-signé de l'AC Justice 2, et s'assurer qu'au moment de l'échange aucun des certificats du chemin n'est en dehors de sa période de validité ou révoqué.

Pour la vérification en temps différé d'une signature électronique, le logiciel doit construire un chemin de certification entre le certificat du porteur et le certificat auto-signé de l'AC Justice 2, et s'assurer qu'au moment où la signature numérique a été horodatée par une unité d'horodatage de confiance qu'aucun des certificats du chemin n'était en dehors de sa période de validité ou révoqué. Il doit en outre s'assurer que le certificat de l'unité d'horodatage est valide.

4.6 Renouvellement d'un certificat

Dans le cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. La délivrance d'un nouveau certificat suite à changement de la bi-clé est traitée à la section 4.7.

Nota - 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).

4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat au porteur lié à la génération d'une nouvelle bi-clé.

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés des porteurs, et les certificats correspondants, sont renouvelés tous les 3 ans.

Une bi-clé et un certificat peuvent aussi être renouvelés par anticipation, suite à la révocation du certificat du porteur (cf. § 4.9, notamment le § 4.9.1 pour les différentes causes possibles de révocation) ou pour anticiper un renouvellement massif de certificats.

4.7.2 Origine d'une demande d'un nouveau certificat

En temps normal, le certificat est renouvelé tous les trois ans :

- Une fois sur deux, la carte est conservée et le renouvèlement des bi-clés et des certificats s'effectue en ligne ;
- Une fois sur deux, une nouvelle carte est générée.

L'IGC gère automatiquement la durée de 3 ans.

4.7.3 Procédure de traitement d'une demande d'un nouveau certificat

Trois mois avant la fin de validité d'un certificat, l'IGC ajoute automatiquement à la liste des demandes initiales de certificats à valider, les demandes de renouvèlement de certificats à valider. Ces demandes sont ventilées auprès des personnes ayant le rôle d'AED.

Ces personnes vérifient que les personnes pour lesquelles le renouvellement est demandé font toujours partie de leurs effectifs et, si cela est le cas, valident la demande de renouvellement.

4.7.4 Notification au porteur de l'établissement du nouveau certificat

Lorsque la carte est conservée, le porteur est invité par la réception d'un courriel à effectuer le renouvèlement des bi-clés et des certificats en se connectant à un portail dont l'adresse est spécifiée dans ce courriel.

Lorsque la carte est changée et une fois que la nouvelle carte a été fabriquée, le porteur est convoqué par courriel par son AE ou OC pour remise de sa carte en face-à-face.

Lorsque les certificats d'une carte ont été révoqués, la procédure est alors analogue à une demande de carte initiale.

Lors d'un renouvèlement anticipé, le porteur peut recevoir, selon le cas, un courriel avant la date anniversaire.

4.7.5 Démarche d'acceptation du nouveau certificat

Lorsqu'il s'agit de la délivrance d'une nouvelle carte, se reporter à la section § 4.4.1.

Lorsqu'il s'agit d'un renouvèlement des bi-clés et des certificats sans changement de carte, le porteur se connecte à un portail en utilisant sa carte. Il doit alors suivre les instructions données par le portail.

4.7.6 Publication du nouveau certificat

Après l'acceptation des certificats par le porteur, ceux-ci sont publiés dans l'annuaire du ministère de la justice et dans la base de données de l'IGC.

4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Une fois la publication faite, l'ensemble des composantes de l'IGC, à l'exception du SP, est informé de la délivrance du certificat.

4.8 Modification du certificat

La modification du certificat n'est pas autorisée au titre de la présente PC.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats de porteurs

Un certificat de porteur est révoqué quand l'association entre ce certificat, la clé publique et le porteur qu'il certifie n'est plus considérée comme valide. Les motifs qui invalident cette association peuvent être :

- Le décès du porteur ou la cessation d'activité du porteur ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ;
- L'information contenue dans le DN du certificat n'est plus valide (par exemple, changement de nom) ;
- Le porteur n'a pas respecté les modalités applicables à l'utilisation du certificat ;
- Le support de clés du porteur a été perdu ou volé ;
- L'une des données d'activation a été compromise ou est suspectée d'avoir été compromise ;
- Le support de clés du porteur est bloqué et ne peut être débloqué
- Le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le porteur n'a pas respecté ses obligations découlant de cette PC ;
- La modification de la taille des clés imposée par des institutions nationales compétentes ;
- La perte de l'autorisation de possession d'un certificat.

Lorsque l'une de ces occurrences se produit, le certificat du porteur en question doit être révoqué.

4.9.1.2 Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats ou de LCR) :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats de porteurs

Les personnes / entités qui peuvent demander la révocation d'un certificat porteur sont les suivantes :

- Le porteur au nom duquel le certificat a été émis ; ou
- Une personne ayant le rôle d'AED, dans l'AED de rattachement du porteur.

4.9.2.2 Certificats d'une composante de l'IGC

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

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat de porteurs

Une demande de révocation peut être effectuée par le porteur sur un site web configuré en mode HTTPS (par Internet : https://justice-crd.cms.plateforme-cartes-agents.ingroupe.com/cms-fo/page/usernamelogin.xhtml ou par le RIE : https://justice-crd.cms.plateforme-cartes-agents.rie.gouv.fr/cms-fo/page/username-login.xhtml), disponible 24h/24 et 7j/7. Dans ce cas, les demandes de révocation sont authentifiées à l'aide du mot de passe personnel du porteur et de trois réponses aux questions secrètes.

Une demande de révocation peut également être effectuée sur un autre site web configuré en mode HTTPS (https://justice.cms.plateforme-cartes-agents.ingroupe.com/cms-fo), disponible 24h/24 et 7j/7, par toute personne habilitée dans son rôle d'AEC ou d'AED vis-à-vis du porteur. Dans ce cas, l'authentification se fait alors à l'aide de la carte à micro-circuit du demandeur.

Les informations suivantes figurent dans la demande de révocation du certificat :

- L'identifiant (DN) du porteur du certificat ;
- Le nom du demandeur de la révocation et ses contacts (téléphone, email) ;
- La cause de la révocation.

Dans le cas où la demande de révocation est faite par un AEx (AEC ou AED) autre que le porteur, une fois la demande authentifiée et contrôlée, l'AEx doit choisir le motif de la révocation, puis valider l'opération.

La fonction de gestion des révocations révoque alors le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée via une LCR signée par l'AC Personnes.

Les causes de révocation ne sont pas publiées dans les Listes de Certificats Révoqués (LCR). Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du certificat.

L'AE authentifie la demande de révocation (Voir § 4.9.2).

L'AE transmet la demande de révocation auprès de l'AC.

Les informations suivantes figurent dans la demande de révocation de certificat :

- L'identifiant (DN) du porteur du certificat ;
- Le nom du demandeur de la révocation et ses contacts (téléphone, email) ;
- Le motif de la révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée via la LCR signée par l'AC Personnes sans contenir la cause de révocation.

Le demandeur de la révocation et l'AED sont informés du bon déroulement de l'opération et de la révocation effective du certificat. Dans le cas où le porteur du certificat n'est pas le demandeur, il est informé de la révocation effective de son certificat par l'envoi d'un courriel ou de tout autre moyen la disposition de l'AED.

Dans tous les cas où la carte est présente ; l'AED doit détruire cette carte et inscrire sa destruction dans le champ commentaire réservé à cet effet dans PGCA.

Lors des opérations de maintenance de PGCA, lorsque celui-ci est indisponible sans bascule sur le site de secours, il existe également une procédure de révocation par courriel. Cette procédure est directement disponible sur la page de maintenance de PGCA. Elle repose principalement sur une révocation directement au niveau de l'IGC impliquant, lors du retour à la normale, une procédure de resynchronisation entre les données de l'IGC et celles de PGCA.

4.9.3.2 Révocation d'un certificat d'une composante de l'IGC

L'AC précise dans sa DPC les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs et des utilisateurs de certificats concernés. Pour cela, l'AC utilise les moyens d'information à destination des agents du ministère qui sont à sa disposition (intranet, directive).

Le FSSI doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

Le DITP et l'ANSSI se réservent le droit de diffuser par tout moyen l'information.

NB : Conformément à la section IV.9.3.2 de la PC Type (Révocation d'un certificat d'une composante de l'IGC), l'ANSSI doit être informée et se réserve le droit de diffuser cette information par tout moyen à sa disposition).

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Dès que le porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

4.9.5 Délai de traitement par l'AC d'une demande de révocation

4.9.5.1 Révocation d'un certificat de porteur

Par nature, une demande de révocation doit être traitée en urgence.

La fonction de gestion des révocations est disponible 24h/24 7j/7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 1 heure et une durée maximale totale d'indisponibilité par mois de 4 heures.

Toute demande de révocation d'un certificat porteur est traitée dans un délai inférieur ou égal à 24 heures. Il s'agit du délai entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

4.9.5.2 Révocation d'un certificat d'une composante de l'IGC

La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat. La révocation d'un certificat de signature de l'AC (signature de certificats et de LCR) est effectuée après accord ou sur demande du ministère de la justice.

4.9.6 Exigences de vérification de révocation par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier, l'état des certificats de l'ensemble du chemin de certification correspondant, en utilisant une LCR pour chaque certificat faisant partie du chemin.

4.9.7 Fréquence d'établissement des LCR

Une nouvelle LCR est émise toutes les 24 heures.

Il n'est pas mis en place de mécanisme de delta LCR.

4.9.8 Délai maximum de publication d'une LCR

Une LCR est publiée dans un délai maximum de 30 minutes après sa génération.

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

Un service OCSP existe et est consultable à l'adresse « http://ocsp.ants.gouv.fr/justice/ac_personnes_X » où la valeur de « X » commence à 4. Une nouvelle URL sera mise en place à chaque renouvellement d'AC et incrémentera de 1 la valeur de « X ».

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Les utilisateurs de certificats n'utilisant pas la lecture de la LCR doivent utiliser le service OCSP.

4.9.11 Autres moyens disponibles d'information sur les révocations

En cas de changement de ce certificat auto-signé avant la date initialement prévue, le SP informe les porteurs et les utilisateurs de certificats qu'un nouveau certificat auto-signé est disponible et de la date de révocation programmée du certificat auto-signé courant.

4.9.12 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 dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Le porteur, en cas de compromission de sa clé privée ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé.

4.9.13 Causes possibles d'une suspension

Dans le cadre de la présente PC, la suspension de certificats n'est pas autorisée.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LAR / LCR au format v2. De ce fait, les LAR / LCR comportent la date au plus tard de leur prochaine publication.

Les LAR sont publiées aux points de distribution des LAR (ARL Distribution Point). Chaque certificat d'AC comporte l'adresse du point de distribution de la LAR le concernant.

Les LCR sont publiées aux points de distribution des LCR (CRL Distribution Point). Chaque certificat d'un porteur comporte l'adresse du point de distribution de la LCR le concernant.

La LCR intègre aussi les certificats révoqués, ayant expiré après la date valorisant l'attribut « expiredCertsOnCRL ». Ce dernier est renseigné avec la valeur mentionnée dans le tableau du chapitre **Erreur ! Source du renvoi introuvable.**.

Une semaine avant l'expiration du certificat d'AC, les certificats émis par l'AC et non expirés sont révoqués. L'AC émet alors une dernière LCR dont la date de fin de validité est positionnée au 31 Décembre 9999, 23h59m59s.

4.10.2 Disponibilité de la fonction

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

4.10.3 Dispositifs optionnels

Un service OCSP est disponible. Il est décrit au paragraphe 4.9.9.

4.11 Fin de la relation entre le porteur et l'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, le certificat de porteur doit être révoqué, et la carte doit être détruite en coupant la puce en deux endroits à l'aide d'une paire de ciseaux.

4.12 Séquestre de clé et recouvrement

Le séquestre des clés privées des porteurs est interdit par la présente PC.

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physique

La section § 1.3 définit les différentes entités intervenant dans l'IGC.

- Service d'enregistrement,
- Service de génération des certificats,
- Service de génération des éléments secrets du porteur,
- Service de remise au porteur,
- Service de publication,
- Service de gestion des révocations,
- Service d'information sur l'état des certificats, et
- Service de journalisation.

Ces services ne sont pas réalisés sur le même site.

Le site d'exploitation de l'IGC regroupe les services suivants : service de génération des certificats, service de génération des éléments secrets du porteur, service de gestion des révocations et service de journalisation. Ce site est placé sous la responsabilité de l'INGroupe.

Le site de mise à disposition des informations aux utilisateurs supporte le service suivant : service de publication et service d'information sur l'état des certificats. Ce site est placé sous la responsabilité du ministère de la justice.

Le service d'enregistrement et le service de remise au porteur sont des services décentralisés dans les locaux du MJ. Il s'agit des AED et des OC.

5.1.1 Situation géographique et construction des sites

Le site d'exploitation de l'IGC est installé dans les locaux du PSCE, situés sur le territoire national. La construction des sites respecte les règlements et normes en vigueur, ainsi que les recommandations de l'ANSSI. Les caractéristiques ont été définies selon les résultats de l'analyse de risques précisée dans la DPC. Les opérations cryptographiques réalisées pour la génération des certificats issus de l'AC Personnes 4, se font au sein des locaux du PSCE qui sont à plus de 20 mètres à l'intérieur d'une zone réservée au sens de l'IGI 1300.

Le site de mise à disposition des informations est installé dans les locaux du ministère de la justice.

Les sites où sont implantées les AED et les OC sont répartis sur tout le territoire national, dans les locaux du ministère de la justice.

5.1.2 Accès physique

Les moyens et informations du site d'exploitation de l'IGC utilisés dans le cadre de la mise en œuvre opérationnelle de l'IGC sont installés dans une enceinte des locaux d'exploitation du PSCE dont les accès sont contrôlés et réservés aux personnels habilités.

Le PSCE met en œuvre un système de contrôle des accès qui permet de garantir la traçabilité des accès aux zones en question. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. Si des personnes non habilitées doivent pénétrer dans les installations, elles font l'objet d'une prise en charge par une personne habilitée qui en assure la surveillance. Ces personnes doivent en permanence être accompagnées par des personnels habilités.

Le PSCE a défini un périmètre de sécurité physique où sont installées ces machines. La mise en œuvre de ce périmètre permet de respecter la séparation des rôles de confiance telle que prévue dans la présente PC. Ce périmètre de sécurité garantit, en cas de mise en œuvre dans des locaux en commun, que les fonctions et informations hébergées sur les machines ne sont accessibles qu'aux seules personnes ayant des rôles de confiance reconnus et autorisées. Ces points sont précisés dans la DPC. Ces dispositions permettent d'être conforme au niveau (***).

5.1.3 Alimentation électrique et climatisation

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

5.1.4 Vulnérabilité aux dégâts des eaux

Les mesures de protection contre les dégâts des eaux mis en œuvre par le PSCE permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC, notamment en matière de disponibilité de ses fonctions de gestion des révocations de publication et d'information sur l'état de validité des certificats.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies mis en œuvre par le PSCE permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC, notamment en matière de disponibilité de ses fonctions de gestion des révocations, de publication et d'information sur l'état de validité des certificats.

5.1.6 Conservation des supports

Les mesures et moyens de conservation des supports d'information mis en œuvre par le PSCE permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC. En particulier la disponibilité, la confidentialité et l'intégrité des données conservées dans les journaux, les archives et les logiciels utilisées par l'AC est assurée.

5.1.7 Mise hors service des supports

Le site d'exploitation de l'IGC utilise des mécanismes de destruction des supports papiers (tels que des broyeurs) et des supports magnétiques d'information. Les matériels réformés ayant servi à supporter l'IGC font l'objet de mesures préalables de neutralisation. En fin de vie, les supports sont détruits.

L'ensemble des porteurs, en possession d'une carte dont la fin de vie est effective, doit s'assurer de la destruction du composant électronique de deux coups de ciseaux dans la puce de la carte.

5.1.8 Sauvegardes hors site

Le site d'exploitation de l'IGC réalise des sauvegardes en s'appuyant majoritairement sur les procédures d'exploitation interne existantes du PSCE, ajustées en fonction des particularités de cette IGC. Celles-ci sont de nature à permettre une reprise rapide des fonctions de gestion des révocations, de publication et d'information sur l'état des certificats, suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces fonctions.

Le site de mise à disposition des informations du ministère de la justice met en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.). Cette disposition permet d'être conforme au niveau (***).

5.2 Mesures de sécurité procédurales

L'ensemble de ce chapitre est respecté par les entités intervenant dans la gestion du cycle de vie des certificats émis par l'AC. En particulier, le PSCE s'assure de la mise en œuvre effective des mesures de sécurité procédurales pour l'utilisation opérationnelle des certificats d'AC au sein de ses locaux.

5.2.1 Rôles fonctionnels de confiance

Les personnes auxquelles sont attribués des rôles fonctionnels de confiance de l'IGC sont toutes des personnes habilitées du PSCE ou du MJ.

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

Les rôles fonctionnels de confiance sont classés en cinq groupes :

- « Responsable de sécurité » : Il est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux d'évènements Il est responsable des opérations de génération et de révocation des certificats.
  NB : au sein de l'IGC justice ce rôle est tenu par le Fonctionnaire de Sécurité des Systèmes d'Information (FSSI) avec comme vecteurs de diffusion les Responsables de la Sécurité des systèmes d'information (RSSI) de chaque entité.

- « Responsable d'application » : Il est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
  NB : au sein de l'IGC justice ce rôle est tenu par le directeur de programme PGCA. Pour ces responsabilités il s'appuie sur le RCSSI et les RSSI d'application (« responsable d'application SP » et le « responsable d'application PSCE » pour leurs domaines de compétences propres).
- « 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 des réseaux de la composante.
  NB : au sein de l'IGC justice ce rôle est tenu par les superviseurs techniques
- « 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
  NB : au sein de l'IGC justice ce rôle est tenu par les opérateurs de certification (OC) et les autorités d'enregistrement (AE, AEC et AED) globalement désignées par AEx.
- « Contrôleur » : Personnel, dont la responsabilité est de réaliser les opérations de vérification de la bonne application des mesures et de la cohérence de fonctionnement de l'IGC Personnes. Le contrôleur est autorisé 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, etc.

Ce personnel est désigné par le HFDS du ministère de la justice, ou par le responsable d'application du PSCE (avec dans ce dernier cas une portée des opérations de vérification limitées aux prestations opérées par le PSCE).

NB : au sein de l'IGC justice, ce rôle est tenu par les RSSI de chaque entité (RCSSI) pour le ministère de la justice et des chargés d'audit (CHAD).

Les attributions détaillées de chaque rôle de l'IGC sont données au chapitre 1.3 de la DPC.

5.2.2 Nombre de personnes requises par tâche

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 » de la DPC définit le nombre d'exploitants nécessaires à chaque opération.

5.2.3 Identification et authentification pour chaque rôle

Le PSCE procède à la vérification de l'identité et des autorisations de tout membre de son personnel amené à travailler au sein de l'IGC 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 l'IGC ;
- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement aux systèmes ;
- Le cas échéant et en fonction du rôle tenu, qu'un compte soit ouvert à son nom sur les systèmes ;
- Que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu au sein de l'IGC.

Les contrôles effectués sont décrits dans la DPC de l'AC et sont conformes à la politique de sécurité applicable. Chaque attribution d'un rôle à un membre du personnel de l'IGC est notifiée par écrit.

5.2.4 Rôles exigeant une séparation des attributions

Les attributions de chaque rôle de l'IGC sont données dans l'annexe « Rôles » de la DPC qui précise comment et sous quelles conditions ces rôles peuvent être cumulés par un même exploitant.

La séparation de ces rôles repose sur :

- La notion de séparation des rôles dits « d'administration », des rôles dits « opérationnels » : une personne qui peut assigner des fonctions et/ou un rôle sur une composante d'IGC pour la mise en œuvre d'un service ne met pas en œuvre le service correspondant ;
- La notion de double contrôle sur un service de l'IGC : une double validation est nécessaire sur les opérations dites « sensibles » (cérémonie des clés, demande et génération d'un certificat, ...).

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

- Responsable de sécurité et ingénieur système/opérateur/contrôleur ;
- Ingénieur système, opérateur et contrôleur.

Ces dispositions permettent d'être conforme au niveau (***).

La mise en œuvre de cette séparation repose sur des mécanismes organisationnels et/ou techniques.

5.3 Mesures de sécurité vis-à-vis du personnel

L'ensemble des mesures décrites dans ce chapitre est respecté par les entités intervenant dans la gestion du cycle de vie des certificats émis par l'AC. En particulier, le PSCE s'assure de la mise en œuvre effective des mesures de sécurité du personnel lors de la mise en œuvre opérationnelle des certificats d'AC au sein de ses locaux.

5.3.1 Qualifications, compétences et habilitations requises

Tout le personnel opérant pour le compte de l'IGC Personnes 4 est formé pour comprendre les rôles qui leur sont attribués. Le nom et la fonction de tout le personnel intervenant pour le compte de l'IGC Personnes sont répertoriés. Le ministère de la justice et le PSCE font en sorte que les compétences professionnelles des personnes placées sous leur responsabilité soient cohérentes à leurs attributions.

5.3.2 Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC s'assure de l'honnêteté de ses personnels amenés à travailler au sein de la composante.

Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. Leurs antécédents sont vérifiés :

- Par le Service de Sécurité du Ministère de l'Intérieur pour le PSCE ;
- Lors de la constitution du dossier administratif pour les agents du ministère ;
- Lors de la constitution du dossier d'habilitation d'accès aux établissements pénitentiaires pour les personnels extérieurs (autres fonction publique ou personnels de sociétés privées) ;

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches. Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues au minimum tous les 3 ans.

5.3.3 Exigences en matière de formation initiale

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, au sein de l'entité dans laquelle il opère. Le personnel a eu connaissance et est réputé avoir compris les implications des opérations dont il a la responsabilité.

5.3.4 Exigences et fréquence 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 et dans l'organisation, en fonction de la nature de ces évolutions.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Aucune rotation n'est imposée dans le cadre de la présente PC.

5.3.6 Sanctions en cas d'actions non autorisées

Le responsable de l'AC décide des sanctions à appliquer lorsqu'un agent sous la responsabilité MJ abuse de ses droits ou effectue une opération non conforme à ses attributions, selon les modalités applicables.

Lorsque le manquement est commis par un agent du PSCE, le responsable de l'AC demande au responsable du PSCE de prendre les sanctions appropriées et de lui en rendre compte. Les modalités d'application et de délégation sont précisées dans la DPC.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Les éventuels personnels contractants doivent respecter les mêmes conditions que celles énoncées dans le § 5.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8 Documentation fournie au personnel

Chaque personnel dispose 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 en termes de sécurité.

5.4 Procédures de constitution des données d'audit

L'ensemble de ce chapitre est respecté par les entités intervenant dans la gestion du cycle de vie des certificats émis par l'AC. En particulier, le PSCE s'assure de la mise en œuvre effective des mesures de constitution des données d'audit dans la mise en œuvre opérationnelle des certificats, des supports de clé et des données d'activation au sein de ses locaux.

5.4.1 Type d'évènements à enregistrer

L'IGC enregistre les évènements liés aux services et à la protection de l'AC (accès physique, ...) qu'elle met en œuvre.

Chaque enregistrement d'un évènement dans un journal contient au minimum les informations suivantes :

- Le type d'évènement ;
- Le nom de l'exécutant ou la référence du système déclenchant l'évènement ;
- La date et heure de l'évènement ;
- Le résultat de l'évènement (échec ou réussite).

Pour les types d'évènements pour lesquels ces informations existent, les enregistrements comporteront également les champs suivants :

- Le destinataire de l'opération ;
- Le nom du demandeur de l'opération ou la référence du système effectuant la demande ;
- Le nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- La cause de l'évènement ;
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation sont effectuées en tâche de fond tout au long de la vie de l'IGC. L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée.

En cas de saisie manuelle, l'écriture est effectuée, sauf exception, le même jour ouvré que l'évènement.

5.4.2 Fréquence de traitement des journaux d'évènements

Les responsables sécurité de chaque composante de l'IGC analysent et contrôlent quotidiennement les journaux d'évènements afin d'identifier les anomalies (tentatives en échec, usurpation, ...).

Ces analyses sont transmises de manière hebdomadaire au responsable de sécurité de la partie technique du PSCE Ce responsable de sécurité contrôle et analyse de façon globale la totalité des analyses des journaux, ce qui donne lieu à un résumé mensuel qui fait apparaitre les différentes anomalies.

Ce résumé est transmis de manière mensuelle au responsable sécurité de l'IGC.

Ces analyses et contrôles sont détaillés dans la DPC.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés pendant 7 ans après leur génération. Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous 1 mois. Ils restent sur le site au moins 1 mois.

5.4.4 Protection des journaux d'évènements

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 à partir de leur constitution.

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

Le système interne de datation de l'IGC associe à toutes les archives une date locale.

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

5.4.5 Procédure de sauvegarde des journaux d'évènements

Chaque entité intervenant pour le compte de l'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité de ses journaux d'évènements, conformément aux exigences de la présente PC. Cette procédure est précisée dans le document « fiche de sauvegarde des journaux de l'IGC Justice » disponible auprès du SNum.

5.4.6 Système de collecte des journaux d'évènements

Le système de collecte des journaux assure la collecte des archives en respectant le niveau de sécurité relatif à l'intégrité, la disponibilité et la confidentialité des données. Le système de collecte doit garantir que les journaux ne sont pas altérés depuis leur génération au niveau de l'applicatif.

5.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement

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

5.4.8 Évaluation des vulnérabilités

Chaque entité intervenant pour le compte de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de son fonctionnement.

Les journaux d'évènements sont analysés dans leur totalité chaque jour ouvré ou dès la détection d'une anomalie par un responsable de sécurité du PSCE afin d'identifier celles liées à des tentatives en échec. Ces contrôles sont réalisés par un personnel habilité du PSCE, dans son rôle de confiance de « Contrôleur ». Ces analyses donnent lieu à un résumé qui fait apparaître les anomalies constatées.

Un rapprochement entre les journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, par exemple) est effectué sur une base hebdomadaire par un responsable de sécurité du PSCE afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie. Le résultat est transmis au RSSI du PSCE et à celui du ministère de la justice.

Les procédures sont détaillées dans la DPC.

5.5 Archivage des données

5.5.1 Types de données à archiver

L'archivage permet d'assurer la pérennité des données numériques constituées lors des opérations effectuées au profit de l'IGC. Il permet également la conservation de pièces papier, ainsi que leur disponibilité en cas de nécessité.

Les informations archivées sont les suivantes :

- Les PC ;
- Les DPC ;

- Les conditions générales d'utilisation (CGU) ;
- Les accords contractuels avec les autres AC ;
- Les certificats de l'AC, y compris les certificats révoqués ou devenus invalides ;
- Les certificats et LCR tels qu'émis ou publiés ;
- Les récépissés ou notifications (à titre informatif) ;
- Les engagements signés électroniquement des porteurs ;
- Les justificatifs d'identité des porteurs (sont conservés via le SIRH Harmonie) et, le cas échéant, de leur entité de rattachement ;
- Les demandes d'enregistrement au travers de l'annuaire justice ;
- Les journaux d'événements des différentes entités de l'IGC ;
- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques.

5.5.2 Période de conservation des archives

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.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat est en mesure d'être présenté par l'AC lors de toute sollicitation par les autorités habilitées. Ce dossier, complété par les mentions consignées par une personne ayant le rôle d'AED, permet de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

Noms Distinctifs

Tout DN (Distinguished Name) est conservé aussi longtemps que le DN de l'AC Personnes 4 perdure. Les informations personnelles associées au DN sont conservées pendant la même durée afin de garantir qu'un même DN n'est jamais utilisé par une autre personne que le premier titulaire du DN.

Certificats et LCR émis par l'AC

Les certificats de clés de porteurs et d'AC, ainsi que les LCR / LAR produites, sont archivés pendant au moins 5 années après leur expiration. La période de conservation ne doit pas excéder les 30 années.

Journaux d'évènements

Les journaux d'évènements sont archivés pendant au moins 7 ans après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage offrent le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des journaux est assurée tout au long de leur cycle de vie.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes :
- Sont protégées en intégrité ;
- Ne sont accessibles qu'aux personnes autorisées ;
- Peuvent être relues et exploitées.

5.5.4 Procédure de sauvegarde des archives

Le responsable de l'AC et le PSCE ont la responsabilité de mettre en place et maintenir les mesures requises afin d'assurer l'intégrité et la disponibilité de leurs archives, conformément aux exigences de la présente PC.

5.5.5 Exigences d'horodatage des données

Tous les composants de l'AC sont régulièrement synchronisés avec un serveur Network Time Protocol (NTP).

5.5.6 Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données (voir § 5.5.3).

5.5.7 Procédures de récupération et de vérification des archives

Les archives (papiers et électroniques) sont accessibles dans un délai maximum de 2 jours ouvrés.

5.6 Changement de clé d'AC

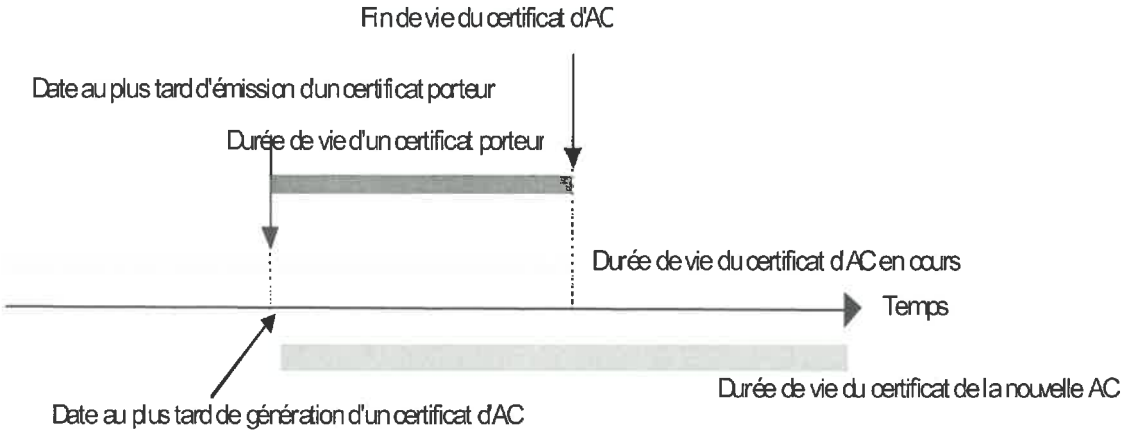
La durée de vie d'un certificat d'AC est conforme aux recommandations cryptographiques de sécurité relatives aux longueurs de clés formulées par les autorités nationales compétentes en la matière.

Une AC ne peut pas générer de certificats porteurs dont la durée de vie dépasse la période de validité de son certificat d'AC. C'est pourquoi la bi-clé d'une AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats porteurs émis. La durée de vie des certificats des porteurs est de 3 ans.

Dès qu'une nouvelle clé privée est générée pour l'AC, seule celle-ci est utilisée pour générer de nouveaux certificats de porteurs et les LCR de l'AC. Le précédent certificat d'AC reste valable pour valider le chemin de certification des anciens certificats porteurs 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. L'ancienne clé de l'AC sert alors à signer les LCR pour les certificats émis sous cette ancienne clé d'AC.

Le nommage utilisé pour distinguer les clés successives de l'autorité de certification répond aux règles suivantes.

- Dans le champ « Subject » du certificat AC Personnes, la valeur « CN » est construite comme suit :
  - Pour la première clé cette valeur est « Autorité de certification personnes 4 » ;
  - Pour les clés suivantes, cette valeur est « Autorité de Certification Personnes *N* » où N est un entier incrémenté par pas de 1 à chaque changement de clé d'AC, à partir de la valeur « 5 » pour le premier changement (le deuxième jeu de clés).
- La valeur « CN » du champ « Issuer » des certificats porteurs prend la valeur « CN » du champ « Subject » du certificat d'AC ayant servi à les signer.



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 ou compromise.

5.7 Reprise suite à compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

Notamment chaque entité agissant pour le compte de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents. Ce plan est régulièrement testé. L'IGC dispose d'un plan de reprise d'activité en cas de sinistre. La référence au plan anti-sinistre, ses modalités de déclenchement et les personnes responsables de ce plan sont identifiées dans la DPC. Le plan de reprise d'activité en cas de sinistre prend en compte les paramètres suivants :

- Priorisation des actions à mener et délais maximums de recouvrement pour la continuité des services ;
- Politique de sécurité et de protection des secrets ;
- Procédures de secours ;
- Tests pratiques, formation et entraînement des personnels ;
- Procédure de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données) ;
- Procédure de reprise en cas de compromission de clés ;

Ces procédures sont établies en cohérence avec la politique de sécurité des systèmes d'information du PSCE.

En cas de révocation du certificat d'AC, l'AC Racine 2 peut demander un contrôle préalable à la remise en service de l'AC.

5.7.2 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, des engagements de l'AC dans sa propre PC notamment en ce qui concerne les fonctions liées à la publication et à la révocation des certificats.

Ce plan de continuité est testé au minimum une fois par an.

Si le matériel de l'AC est endommagé ou hors service alors que les clés privées de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des services de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC.

5.7.3 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 (voir § 5.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat de l'AC doit être immédiatement révoqué.

Si la clé de signature de l'AC est compromise, perdue, détruite, ou soupçonnée d'être compromise :

- Le responsable de l'AC, après enquête sur l'évènement décide de demander à l'AC de niveau supérieur (l'AC Justice) de révoquer le certificat de l'AC ;
- Tous les porteurs dont les certificats ont été émis par l'AC compromise, sont avisés dans les plus brefs délais que le certificat d'AC a été révoqué ;
- Les personnes ayant le rôle d'AE, AEC, AED ou OC sont avisés dans les plus brefs délais que le certificat d'AC a été révoqué ;
- Une nouvelle bi-clé AC est générée et un nouveau certificat d'AC est émis ;

- Le responsable de l'AC demande à l'AC de niveau supérieur (l'AC Justice) de générer un nouveau certificat d'AC ;
- Les personnes ayant le rôle d'AE, AEC, AED ou OC sont informées de la capacité retrouvée de l'AC de générer des certificats
- Les porteurs sont informés de la capacité retrouvée de l'AC de générer des certificats.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Le plan de reprise d'activité après sinistre traite de la continuité d'activité telle qu'elle est décrite au § 5.7.1.

Le SP est installé afin d'être disponible 24 heures sur 24 et 7 jours sur 7.

5.8 Fin de vie d'AC

Le transfert d'activité est défini comme la fin d'activité d'une entité agissant pour le compte de l'IGC qui n'induit pas d'incidence sur la validité des certificats antérieurement émis. La reprise de cette activité vers une autre entité est organisée par l'AC.

La cessation d'activité est définie comme la fin d'activité de l'autorité responsable d'une entité agissant pour le compte de l'IGC, qui induit une incidence sur la validité des certificats antérieurement émis, autres que les certificats de l'AC.

5.8.1 Transfert d'activité

Dans le cas d'un transfert d'activité d'une entité œuvrant pour le compte de l'IGC, l'AC s'engage à :
- Mettre 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) ;
- Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC ;
- Informer ses partenaires du transfert d'activité et de sa réalisation.

L'AC précise dans la DPC qu'elle doit prévenir comment se déroule le transfert des obligations (archives et logs à une autre entité), et comment seront traités les certificats encore valides qui seraient amenés à être révoqués.

L'entité œuvrant pour le compte de l'IGC et procédant au transfert de son activité s'engage à :

- Avertir l'AC de son intention de transférer son activité avec un préavis d'au moins trois mois ;
- Remettre ses archives à l'autorité responsable de l'AC ;
- Mettre à disposition de l'entité à laquelle son activité est transférée les informations et moyens nécessaires au maintien ou la reprise de l'activité ;
- Communiquer au FSSI les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à la cessation d'activité ou au transfert d'activité de la composante ;
- Communiquer à l'ANSSI à minima six (6) mois avant la date prévue de réalisation, et à la DITP (Direction Interministérielle de la Transformation Publique) en tant que de besoin, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus ; en en mesurant l'impact et en faisant l'inventaire des conséquences
- Tenir informées l'ANSSI et à la DITP en tant que de besoin de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

5.8.2 Cessation d'activité

La cessation d'activité peut être totale ou partielle, typiquement, la cessation d'émission de nouveaux certificats sous cette PC.

En cas de cessation partielle d'activité et dans le cadre d'une cessation de l'émission de nouveaux certificats sous cette PC, l'AC :

1) en informe à l'avance, via le SP, les porteurs et les utilisateurs de certificats ;
2) continue à assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans sa PC, le temps que les porteurs soient équipés de nouveaux certificats, et au plus tard jusqu'à la fin de validité du dernier certificat émis.

Dans l'hypothèse d'une cessation partielle d'activité et dans le cadre d'une cessation de gestion totale des certificats émis sous cette PC, l'AC :

1) en informe à l'avance, via le SP, les porteurs et les utilisateurs de certificats ;
2) cesse d'émettre des LCR, ce qui a pour conséquence d'empêcher la validation des chemins de certification.

Dans l'hypothèse d'une cessation totale d'activité de l'AC, c'est-à-dire pour tous les certificats émis sous cette clé d'AC (toutes PC confondues), l'AC :

1) S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;
2) Prend toutes les mesures nécessaires pour détruire la clé privée lui ayant permis d'émettre des certificats (y compris les copies de sauvegarde) ou la rendre inopérante ;
3) Demande la révocation de son certificat par l'AC de niveau supérieur (AC Justice 2) ;
4) Informe via le SP les porteurs et les utilisateurs de certificats.

6 MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation des bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

Les bi-clés de signature d'AC sont générées lors d'une cérémonie de clé à l'aide d'une ressource cryptographique matérielle.

Les cérémonies de clés se déroulent sous le contrôle d'au moins trois personnes dans des rôles de confiance (maître de cérémonie et témoins). Elle se déroule dans les locaux du PSCE. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement approuvé par le ministère de la justice. Les rôles des personnels impliqués dans les cérémonies de clés sont précisés dans la DPC.

Les manipulations de données secrètes en clair (clés privées d'AC, clés privées des porteurs, parts de secrets d'IGC) sont effectuées dans un environnement protégé contre les rayonnements parasites compromettant : matériels protégés, locaux limitant les risques de fuites d'information par observation visuelle ou rayonnements électromagnétiques (zonage).

Ces dispositions permettent d'être conformes au niveau (***).

6.1.1.2 Transmission de la clé privée à son propriétaire

6.1.1.2.1 Clés porteurs générées par l'AC

Ce paragraphe ne s'applique que lorsque la bi-clé d'un porteur est générée par l'AC.

La génération des clés des porteurs est effectuée dans un environnement sécurisé (voir § 6.4.1). Le PSCE génère, pour une bi-clé, les données d'activations associées (voir § 6.4.1).

Les bi-clés des porteurs sont générées dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré, puis la clé privée est transférée de manière sécurisée dans le support de clés destiné au porteur, sans que l'AC n'en garde aucune copie, tandis que la clé publique est incorporée à la demande de certificat afin d'obtenir un certificat.

Les clés privées sont protégées à la fois en intégrité et en confidentialité et protégées contre un usage abusif à l'aide de données d'activation temporaires au sein de leur support de clés de telle sorte qu'elles ne soient utilisables que par le détenteur des données d'activation.

6.1.1.2.2 Clés porteurs générées par le porteur

Ce paragraphe ne s'applique que lorsque la bi-clé d'un porteur est générée par le support de clés.

Dans le cas où le porteur génère sa bi-clé, cette génération est effectuée dans un dispositif répondant aux exigences du chapitre 12 ci-dessous pour le niveau de sécurité considéré. L'AC s'en assure en mettant en œuvre un canal sécurisé (secure channel) entre l'AC et la carte pour récupérer la valeur de la clé publique.

Les clés privées sont protégées à la fois en intégrité et en confidentialité et protégées contre un usage abusif à l'aide de données d'activation courantes au sein de leur support de clés de telle sorte qu'elles ne soient utilisables que par le détenteur des données d'activation.

6.1.2 Transmission de la clé privée à son propriétaire

Lorsque l'AC génère la bi-clé du porteur (cf. chapitre 6.1.1.2), la délivrance du support de clés au porteur s'effectue via l'AE (AEC, AED ou OC) de manière à garantir la confidentialité et l'intégrité des clés privées et à ne les délivrer qu'au seul porteur. Chaque clé privée est protégée dans son support de clés à l'aide d'un code d'activation. L'envoi du support de clés est effectué de manière séparée dans l'espace ou le temps de l'envoi des codes d'activation. L'AE ne garde aucune donnée permettant de récupérer tout ou partie des clés privées qu'elle a transmise au porteur.

La vérification de l'identité du porteur par l'AE (AEC, AED ou OC) est effectuée via un face-à-face physique lors de la remise de la bi-clé générée par l'AC en présence du porteur. Ces dispositions permettent d'être conforme au niveau (***).

6.1.3 Transmission de la clé publique à l'AC

Lorsque l'AC génère la bi-clé d'un porteur (cf. chapitre 6.1.1.2), la clé publique est protégée en intégrité et son origine authentifiée lorsqu'elle est extraite du module cryptographique.

Lorsque la bi-clé d'un porteur est générée par le support de clés, la clé publique est protégée en intégrité et son origine authentifiée lorsqu'elle est extraite du support de clés : un canal sécurisé (secure channel) est mis en œuvre entre l'AC et la carte.

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

Le certificat de l'AC Personnes 4 (et les certificats issus de ses renouvellements) sont publiés à l'URL : http://www.justice.gouv.fr/igc/ants/

6.1.5 Tailles des clés

Les clés d'AC et de porteurs respectent les exigences de caractéristiques (longueurs, algorithmes, etc.) du document [RGS_A_4].

6.1.5.1 Certificat AC

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 d'AC doivent ou ne doivent pas être modifiés.

L'algorithme RSA avec la fonction de hachage SHA-256 est utilisé. La taille des bi-clés de l'AC Personnes 4 est de 2048 bits.

6.1.5.2 Certificat Porteur

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 doivent ou ne doivent pas être modifiés.

L'algorithme RSA avec la fonction de hachage SHA-256 est utilisé pour les certificats de porteur. La taille des bi-clés est de 2048 bits.

6.1.6 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 propres à l'algorithme correspondant à la bi-clé.

6.1.7 Objectifs d'usage de la clé

Certificat d'AC

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

Certificat d'authentification

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service d'authentification (voir § 1.5.2 et § 4.5). L'utilisation du champ "keyUsage" dans le certificat porteur est : « digitalSignature ».

Certificat de signature

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature (cf. § 1.5.2 et § 4.5). L'utilisation du champ "keyUsage" dans le certificat porteur est «nonRepudiation» tel qu'appelé dans le RFC 5280 de l'IETF ou « content Commitment » tel qu'appelé dans la recommandation ITU-T X.509.

6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'AC

Les ressources cryptographiques de l'AC sont qualifiées au niveau renforcé par l'ANSSI.

La ressource cryptographique matérielle de l'AC utilise des générateurs d'aléas qui sont conformes à l'état de l'art, et aux standards en vigueur. Les algorithmes utilisés pour générer l'aléa de départ sont conformes aux standards en vigueur.

6.2.1.2 Dispositifs d'authentification et de signature des porteurs

L'AC fournit aux utilisateurs le dispositif d'authentification et de signature (carte d'agent). Ce dispositif est qualifié au niveau renforcé par l'ANSSI et respecte les exigences du § 12.

Le renouvellement des bi-clés se fait par la mise en place d'un « *secure messaging* » entre la carte et l'AC permettant de s'assurer que le porteur utilise bien le dispositif fournit originellement.

6.2.2 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 (systèmes où 3 porteurs parmi 5 doivent s'authentifier). Cette disposition permet d'être conforme au niveau (***).

6.2.3 Séquestre de clé privée

Les clés privées d'AC et des porteurs ne font jamais l'objet de séquestre.

6.2.4 Copie de secours de la clé privée

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

La bi-clé d'AC est sauvegardée sous le contrôle de plusieurs personnes à des fins de disponibilité. Les copies de secours des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles. Les sauvegardes sont rapidement 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 d'AC sont stockées dans des ressources cryptographiques matérielles ou sous forme chiffrée.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC Personnes 4 et des porteurs ne sont pas archivées.

6.2.6 Transfert de la clé privée vers / depuis le module cryptographique

Les clés d'AC sont générées et stockées dans des modules de sécurité matériels (HSM ou RCM). Lors d'un transfert, la clé privée est chiffrée. Une clé privée d'AC chiffrée ne peut être déchiffrée sans l'utilisation d'une RCM et l'action des personnes identifiées dans les rôles de confiance.

6.2.7 Stockage de la clé privée dans un module cryptographique

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

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'AC

L'activation des clés privées d'AC dans les modules cryptographiques est contrôlée via des données d'activation (cf. chapitre 6.4) et doit faire intervenir au moins trois personnes dans des rôles de confiance. Cette disposition permet d'être conforme au niveau (***).

6.2.8.2 Clés privées des porteurs

La méthode d'activation d'une clé privée du porteur est contrôlée via un code confidentiel (PIN) (voir § 0) et répond aux exigences définies dans le § 12. Les codes d'activation attribués par l'AC doivent être changés par le porteur lors du face-à-face avant de pouvoir repartir avec sa carte.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

La désactivation des clés privées de l'AC dans le module cryptographique est automatique dès qu'il y a arrêt ou déconnexion du module. Les ressources cryptographiques sont stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

6.2.9.2 Clés privées des porteurs

Les conditions de désactivation de la clé privée d'un porteur répondent aux exigences du § 12. Toute mise hors tension de la carte désactive les clés privées. La désactivation peut aussi s'obtenir au moyen de commandes logicielles spécifiques.

Pour la fonction d'authentification, la clé privée à usage d'authentification est désactivée dès que la carte est retirée du lecteur.

Pour la fonction de signature électronique, la clé privée à usage de signature est utilisable une seule fois. L'utilisation du code PIN de signature électronique est nécessaire pour chaque signature électronique.

La carte agent est configurée de telle sorte que suite à la saisie de trois mauvaises valeurs d'un code PIN, les présentations de ce code ne sont plus possibles. Selon le code concerné, la fonction d'authentification ou la fonction de signature est bloquée. Une procédure particulière permet de débloquer l'une ou l'autre fonction.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'AC

Les clés privées d'AC sont détruites quand elles ne sont plus utilisées ou quand les certificats auxquels elles correspondent sont expirés ou révoqués. La destruction d'une clé privée implique la destruction des copies de sauvegarde, et l'effacement de cette clé sur la ressource cryptographique qui la contient, de manière à ce qu'aucune information ne puisse être utilisée pour la recouvrer.

6.2.10.2 Clés privées des porteurs

En fin de vie de la clé privée d'un porteur, la méthode de destruction de cette clé privée permet de répondre aux exigences définies dans le chapitre 12 pour le niveau de sécurité considéré.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs

Les ressources cryptographiques des AC de l'IGC Justice et des dispositifs des porteurs sont qualifiées au niveau renforcé par l'ANSSI conformément aux exigences du § 11.

6.2.11.1 Niveau de qualification du module cryptographique et des dispositifs d'authentification

Les dispositifs d'authentification des porteurs sont évalués conformément aux exigences du § 12.

Les dispositifs sont choisis dans les produits qualifiés référencés dans le catalogue de l'ANSSI. Des comités sont également réalisés avec l'ANSSI afin de prendre connaissance des produits en cours de qualification au niveau renforcé.

6.2.11.2 Niveau de qualification du module cryptographique et des dispositifs de création de signature

Les dispositifs de création de signature des porteurs sont évalués conformément aux exigences du § 12.

Les dispositifs sont choisis dans les produits qualifiés référencés dans le catalogue de l'ANSSI. Des comités sont également réalisés avec l'ANSSI afin de prendre connaissance des produits en cours de qualification au niveau renforcé.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques sont archivées par archivage des certificats (Voir § 5.5.2).

6.3.2 Durées de vie des bi-clés et des certificats

La durée de vie opérationnelle d'un certificat est limitée par son expiration ou sa révocation. La durée de vie opérationnelle d'une bi-clé est équivalente à celle du certificat auquel elle correspond.

L'AC Personnes 4 ne peut pas émettre des certificats porteur dont la durée de vie est supérieure à celle de son certificat, cf. § 5.6. Les bi-clés et les certificats des porteurs couverts par la présente PC ont une durée de vie de 3 ans. Les certificats d'AC ont une durée de vie de 6 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

Les données d'activation des clés privées de l'AC Personnes 4 sont générées durant les cérémonies de clés (Voir § 5.2.1). Les données d'activation sont générées automatiquement selon un schéma de type m parmi n. Dans tous les cas les données d'activation sont remises à leurs porteurs immédiatement après leur génération. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

6.4.1.2 Génération et installation des données d'activation correspondant à une clé privée du porteur

Le PSCE transmet par courrier à chaque porteur, protégé en intégrité et en confidentialité, un code d'activation de la carte. Ce code est à usage unique. L'envoi du code d'activation de la carte est séparé dans le temps ou dans l'espace de la remise de la carte.

Chaque donnée d'activation d'une clé privée, appelée « code PIN », est choisie par le porteur lors de l'activation de sa carte :

- Une donnée d'activation de la fonction authentification (code PIN) : donnée d'activation utilisée par le porteur pour s'authentifier. C'est ce code qui est utilisé pour protéger et utiliser la clé privée d'authentification contenue dans le support de clés.
- Une donnée d'activation de la fonction de signature (code PIN) : donnée d'activation utilisée par le porteur pour signer électroniquement un ou plusieurs documents. C'est ce code qui est utilisé pour protéger et utiliser la clé privée de signature contenue dans le support de clés.

Le PSCE transmet au porteur les données d'activation protégées en intégrité et en confidentialité. L'envoi des données d'activation est séparé dans le temps ou dans l'espace de la remise du support matériel protégé à l'aide des données d'activation correspondantes.

Le PSCE conserve le code d'activation jusqu'au moment où le porteur a pris possession de son support, après quoi les données d'activation temporaires sont détruites.

6.4.2 Protection des données d'activation

6.4.2.1 Protection des données d'activation correspondant à la clé privée de l'AC

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de secret sont responsables de la gestion et de la protection des parts de secrets dont ils sont porteurs. Un porteur de secret ne peut détenir plus d'une donnée d'activation d'une même clé d'AC à un même instant.

6.4.2.2 Protection des données d'activation correspondant aux clés privées des porteurs

Le code d'activation est communiqué au porteur au moyen d'un courrier postal envoyé à son attention par courrier sécurisé. Les codes PIN créés par le porteur doivent être mémorisés par le porteur. Le porteur ne doit pas communiquer ses codes PIN, et en cas de suspicion de la compromission de ceux-ci il doit les modifier.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini dans la DPC. Il répond 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 de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlés 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 ou secrètes d'infrastructure et de contrôle fait l'objet de mesures particulières, découlant de l'analyse de risque.

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

6.5.2 Niveau de qualification des systèmes informatiques

Les composants d'IGC utilisés pour supporter les services d'AC et qui sont opérés par le PSCE font tous l'objet d'une homologation de sécurité.

L'AC utilise des RCM et des dispositifs sécurisés (carte à puce des porteurs) qualifiés au niveau renforcé par l'ANSSI. Pour tous les autres produits ou solutions, l'AC tend à n'utiliser que ceux reposants sur une base qualifiée par l'ANSSI.

La qualification d'un produit de sécurité est prévue par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 [ORDONNANCE]. Elle atteste de sa conformité à un niveau de sécurité du RGGS. Elle est délivrée par l'ANSSI.

En application de l'article 23 du décret n° 2010-112 du 2 février 2010 [Décret_RGS], les autorités administratives doivent obtenir la validation de leurs certificats électroniques et de ceux de leurs agents au plus tard dans les trois ans à compter de la publication de l'arrêté du 6 mai 2010. L'AC s'engage à se conformer à ces exigences dans le délai imparti.

Nota : en application de l'article 21 du décret n°2010-112 du 2 février 2010, l'ANSSI a mis en place une procédure de validation des certificats électroniques délivrés aux autorités administratives ou à leurs agents.

6.6 Mesures de sécurité liées au développement des systèmes

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

- les matériels et les logiciels sont achetés de manière à réduire les possibilités qu'un composant particulier soit altéré ;
- les matériels et logiciels sont mis au point dans un environnement contrôlé, et le processus de mise au point est défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce ;
- tous les matériels et logiciels sont expédiés ou livrés de manière contrôlée permettant un suivi continu depuis le lieu de l'achat jusqu'au lieu d'utilisation ;
- les matériels et logiciels sont dédiés aux activités de l'AC. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités de l'AC ;
- les applications nécessaires à l'exécution des activités de l'AC sont acquises auprès de sources autorisées.
- 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 installés par des personnels de confiance et formés selon les procédures en vigueur.

6.6.1 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'AC. Lors de son premier chargement, il est vérifié que le logiciel de l'AC est bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

Toute évolution significative d'un système d'une composante de l'AC est signalée au responsable de l'AC pour validation.

6.6.2 Niveau d'évaluation et 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.

6.7 Mesures de sécurité réseau

Une analyse de risque est menée par le responsable de l'AC afin d'établir les objectifs et les règles de sécurité pour la protection des réseaux qui permettent de mettre en œuvre les services de l'AC. Les solutions de sécurité pour ces réseaux sont déclinées en fonction de ses objectifs et règles de sécurité afin de garantir que l'accès aux réseaux n'est possible qu'aux seules entités autorisées. La DPC précise les mesures mises en œuvre pour la protection des réseaux.

Une partie des composantes de l'AC (AE) est accessible en ligne par des postes informatiques sous contrôle ou sous le contrôle du MJ. Une partie des composantes de l'AC (SP) est connectée à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service conforme aux exigences de disponibilité.

Les autres composantes de l'AC utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de détecteurs d'intrusion, de pare-feu et de routeurs filtrants. Les ports et services réseau non utilisés sont fermés.

Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système est hébergé refuse tout service, hormis ceux qui sont nécessaires au système lui-même, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.

6.8 Horodatage/Système de datation

Il n'y a pas d'horodatage au sens du RFC 3161 de l'IETF utilisé par l'AC mais une datation sûre. Tous les composants de l'AC sont régulièrement synchronisés au moyen d'un serveur NTP (Network Time Protocol). Le temps fourni par ce serveur de temps est utilisé en particulier pour établir :

- La date du début de validité d'un certificat porteur ;
- La date du début de l'instant de révocation d'un certificat porteur ;
- Les dates utilisées dans les journaux.

Des procédures automatiques ou manuelles peuvent être utilisées pour maintenir l'heure du système. Les réglages de l'horloge sont des événements susceptibles d'être audités.

7 PROFILS DES CERTIFICATS ET DES LCR

7.1 Profils des Certificats

Les certificats émis par l'AC sont des certificats au format X.509 v3. Les champs des certificats porteurs et AC sont définis par le RFC 5280 et le RFC 3739.

7.1.1 Extensions de Certificats

7.1.1.1 Certificat AC Personnes 4

Les informations principales contenues dans le certificat de l'AC Personnes 4 sont :

Champ de base	Valeur
Version	3 (= version 4)
Serial number	<Chaîne de caractères unique par certificat>
Issuer DN	C = FR
	O = *Ministère de la Justice*
	OU = 0002 <espace > 110010014
	CN = Autorité de certification Justice 2
Subject DN	C = FR
	O = *Ministère de la Justice*
	OU = 0002 <espace > 110010014
	CN = Autorité de certification personnes <X>
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Taille des clés	2048 bits

Durée de validité	6 ans

Nota : La première valeur de « X » dans le CommonName est également à 4. À chaque renouvellement de l'AC Personnes, la règle d'évolution de la valeur « CN » dans le champ « Subject DN » est conforme au § 5.6.

Le certificat d'AC Personnes contient les extensions suivantes :

- Authority Key Identifier (extension non critique) ;
- Basic Constraints (extension critique) : le booléen CA doit avoir la valeur « TRUE » ;
- Certificate Policies (extension non critique) : toutes les stratégies d'émissions (Any Policy) ;
- CRL Distribution Points (extension non critique) : indique le point de distribution de la LAR pour ce certificat ;
- Key usage (extension critique) : indique les usages du certificat d'AC et de la bi-clé correspondante ;
- Subject Key Identifier (extension non critique).

7.1.1.2 Certificats de porteur

Les informations principales contenues dans un certificat du porteur sont :

Champ de base	**Valeur**
Version	2 (=version 3)
Serial number	<Chaîne de caractères unique par certificat>
Issuer DN	C = FR O = *Ministère de la Justice* OU = 0002 <espace > 110010014 CN = Autorité de certification personnes <X>
Subject DN	C = FR O = *Ministère de la Justice* OU = 0002 <espace > 110010014 CN = Prénom<espace>Nom<espace>Identifiant unique
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Taille des clés	2048 bits
Durée de validité	3 ans

Nota : la première valeur de « X » dans le CommonName est également à 4. À chaque renouvellement de l'AC Personnes, la règle d'évolution de la valeur « CN » dans le champ « Subject DN » est conforme au § 5.6.

Le certificat porteur contient les extensions suivantes :

- Authority Key Identifier (extension non critique) ;
- Basic Constraints (extension non critique) : le booléen CA doit avoir la valeur « true ».

- Certificate Policies (extension non critique) : contient l'identifiant de la politique de certification. Selon le type de certificat, le champ contient un OID différent. Il contient :
  - L'OID 1.2.250.1.120.4.2.1.1 s'il s'agit d'un certificat d'authentification ;
  - L'OID 1.2.250.1.120.4.3.1.1 s'il s'agit d'un certificat de signature.
- CRL Distribution Points (extension non critique) : indique le point de distribution de la LCR pour ce certificat.
- Key usage (extension critique) : selon le type de certificat, le bit 0 prend la valeur 1 s'il s'agit d'un certificat d'authentification ou bien le bit 1 prend la valeur 1 s'il s'agit d'un certificat de signature, tandis que tous les autres bits prennent la valeur 0. Lors de la mise en place du certificat de chiffrement le bit 2 prendra la valeur 1.
- Subject Key Identifier (extension non critique).
- Pour la fonction de signature, le certificat contient une extension QcStatements qui contient identifiants d'objet (OID) l'un indiquant qu'il s'agit d'un certificat qualifié et l'autre indiquant que la clé privée réside sur un dispositif sécurisé de création de signature (SSCD).

7.1.2 Identifiant d'algorithmes

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

7.1.3 Formes de noms

Les formes de noms respectent les exigences du § 3.1.1 pour l'identité des porteurs et de l'AC qui est portée dans les certificats émis par l'AC.

7.1.4 Identifiant d'objet (OID) de la Politique de Certification

Certificat d'authentification

Les certificats porteurs émis par l'AC Personnes 4 contiennent l'OID de la PC qui est : 1.2.250.1.120.4.2.1.1.

Certificat de signature

Les certificats porteurs émis par l'AC Personnes 4 contiennent l'OID de la PC qui est : 1.2.250.1.120.4.3.1.1.

7.1.5 Extensions propres à l'usage de la politique

Sans objet

7.1.6 Syntaxe et sémantique des qualificateurs de politique

Sans objet

7.1.7 Interprétation sémantique de l'extension critique « Certificate Policies »

Sans objet

7.2 Profil des LCR

7.2.1 LCR et champs d'extensions des LCR

Les caractéristiques des LCR sont :

Caractéristiques d'une LCR :	Durée de validité : 6 jours Périodicité de mise à jour : Au moins 1 fois toutes les 24 heures Version de la CRL (v1 ou v2) : v2 Extensions : Numéro de la CRL et AKI URL de publication (http) : adresse variable indiquée dans chaque certificat de porteur.

NB : le certificat contient le champ également le champs « expiredCertsOnCR »

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Ainsi que le précise l'article 8 de l'[Ordonnance], lorsqu'une autorité administrative (AA) met en place un système d'information, elle détermine les fonctions de sécurité nécessaires pour protéger ce système. Pour les fonctions de sécurité traitées par le [RGS], elle fixe le niveau de sécurité requis parmi les niveaux prévus et respecte les règles correspondantes.

Dans le cadre de la présente PC, le niveau de sécurité choisi par le MJ est le niveau (***).

Ainsi que le précise l'article 8 de l'[Ordonnance], les actes des autorités administratives qui font l'objet d'une signature électronique doivent être signés au moyen d'un procédé, conforme aux règles du [RGS] mentionné au I de l'article 9, qui permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte.

Dans le cadre de la présente PC, des certificats à usage de signature sont délivrés pour signer et vérifier des actes. Le niveau de sécurité choisi par le MJ pour ces certificats est le niveau (***).

Le [RGS] liste les règles que les prestataires de service de certification électronique (PSCE) délivrant des certificats électroniques de type signature électronique ou authentification doivent respecter. Les documents de référence du RGS, pour ce qui concerne les certificats objets de cette PC, sont au nombre de trois :

- RGS_A_2 : RGS_v-2-0_A2.pdf
- RGS_A_4 : RGS_v-2-0_A4.pdf
- RGS_B_1 : RGS_v-2-0_B1.pdf

Le RGS v2.0 a été rendu officiel par arrêté du Premier ministre du 13 juin 2014 [Arrêté130614].

L'article 23 du décret du décret n° 2010-112 du 2 février 2010 [Décret RGS] précise que les autorités administratives doivent obtenir la validation de leurs certificats électroniques et de ceux de leurs agents au plus tard dans les trois ans à compter de la publication de l'arrêté du 6 mai 2010 [Arrêté060510] (version 1.0 du RGS).

La version 2.0 du RGS s'applique aux autorités administratives de manière concomitante en application des mesures de transitions suivantes :

- Les certificats électroniques et les contremarques de temps conformes aux annexes de la version 1.0 du RGS pourront continuer à être émis jusqu'au 30 juin 2015 ;
- Les autorités administratives devront accepter ces certificats électroniques et ces contremarques de temps pendant leur durée de vie, avec un maximum de trois ans ;
- Les autorités administratives doivent accepter les certificats électroniques et les contremarques de temps conformes aux annexes de la version 2.0 du RGS à compter du 1er juillet 2015.

Le présent chapitre ne traite pas des audits effectués par les organismes qui procèdent à la qualification des prestataires de services de confiance dans le but d'obtenir la validation des certificats électroniques des agents de l'ANTS. La compétence de ces organismes est appréciée par l'ANSSI à partir d'un audit des moyens, des ressources et de l'expérience de l'organisme, cf. [RGS_C].

Le présent chapitre traite uniquement des audits et des évaluations de la responsabilité de l'AC afin de s'assurer que l'ensemble de son IGC est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

8.1 Fréquences et / ou circonstances des évaluations

Le responsable de l'exploitation des composantes de l'AC demande l'approbation de l'AA pour toute modification jugée comme étant une perte de la conformité avec la présente PC et la DPC qu'il met en œuvre.

L'AA se doit de prévenir les IGC avec lesquelles des accords sont conclus dans la mesure où ces modifications peuvent affecter ces accords ou le niveau de sécurité offert par l'IGC.

Le responsable de l'exploitation des composantes d'IGC demande l'approbation du responsable de l'AC Personnes pour le ministère de la justice pour toute modification jugée comme étant une perte de la conformité avec la présente PC et la DPC qu'il met en œuvre.

L'AC procède ou fait procéder sur l'ensemble des composantes de l'IGC à :

- Un audit interne de conformité tous les ans ;
- Des audits techniques tous les deux ans.

Pour maintenir sa qualification RGS au niveau (***), l'AC fait réaliser un audit de conformité tous les ans, par une société accréditée par le COFRAC.

8.2 Identités / qualifications des évaluateurs

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

8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit n'appartient pas à l'entité opérant la composante contrôlée, quelle que soit cette composante, elle est dûment autorisée à pratiquer les contrôles visés.

8.4 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 définis

dans la présente PC et dans la DPC associée, ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend un avis au responsable d'exploitation et à l'AC Personnes 4 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 au responsable d'exploitation 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 le responsable d'exploitation et doit respecter ses politiques de sécurité internes.
- En cas de résultat "À confirmer", le responsable d'exploitation remet à la composante un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, le responsable d'exploitation confirme à la composante contrôlée la conformité aux exigences de la présente PC et la DPC.

8.6 Communication des résultats

Les résultats des contrôles de conformité sont communiqués à la composante contrôlée ainsi qu'à l'AC Personnes.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

Sans objet.

9.2 Responsabilité financière

Le responsable de l'ACR pour le ministère de la justice s'engage à respecter la présente PC. Toute condition supplémentaire non portée dans ce document ne pourra être valablement considérée comme une obligation de l'ACR du ministère de la justice.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations suivantes (liste non exhaustive) sont considérées comme confidentielles :

- Les clés privées des certificats d'AC et des porteurs de certificats ;
- Les données d'activation associées à une bi-clé cryptographique ;
- Les journaux d'événements des composantes d'IGC ;
- Les rapports d'audits, et plus globalement le dossier de sécurité ;
- Les informations techniques relatives à la sécurité des fonctionnements des modules cryptographiques ;
- Les informations techniques relatives à la sécurité des fonctionnements de certaines composantes d'IGC ;
- La DPC et les procédures associées ;
- Les éléments constitutifs du dossier d'homologation ;
- Les dossiers d'enregistrement des porteurs ;
- Les causes de révocation.

9.3.2 Informations hors du 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.

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'IGC respecte la législation et la réglementation en vigueur sur le territoire français.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel qui est effectuée par l'AC du ministère de la justice sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi informatique et libertés [CNIL] et le règlement européen RGPD.

9.4.2 Informations à caractère personnel

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

- Données d'identification du porteur (hors celles figurant dans le certificat) ;
- Demande (renseignée) de certificat ;
- Demande (renseignée) de révocation ;
- Motif de la révocation.

Les données enregistrées dans PGCA servent exclusivement à la sécurité et la gestion de la carte agent et ne sont conservées que pendant la durée de vie de cette carte. Pour exercer les droits Informatique et Libertés et pour toute information sur ce dispositif ou pour toute question ou réclamation, le porteur peut écrire à l'adresse suivante : referents-caj.depm-sg@justice.gouv.fr qui transmettra au délégué à la protection des données (DPO), ainsi qu'au Haut Fonctionnaire de Défense et de Sécurité : hfds@justice.gouv.fr. *Ces mentions figurent sur les CGU*

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

L'AEC, l'AED, le CPS et l'AC traitent et protègent toutes les données à caractère personnel de manière à ce que seuls des personnels dans des rôles de confiance (internes ou autorités judiciaires) y aient accès, selon la présente PC.

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [CNIL] et la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [LCEN] s'applique au contenu de tous les documents collectés, détenus ou transmis par l'AC dans le cadre de la délivrance d'un certificat.

Les porteurs disposent d'un droit d'accès et de rectification des données collectées par l'AC, l'AEC ou l'AED pour l'émission du certificat et la gestion de son cycle de vie. Ce droit peut s'exercer auprès du ministère de la justice.

Toutes les données collectées et détenues par l'AC sont considérées comme confidentielles, hormis les données figurant dans le certificat.

En vertu des articles 323-1 à 323-7 du Code pénal applicable lorsqu'une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc. Les peines encourues varient de 1 à 10 ans d'emprisonnements assortis d'une amende allant de 15.000 à 300.000 euros pour les personnes morales.

9.4.5 Notification et consentement d'utilisation des données personnelles

Aucune des données à caractère personnel fournies par un porteur ne peut être utilisée par l'AC, pour une autre utilisation que celle définie dans le cadre de la présente PC, sans consentement exprès et préalable de la part du porteur. Ce consentement est considéré comme obtenu lors de la soumission de la demande de certificat et du fait de l'acceptation par le porteur du certificat émis par l'AC (en accord avec la présente PC) au titre de l'utilisation par les UC.

Les composantes d'IGC et les porteurs disposent d'un droit d'accès et de rectification des données collectées par l'IGC. Ce droit peut s'exercer auprès de l'AC Personnes 4. Les opérations demandées par l'AC ne doivent pas porter atteinte à l'intégrité de l'ensemble des données propres aux opérations mise en œuvre pour la gestion de son certificat.

9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

L'AC agit conformément aux réglementations européenne et française et dispose de procédures pour permettre l'accès des autorités judiciaires aux données à caractère personnel.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Les informations relatives à une personne définies comme confidentielles au § 9.4.2 ne peuvent être divulguées qu'à leur propriétaire ou à un tiers habilité au niveau adéquat.

L'AC s'oblige à obtenir l'accord du ministère de la justice pour transférer ses données à caractère personnel dans le cas d'un transfert d'activité tel qu'il est décrit au § 5.8.

9.5 Droits relatifs à la propriété intellectuelle et industrielle

La législation et de la réglementation en vigueur sur le territoire français est applicable.

9.6 Interprétations contractuelles et garanties

L'AC a pour obligation de :

- Respecter et appliquer la PC et la DPC,
- Se soumettre aux contrôles de conformité effectués, d'une part par l'équipe d'audit mandatée par l'AC et, d'autre part par l'organisme de qualification,
- Respecter les clauses qui la lient aux porteurs et aux utilisateurs de certificats,
- Documenter les procédures internes de fonctionnement,
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elle s'engage dans des conditions garantissant qualité et sécurité.

9.6.1 Autorités de Certification

L'AC s'assure que toutes les exigences détaillées dans la présente PC et la DPC associée, sont satisfaites en ce qui concerne l'émission et la gestion de certificats.

L'AC est responsable du maintien de la conformité aux procédures prescrites dans la présente PC. L'AC fournit tous les services de certification en accord avec sa DPC. Les obligations communes aux composantes de l'AC sont :

- De protéger les clés privées et leurs données d'activation en intégrité et confidentialité ;
- De n'utiliser ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles ils ont été générés et avec les moyens appropriés, comme spécifié dans la DPC ;
- De respecter et appliquer les dispositions de la partie de la DPC qui les concerne ;
- De documenter ses procédures internes de fonctionnement afin de compléter la DPC ;
- De mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC ;
- De faire certifier la clé publique, correspondante à sa clé privée, par l'AC Justice ;
- D'apporter les mesures nécessaires et suffisantes à la correction des non-conformités détectées dans les audits, dans les délais préconisés par les auditeurs ;
- De communiquer toutes les informations utiles, d'une part à l'équipe d'audit mandatée par l'AC et, d'autre part à l'organisme de qualification.

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.

9.6.2 Service d'enregistrement

Les obligations découlent des obligations pertinentes de l'AC du chapitre § 0 en se restreignant aux services qu'elle met en œuvre dans le cadre de cette PC. Les obligations communes aux composantes de l'AE sont :

- De respecter et appliquer les dispositions de la partie de la DPC qui les concerne ;
- De documenter ses procédures internes de fonctionnement afin de compléter la DPC ;
- De mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC ;
- D'assurer l'information des agents auxquelles elle délègue, concernant leurs rôles et responsabilités, et le traitement des informations à caractère personnel ou confidentielles, conformément à la présente PC ;
- D'apporter les mesures nécessaires et suffisantes à la correction des non-conformités détectées dans les audits, dans les délais préconisés par les auditeurs ;
- De communiquer toutes les informations utiles, d'une part à l'équipe d'audit mandatée par l'AC et, d'autre part à l'organisme de qualification.

9.6.3 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
- Informer l'AC de toute modification concernant les informations contenues dans son certificat
- S'engager à ne pas prêter sa carte et à la conserver constamment sous sa garde ;
- S'engager à prendre toutes les précautions pour les données d'activation qu'il détient ne soient pas divulguées ;
- S'engager à rendre sa carte à sa hiérarchie en cas de cessation d'activité ou à remettre sa carte à la demande de sa hiérarchie ;
- S'engager à ne s'authentifier au moyen de sa carte que sur les systèmes d'information en relation avec son activité professionnelle au sein du ministère de la justice ;
- S'engager à ne signer les décisions judiciaires que sur des applications diffusées par le ministère de la justice, sur le réseau privé virtuel justice et sur le poste de travail fourni par le MJ et dans l'enceinte des locaux du ministère ;
- En cas de perte ou vol de leur carte ou bien de divulgation d'un PIN, et dès la découverte du vol ou de la perte, s'engager à en faire la déclaration auprès du service qui lui a remis sa carte ou sur le site prévu à cet effet (https://justice-crd.cms.plateforme-cartes-agents.rie.gouv.fr/cms-fo/page/username-login.xhtml via le RIE ou https://justice-crd.cms.plateforme-cartes-agents.ingroupe.com/cms-fo/page/usernamelogin.xhtml via Internet) ;
- En cas de perte ou vol de leur carte et dès la découverte du vol ou de la perte s'engagent à demander la révocation des certificats contenus dans la carte dans les plus brefs délais ;
- En cas de divulgation d'un code PIN et dès la découverte la divulgation d'un code PIN, s'engagent à en changer dans les plus brefs délais.
- S'assurer que les données transmises au MJ sont à jour ;
- Avertir son AEC de toute modification concernant les informations contenues dans son certificat.

La relation entre le porteur et l'AC est formalisée dans les Conditions Générales d'Utilisation.

9.6.4 Utilisateurs de certificats

Les utilisateurs de certificats doivent :

- Vérifier et respecter l'usage (authentification ou signature électronique) pour lequel un certificat a été émis ;
- Pour chaque certificat du chemin de certification, depuis le certificat du porteur jusqu'à un certificat de l'AC Racine 2, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- Utiliser le certificat auto-signé de l'AC Racine 2 qui est disponible sur le site du ministère à l'adresse http://www.justice.gouv.fr/igc/ants.
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC publiée sur le site du ministère à l'adresse Intranet http://www.justice.gouv.fr/igc/ants.

9.6.5 Autres participants

La DPC précisera les exigences si besoin est.

9.7 Limite de garantie

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

- L'identification et l'authentification des porteurs avec les certificats générés par l'AC ;
- La gestion des certificats correspondant et des informations de validité des certificats selon la présente PC.

Aucune autre garantie ne peut être mise en avant par l'AC, les porteurs et les UC dans leurs accords contractuels (s'il en est).

9.8 Limites de responsabilité

L'AC décline toute responsabilité à l'égard de l'usage des certificats émis par elle ou des bi-clés publiques/privées associées dans des conditions et à des fins autres que celles prévues dans la présente PC.

Seule la responsabilité de l'État peut être mise en cause en cas de non-respect des dispositions prévues par les présentes.

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

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 politique 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 1218 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 n'est en aucun cas responsable des préjudices indirects subis par les entités utilisatrices, ceux-ci n'étant pas préqualifiés par les présentes.

En cas de prononcé d'une quelconque responsabilité de l'AC, les dommages, intérêts et indemnités à sa charge toutes causes confondues, et quel que soit le fondement de sa responsabilité, sont limités par certificat à la somme prévue au titre de limite de responsabilité dans les conditions générales d'utilisation applicable audit certificat.

Pour les certificats de signature, l'AC est responsable du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas précisés par l'article 33 de la [LCEN].

9.9 Indemnités

Sans Objet

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

La présente PC devient effective une fois approuvée par le ministère de la justice. La PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

La publication d'une nouvelle version de la présente PC peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer la PC qu'elle met en œuvre.

En fonction de la nature et de l'importance des évolutions apportées à la PC, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

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

9.10.3 Effets de la fin de validité et clauses restant applicables

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

9.11 Notifications individuelles et communications entre les participants

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

- Au plus tard un mois avant le début de l'opération, à 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'ACR et de ses différentes composantes.
- Au plus tard un mois après la fin de l'opération, à en informer l'organisme de qualification.

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

L'AC s'engage à contrôler que tout projet de modification de sa PC reste conforme aux exigences de la présente PC Type et des éventuels documents complémentaires du [RGS]. L'AC pourra réviser sa PC et/ou sa DPC chaque fois qu'une évolution remarquable de l'état de l'art le justifie.

9.12.2 Mécanisme et période d'information sur les amendements

Le ministère de la justice 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.

9.12.3 Circonstances selon lesquelles un OID doit être changé

L'OID de la PC est inscrit dans les certificats émis. Toute évolution d'une 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) se traduira par un changement de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

9.13 Dispositions concernant la résolution de conflits

Les conflits entre des personnes appartenant au ministère de la justice sont traités au niveau du secrétariat général du ministère de la justice. À défaut, ils sont du ressort du Tribunal Administratif.

9.14 Juridictions compétentes

Le Tribunal Administratif compétent est soit celui du plaignant soit celui du défendant.

9.15 Conformité aux législations et réglementations

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

L'environnement législatif pour la mise en œuvre de l'AC Personnes 4 est notamment constitué des textes de lois et règlements suivants :

- La directive 1999/93/CE du Parlement européen et du Conseil en date du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques [Directive] ;
- L'article 1367 du Code Civil relatif à la signature électronique [CC1367] ;
- Le décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique
- L'article 801-1 du CPP [CPP801] ;
- La loi n° 2004-575 du 21 juin 2004 modifiée, pour la confiance dans l'économie numérique, et en particulier l'article 33 [LCEN] ;
- La loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés [CNIL] ;
- L'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives [Ordonnance] ;
- L'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation [Arrêté260704] ;
- Le décret n°2010-112 du 2 février 2010 pris pour application des articles 9 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives [Décret RGS] ;
- L'arrêté du 10 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques [Arrêté060510].
- au règlement n°910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS ».
- le règlement européen Règlement Général sur la Protection des Données no 2016/679 du 14 avril 2016, dit RGPD (*ou encore GDPR, de l'anglais General Data Protection Regulation)*

9.16 Dispositions diverses

9.16.1 Accord global

Les éventuels accords passés avec les partenaires doivent être validés par le ministère de la justice.

9.16.2 Transfert d'activités

Voir § 5.8.

9.16.3 Conséquences d'une clause non valide

Les conséquences, le cas échéant, seront traitées en fonction de la législation en vigueur.

9.16.4 Application et renonciation

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

9.16.5 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement à la fois imprévisible, irrésistible (insurmontable) et échappant au contrôle des personnes concernées.

9.17 Autres dispositions

Le cas échéant, la DPC en fournira les détails.

10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 Réglementation

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
[Règlement]	DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FRA&toc=OJ:L:2016:119:TOC
[eIDAS]	Règlement n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (Publié au JOUE du 28 août 2014) : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32014R0910
[CPP801]	Article 801-1 du code de procédure pénale
[CC1367]	Article 1367 du Code Civil relatif à la signature électronique
[Décret RGS]	Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'[Ordonnance]. Disponible en ligne : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&dateTexte=vig
[RGS]	Référentiel Général de Sécurité – Version 2.0 http://www.ssi.gouv.fr/administration/reglementation/administration-electronique/le-referentiel-general-de-securite-rgs//
[Décret2017-1416]	Décret n°2017-1416 du 28 septembre 2017 relatif à la signature électronique. Disponible en ligne : https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=82E8198684B5A264A1A1D5791267DA1A.tplgfr38s_3?cidTexte=LEGITEXT000035678038&dateTexte=20170930&categorieLien=cid#LEGITEXT000035678038
[Arrêté260704]	Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation. Disponible en ligne : http://www.legifrance.gouv.fr/./affichTexte.do?cidTexte=JORFTEXT000000441678&dateTexte=vig
[Arrêté060510]	Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques. Disponible en ligne : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022220429&fastPos=1&fastReqId=1704766824&categorieLien=id&oldAction=rechTexte
[LCEN]	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
[eIDAS]	Règlement n°910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS ».
RGPD	**Règlement général sur la protection des données n° 2016/679**, du 14 avril 2016 (ou encore **GDPR**, de l'anglais *General Data Protection Regulation)*

10.2 Documents techniques

Renvoi	Document
[RGS]	Référentiel Général de Sécurité – Version 2.0 http://www.ssi.gouv.fr/administration/reglementation/administration-electronique/le-referentiel-general-de-securite-rgs//
[RGS_v-3-0_A1]	RGS –fonctions de sécurité basées sur l'emploi de certificats électroniques
[RGS_v-3-0_A2]	RGS – Politique de Certification Type Authentification – Version 2.3
[RGS_v-3-0_A3]	RGS - PC Type certificats électroniques de services applicatifs
[RGS_v-3-0_A4]	RGS - Profils de Certificats - LCR - OCSP et algorithmes crypto
[RGS_v-3-0_A5]	RGS - Politique d'Horodatage Type
[RGS_v-2-03_B1]	RGS – Mécanismes cryptographiques
[RGS_v-2-0_B2]	RGS - Gestion des clés cryptographiques
[X.509]	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. 6 th Edition. Version de novembre 2008. Disponible à l'adresse : http://www.itu.int/rec/T-REC-X.509
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003. Disponible à l'adresse : http://www.ietf.org/rfc/rfc3647.txt
[RFC5280]	IETF - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – mai 2008 Disponible à l'adresse : http://www.ietf.org/rfc/rfc5280.txt

11 ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC

11.1 Exigences sur les objectifs de sécurité

Le module cryptographique (HSM ou RCM), utilisé par l'AC pour générer et mettre en œuvre ses clés d'authentification (pour la génération des certificats électroniques, des LCR) et ses clés de signature (pour la génération des certificats électroniques, des LCR) répond aux exigences de sécurité suivantes :

- Assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie,
- Être capable d'identifier et d'authentifier ses utilisateurs,
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné,
- Être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur,
- Permettre de signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance des clés privées,
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité,
- Dans le cadre des fonctions de sauvegarde et de restauration des clés privées de l'AC, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

11.2 Exigences sur la qualification

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

12 ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF DE CREATION DE SIGNATURE

12.1 Exigences sur les objectifs de sécurité

12.1.1 Authentification

Le dispositif d'authentification, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée répond aux exigences de sécurité suivantes :

- Lorsque la bi-clé de signature du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.
- Détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- Garantir la confidentialité et l'intégrité de la clé privée ;
- Générer une signature numérique qui ne peut être falsifiée sans la connaissance de la clé privée (dans la mesure où la fonction de hachage utilisée à l'extérieur du dispositif soit exempte de collisions et que le protocole d'authentification soit exempt de faiblesses et de possibilités de rejeu) ;
- Assurer la fonction d'authentification pour le porteur légitime uniquement en utilisant un code d'activation personnel et spécifique pour mettre en œuvre la fonction.

12.1.2 Signature

Le dispositif de création de signature, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, répond aux exigences de sécurité suivantes :

- Lorsque la bi-clé de signature du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.
- Détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- Garantir la confidentialité et l'intégrité de la clé privée ;
- Générer une signature numérique qui ne peut être falsifiée sans la connaissance de la clé privée (dans la mesure où la fonction de hachage utilisée à l'extérieur du dispositif soit exempte de collisions et que le format de signature électronique soit exempt de faiblesses et de possibilités d'anti-datation) ;
- Assurer la fonction de signature électronique pour le porteur légitime uniquement en utilisant un code d'activation personnel et spécifique pour mettre en œuvre la fonction.

Les dispositifs d'authentification des porteurs sont des cartes à puce respectant le socle commun IAS (Identification, Authentification, Signature) et permettent de répondre à l'ensemble de ces exigences de sécurité.

12.2 Exigences sur la qualification

12.2.1 Authentification

Le dispositif d'authentification utilisé par le porteur fait l'objet d'une qualification au niveau renforcé, selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 12.1.1 ci-dessus.

12.2.2 Signature

Le dispositif de création de signature utilisé par le porteur fait l'objet d'une qualification au niveau renforcé, selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 12.1.2 ci-dessus.