Politique de Certification de l'ACR Infrastructure Justice

CIRCUIT DE VALIDATION

Date application	Version	Objet	Rédaction	Vérification	Approbation
23/11/2018	1.0	Version applicable	Le 07/11/2018 L.Flament	Le 13/11/2018 L. Loffredo	Le 23/11/2018 AA-PEKIN

SIGNATURE D'APPROBATION DE l'AA-PEKIN

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA JUSTICE

Signature numérique de Autorité Administrative PEKIN
DN : cn=Autorité Administrative PEKIN, ou=0002 110010014, o=Ministere de la Justice, c=FR
Date : 2018.11.23 14:44:36 +01'00'

DIFFUSION Elargie ☒ Restreinte ☐ Contrôlée ☐ exemplaire n°

Pour action	
Pour information	

HISTORIQUE DES MODIFICATIONS

Date application	Version	Objet	Rédaction	Vérification	Approbation
	0.1	document initial	Le 11/07/2018 L.Flament	Le 20/07/2018 L. Loffredo	
	0.2	intégration des remarques du vérificateur	Le 24/07/2018 L. Flament		
	0.3	séparation PC/DPC	Le 07/11/2018 L.Flament	Le 15/11/2018 L. Loffredo	

SOMMAIRE

1. INTRODUCTION

1.1. GÉNÉRALITÉS

Le Ministère de la Justice possède une Infrastructure de Gestion de Clés (IGC) afin de gérer les certificats d'AC utilisés dans le cadre de ses projets internes. Cette IGC est appelée PEKIN.

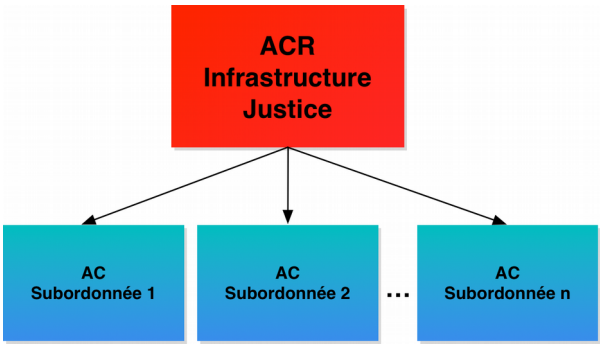
Cette IGC est constituée d'une autorité racine dénommée « ACR Infrastructure Justice » dont le rôle est de signer des certificats pour des AC filles. l'« ACR Infrastructure Justice » est une autorité qui est hors ligne de part le fait que son seul rôle est la délivrance de certificats d'autorités et la signature de la liste des autorités révoquées.

Les AC signées par l'« ACR Infrastructure Justice » pourront à leur tour être en ligne ou hors ligne en fonction de leur usage.

Le présent document constitue la Politique de Certification (PC) de l'« ACR Infrastructure Justice ». Il décrit les engagements minimums que le Ministère de la Justice respecte dans la délivrance et la gestion des certificats de l'« ACR Infrastructure Justice » tout au long de son cycle de vie.

Le certificat de L'« ACR Infrastructure Justice » est auto-signé et permet la signature des Listes des Autorités Révoquées (LAR) et des certificats des AC subordonnées, qui délivrent des certificats d'AC ou finaux.

La hiérarchie d'autorités de certification de l'IGC PEKIN est donc la suivante :



La structure de la présente PC est conforme à la RFC 3647 « X.509 Public Key Infrastructure Certificate Policy Certification Practice Statement Framework ».

1.2. IDENTIFICATION DU DOCUMENT

La présente PC est dénommée Politique de Certification de l'ACR Infrastructure Justice et est la propriété du Ministère de la Justice. Elle peut être identifiée par son numéro d'IDentifiant d'Objet (OID – cf. entête de chaque page). D'autres éléments, plus explicites, comme le nom, le numéro de version et la date de mise à jour permettent également de l'identifier sans ambiguïté.

Le numéro d'OID du présent document est : 1.2.250.1.120.3.1.1.1

1.3. DÉFINITIONS ET ACRONYMES

1.3.1. ACRONYMES

Les acronymes utilisés dans la présente PC sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
ACR	Autorité de Certification Racine
ACS	Autorité de Certification Subordonnée
AE	Autorité d'Enregistrement
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CEN	Comité Européen de Normalisation
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
IGC	Infrastructure de Gestion de Clés
IJ	Infrastructure Justice
KC	Cérémonie des clés (Key Ceremony)
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
MJ	Ministère de la Justice
OC	Opérateur de Certification
OID	Object Identifier
PC	Politique de Certification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure – X 509
PP	Profil de Protection
PSCE	Prestataire de Services de Certification électronique
RC	Responsable de Certificat
RSA	Rivest Shamir Adelman

SSI Sécurité des Systèmes d'Information

UC Utilisateur de Certificat

URL Uniform Resource Locator

1.3.2. DÉFINITIONS

Les termes utilisés dans la présence PC sont les suivants :

Applications utilisatrices : Services applicatifs exploitant les certificats émis par l'AC, afin de délivrer des certificats aux utilisateurs de certificats pour des besoins d'authentification, de chiffrement ou de signature ou des besoins d'authentification ou de cachet pour des serveurs dont elle a la gestion.

Authentification : L'authentification vise à renforcer selon le besoin, le niveau de confiance entre l'identifiant et la personne associée. On distingue l'authentification dite « faible » (ex : mot de passe) et l'authentification dite « forte » (ex :carte à puce associée à un code PIN).

Autorité Administrative (AA) : entité responsable de l'ensemble des fonctions de l'IGC PEKIN avec pouvoir décisionnaire, L'AA-PEKIN est responsable de toutes les ACs du Ministère de la Justice qu'elle délivre.

Autorité d'Enregistrement (AE) : cf. Autorité d'Enregistrement (AE)

Autorité de Certification (AC) : entité qui délivre et est responsable des certificats électroniques signés en son nom. L'AA-PEKIN assure elle-même l'exploitation de l'IGC PEKIN, elle dispose de locaux sécurisés, du personnel et de l'infrastructure technique qui lui permettent de réaliser l'ensemble des tâches de gestion des certificats.

Bi-clé : Couple clé privée/publique utilisé dans des algorithmes de cryptographie asymétrique.

Cérémonie des Clés : réunion spéciale des personnes autorisées pour générer le certificat d'une Autorité de Certification. La bi-clé de ce certificat doit être générée avec toutes les précautions nécessaires (voir la DPC) pour éviter sa compromission.

Certificat électronique : Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de la présente PC, le terme "certificat électronique" désigne uniquement un certificat délivré à une AC subordonnée et portant sur une bi-clé de signature, sauf mention explicite contraire.

Composante : Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

Déclaration des pratiques de certification (DPC) : Identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) 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.

Dispositif de protection des éléments secrets : Dispositif de stockage des éléments secrets remis au porteur ou au RC (exemples : clé privée, code PIN, etc). Il peut prendre la forme d'une carte à puce, d'une clé USB à capacités cryptographique ou se présenter au format logiciel (exemple : fichier PKCS#12).

Hardware Security Module : cf. Module matériel de sécurité

Infrastructure de Gestion de Clés (IGC) : Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication...

Mandataire de certification : cf. participants

Module matériel de sécurité : matériel dédié à la génération, au stockage et à la destruction d'éléments cryptographiques sensibles (clés privées, secrets). L'usage d'un Module matériel de sécurité rend très difficile la compromission des éléments qu'il contient (divulgation, altération) grâce à des protections physiques et cryptographiques.

Personne autorisée : cf. participants

PKIX : Groupe de travail de l'IETF (Internet Engineering Task Force) visant à faciliter la genèse d'IGC basées sur la norme X.509 pour des applications Internet. PKIX a produit des normes telles que les extensions de X.509 pour l'Internet, OCSP...

Politique de certification (PC) : - Ensemble de règles, identifié par un nom (OID), définissant 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. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Prestataire de services de certification électronique (PSCE) : 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 peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

Produit de sécurité : - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Public Key Infrastructure (PKI) : cf. IGC

Qualification d'un produit de sécurité : - Acte par lequel 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 [DécretRGS]. Le [RGS] précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

Responsable de certificat (RC) : cf. participants

Usager : Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques au sein du Ministère de la Justice. Selon le contexte, un usager peut être un porteur, un RC, un VC ou un utilisateur de certificats.

Utilisateur de certificat : cf. participants

1.4. ENTITÉS INTERVENANT DANS L'ACR INFRASTRUCTURE JUSTICE

1.4.1. AUTORITÉ DE CERTIFICATION (AC)

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuie pour cela sur une infrastructure technique de gestion de clés (IGC).

l'IGC PEKIN du Ministère de la Justice est constituée d'une AC racine unique « ACR Infrastructure Justice » dont le rôle est la délivrance exclusive de certificats d'AC subordonnées. De ce fait l'« ACR Infrastructure Justice » ne délivre par de certificats à des entités finales. De part le fait que l'« ACR Infrastructure Justice » est une autorité racine, son certificat est auto-signé et il représente la base de confiance de l'IGC PEKIN.

La mise en œuvre opérationnelle de l'« ACR Infrastructure Justice » est à la charge de l'Autorité Administrative de l'IGC PEKIN (AA-PEKIN) qui est responsable de l'ensemble des services de l'IGC et à le seul pouvoir décisionnaire pour cette IGC (définition des PC, vérification des conformités des DPC vis à vis des PC pour chaque AC subordonnée).

Les services rendus par l'« ACR Infrastructure Justice » correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats. Dans la présente PC nous distinguons les services suivants directement ou indirectement rendus par l'« ACR Infrastructure Justice » :

1.4.1.1. ENREGISTREMENT

Cette fonction vérifie et valide les informations d'identification du futur responsable du certificat (RC) et du service applicatif ou du porteur auquel le certificat doit être rattaché, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. L'AE a également en charge, lorsque cela est nécessaire, la revérification des informations du RC et du service applicatif ou du porteur lors du renouvellement du certificat.

1.4.1.2. GÉNÉRATION DES CERTIFICATS

Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'AE et de la clé publique de l'AC subordonnée provenant du RC, soit de la fonction de génération des éléments secrets du service, si c'est cette dernière qui génère la bi-clé de l'AC subordonnée.

1.4.1.3. GÉNÉRATION D'ÉLÉMENTS SECRETS

Cette fonction génère les éléments secrets du service à destination du RC, et les prépare en vue de leur remise au RC. Les éléments secrets, dans le cadre de la présente PC, peuvent directement être la bi-clé de l'AC subordonnée, des codes ou clés temporaires permettant au RC de mener à distance le processus de génération / récupération du certificat électronique de l'AC subordonnée.

Il est à noter que la présente PC ne supporte la génération de la bi-clé pour le compte de l'AC subordonnée que si cette dernière se retrouve dans l'incapacité de la générée pour des raisons techniques ou si l'AA-PEKIN est en charge de la gestion de l'AC subordonnée qui sera délivrée. Dans tous les cas, la bi-clé devra être générée en respectant les exigences définies aux chapitres Génération et installation de bi-clés et Standards et mesures de sécurité pour les modules cryptographiques.

1.4.1.4. REMISE AU RC

Dans le cas d'un certificat pour une AC subordonnée, cette fonction remet au RC au minimum le certificat de l'AC subordonnée ainsi que, le cas échéant, les autres éléments fournis par l'AC (clé privée de l'AC subordonnée, codes d'activation, clé de protection de la clé privée,...).

1.4.1.5. PUBLICATION DES CERTIFICATS

Cette fonction met à disposition des Utilisateurs de Certificats du Ministère de la Justice (UC-MJ) les éléments suivants :

- certificat de l'« ACR Infrastructure Justice » ;
- conditions générales d'utilisation de l'« ACR Infrastructure Justice » ;
- politiques et pratiques de l'« ACR Infrastructure Justice » ;
- toute autre information pertinente, hors informations d'état des certificats.

1.4.1.6. RÉVOCATION DES CERTIFICATS

La révocation des certificats des AC subordonnées de l'« ACR Infrastructure Justice » est assurée par l'AE qui se charge de la vérification des informations d'identification du Responsable du Certificat et de la validité du formulaire de révocation de certificat d'autorité conformément aux notices décrivant le contenu attendu pour ce dernier. Si la demande est valide, l'AE demande à l'AA-PEKIN de révoquer le certificat et une nouvelle Liste des Autorités Révoquées (LAR) est générée par cette dernière.

1.4.1.7. INFORMATION SUR L'ÉTAT DES CERTIFICATS

Cette fonction, assurée par l'AA-PEKIN, gère la mise à disposition aux utilisateurs de certificats des informations sur l'état des certificats des autorités signés par l'« ACR Infrastructure Justice » (révoqués, suspendus, etc.). Ce service est rendu par la publication de la LAR de l'« ACR Infrastructure Justice » à intervalles réguliers ou dès lors qu'une opération de révocation est effectuée.

1.4.1.8. PARTICIPANTS

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

- **Mandataire de certification (MC) :** dans le cadre de la présente PC, le rôle de MC est confondu avec celui de RC (voir ci-dessous) ;
- **Responsable de certificat (RC) :** Le responsable de certificat est désigné par et placé sous la responsabilité de l'entité cliente qui dans la présente PC ne peut-être qu'un service du Ministère de la Justice. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et les attributs des services applicatifs ou des porteurs de cette entité ;

- **Utilisateur de Certificat (UC) :** Entité ou personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur de cachet ou d'authentification serveur provenant du service applicatif auquel le certificat est rattaché, ou pour établir une clé de session, ou pour vérifier une signature électronique ou une valeur d'authentification provenant du porteur du certificat ou chiffrer des données à destination du porteur du certificat ;
- **Personne autorisée :** Personne autre que le RC et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, ...).

1.4.2. AUTORITÉ D'ENREGISTREMENT (AE)

l'AE est en charge de la vérification des informations d'identification du Responsable du Certificat et de la validité du formulaire de demande de certificat d'autorité conformément aux notices décrivant le contenu attendu pour ce dernier. Si la demande est valide, elle est transmisse au service de génération des certificats. De part le fait que les demandes concernent uniquement des AC subordonnées, c'est l'AA-PEKIN qui est la seule habilitée à traiter, approuver les demandes et effectuer le processus de génération du certificat d'AC demandé. De fait, le rôle d'AE de l'« ACR Infrastructure Justice » est de la responsabilité de l'AA-PEKIN.

Afin de mener à bien son rôle, l'AE assure les tâches suivantes :

- La prise en compte et la vérification des informations du RC ainsi que leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- La vérification que la version des formulaires reçus est bien celle actuellement autorisée ;
- La prise en compte et la vérification des informations de l'AC subordonnée ainsi que son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- La réalisation de la Cérémonie des Clés permettant la délivrance du certificat demandé qui est signé par l'« ACR Infrastructure Justice » ;
- L'archivage des dossiers de demande de certificat ;
- La conservation et la protection en confidentialité et intégrité des données personnelles d'authentification du RC ;
- La vérification des demandes de révocation de certificat.

1.4.3. RESPONSABLE DE CERTIFICATS

Dans le cadre de la présente PC, un RC ne peut être qu'une personne physique qui est responsable de l'utilisation du certificat électronique identifié dans le certificat et de la clé privée associée, pour le compte de l'entité également identifiée dans ce certificat. Le RC a un lien contractuel / hiérarchique / réglementaire avec cette entité.

Le RC respecte les conditions qui lui incombent et qui sont définies dans la présente PC et dans les CGU.

Le certificat de l'AC subordonnée étant attaché au service et non au RC, en cas de changement de RC, l'entité doit le signaler à l'« ACR Infrastructure Justice » préalablement sauf cas exceptionnel et lui désigner un successeur sans délai.

l'« ACR Infrastructure Justice » révoque les certificats pour lesquels il n'y a plus de RC explicitement identifié.

1.4.4. UTILISATEURS DE CERTIFICATS

Un utilisateur (ou accepteur) de certificats électroniques d'AC subordonnée peut être tout service applicatif, personne, usager devant valider un certificat émis par l'AC subordonnée pour le compte d'un service applicatif (authentification server, cachet serveur, horodatage, ...) ou d'une personne (authentification, signature, ...).

1.4.5. AUTRES PARTICIPANTS

1.4.5.1. COMPOSANTES DE L'IGC

La décomposition en fonctions de l'IGC est présentée au chapitre Autorité de Certification (AC). Les composantes de l'IGC mettant en œuvre ces fonctions seront présentées dans la DPC de l'AC.

1.4.5.2. MANDATAIRE DE CERTIFICATION

dans le cadre de la présente PC, le rôle de MC est confondu avec celui de RC.

1.5. USAGES DES CERTIFICATS

1.5.1. DOMAINES D'UTILISATION APPLICABLES

Les certificats générés par l'« ACR Infrastructure Justice » sont destinés aux AC subordonnées du Ministère de la Justice qu'elle fédère. Ces AC subordonnées peuvent être des Autorités de Certification « hors ligne » ou « en ligne ».

Les domaines d'utilisation des certificats internes de l'IGC se répartissent en trois catégories :

- la bi-clé et le certificat de l'« ACR Infrastructure Justice » (certificat auto-signé), utilisés pour signer les certificats des AC subordonnées rattachées à l'« ACR Infrastructure Justice », et signer la LAR de l'« ACR Infrastructure Justice » ;
- les bi-clés et les certificats d'AC Racine subordonnée pouvant délivrer à leur tour des certificats d'AC subordonnées. Ils sont signés par l'« ACR Infrastructure Justice », uniquement utilisés pour la signature d'AC subordonnées et directement sous le contrôle de l'AA-PEKIN au même titre que l'« ACR Infrastructure Justice » dans la mesure où ils sont considérés comme des AC Racine de niveau inférieur à l'« ACR Infrastructure Justice » ;
- les bi-clés et les certificats d'AC subordonnées signés par l'« ACR Infrastructure Justice ». Ils sont utilisés uniquement pour la signature des certificats utilisateurs finaux, chacun de ces certificats peut être utilisé sur le domaine défini dans le dossier de demande de chaque AC subordonnée et validé par l'AA-PEKIN.

Les administrateurs de l'AA-PEKIN disposent également de certificats nominatifs permettant d'effectuer diverses opérations internes à la gestion de l'IGC, notamment une authentification forte sur l'IGC afin de réaliser les différentes opérations qui leur incombent.

1.5.2. DOMAINES D'UTILISATION INTERDITS

L'utilisation des certificats émis par l'« ACR Infrastructure Justice » pour des usages autres que ceux prévus dans la présente PC sont interdits. Par conséquent, l'« ACR Infrastructure Justice » ne peut être tenue pour responsable d'une utilisation des certificats émis dans un cadre autre que celui prévu dans la présente PC. Par ailleurs, les certificats émis doivent être utilisés conformément aux lois en vigueur et applicables. l'« ACR Infrastructure Justice » respecte également ces restrictions d'usages et impose leur respect aux AC subordonnées qu'elle a signées.

A cette fin, l'AC publie à destination des RC et des utilisateurs potentiels des CGU qui peuvent être consultées sur le site du Ministère de la Justice http://www.justice.gouv.fr/igc/sdit avant toute demande de certificat ou toute

utilisation d'un certificat.

1.6.Gestion de la PC

1.6.1.Entité gérant la PC

L'AA-PEKIN est responsable de la validation et de la gestion de la présente PC.

1.6.2.Point de contact

l'AA-PEKIN est l'entité à contacter pour toutes questions relatives à la présente PC.

Autorité Administrative de l'IGC PEKIN :

Ministère de la Justice / Secrétariat Général / Services des Systèmes d'Information et de Communication

13 Place Vendôme

75042 Paris Cedex 01

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

L'AA-PEKIN a autorité et est responsable pour déterminer la conformité d'une DPC avec la présente PC.

L'AA-PEKIN a également autorité pour mandater des audits à des fins de contrôle.

1.6.4.Procédures d'approbation de la conformité de la DPC

La DPC traduit en termes technique, organisationnel et procédural les exigences de la PC en s'appuyant sur la politique de sécurité du Ministère de la Justice. L'AA-PEKIN s'assure que les moyens mis en œuvre et décrits dans la DPC répondent à ces exigences selon le processus d'approbation mis en place. Un contrôle de conformité de la DPC par rapport à la PC est effectué lors des audits internes ou externes réalisés.

Toute demande de mise à jour de la DPC suit également ce processus.

2. RESPONSABILITÉS CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIÉES

2.1. ENTITÉS CHARGÉES DE LA MISE À DISPOSITION DES INFORMATIONS

L'AA-PEKIN est en charge de la mise à disposition des informations devant être publiées à destination des utilisateurs de certificats.

2.2. INFORMATIONS DEVANT ÊTRE PUBLIÉES

Les informations suivantes sont publiées à destination des porteurs et utilisateurs de certificats :

- la présente politique de certification dans sa version en cours de validité :
  - http://www.justice.gouv.fr/igc/sdit/mj_pc_acr-infra_justice.pdf
- le certificat auto-signé de l'« ACR Infrastructure Justice » ;
  - http://www.justice.gouv.fr/igc/sdit/mj_acr-infra_justice.cer
- la LAR de l'« ACR Infrastructure Justice » :
  - http://www.justice.gouv.fr/igc/sdit/mj_arl-infrastructure.crl
- les Conditions Générales d'Utilisation liées au service de certification :
  - http://www.justice.gouv.fr/igc/sdit/mj_cgu_acr-infra_justice.pdf

Certain documents à destination du personnel du Ministère de la Justice (RC, ...) sont uniquement publiées sur le réseau interne du MJ. Se référer au chapitre correspondant de la DPC.

2.3. DÉLAIS ET FRÉQUENCES DE PUBLICATION

La présente PC et les documentations relatives aux demandes de certificat et de révocation sont publiées 24 heures sur 24 et 7 jours sur 7.

Les certificats d'AC sont publiés 24 heures sur 24 et 7 jours sur 7.

La LAR est publiée 24 heures sur 24 et 7 jours sur 7 avec une fréquence de mise à jour annuelle ou plus fréquemment à l'occasion de chaque Cérémonie des Clés d'une nouvelle AC subordonnée ou de la révocation d'une AC subordonnée.

Toute nouvelle version des informations et documents relatifs à l'« ACR Infrastructure Justice » fait l'objet d'une publication sous 4 heures afin d'assurer à tout moment une cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.

2.4. CONTRÔLE D'ACCÈS AUX INFORMATIONS PUBLIÉES

l'IGC PEKIN pouvant nécessiter une visibilité à l'extérieur du Ministère de la Justice, l'ensemble des informations publiées est constitué des documents au niveau « diffusion élargie ». Les documents référencés dans la présente PC/PDC qui sont d'un niveau différent, ne seront pas accessible aux utilisateurs. Le respect des niveaux de confidentialité des documents est du ressort de l'AA-PEKIN qui est en charge de la publication des ces informations.

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 de type mot de passe basé sur une politique de gestion stricte des mots de passe.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. NOMMAGE

3.1.1. TYPE DE NOMS

Les noms utilisés dans les certificats émis par l'« ACR Infrastructure Justice » sont conformes aux spécifications de la norme X.500. Dans chaque certificat X.509v3, le champ « issuer » (AC émettrice, soit l'« ACR Infrastructure Justice ») et le champ « subject » (AC subordonnée) sont identifiés par un « Distinguish Name ».

Les noms utilisés dans le certificat de l'« ACR Infrastructure Justice » sont définis dans Profil du certificat de l'« ACR Infrastructure Justice ».

3.1.2. NÉCESSITÉ D'UTILISATION DE NOMS EXPLICITES

Les noms utilisés dans les champs « issuer » et « subject » des certificats d'AC subordonnée et du certificat auto-signé de l'« ACR Infrastructure Justice » sont explicites pour le Ministère de la Justice et toute personne devant les utiliser. Ainsi, ils identifient sans ambiguité le Ministère de la Justice comme émetteur de ces certificats. les champs « issuer » et « subject » contiennent en particulier le code SIREN du Ministère de la Justice.

3.1.2.1. CERTIFICAT DE L'« ACR INFRASTRUCTURE JUSTICE »

Le format exact du DN du certificat de l'« ACR Infrastructure Justice » est le suivant pour les champs « issuer » et « subject » :

Champ du certificat	Valeur
Issuer DN	C = FR O = Ministere de la Justice OU = 0002 110010014 CN = ACR Infrastructure Justice
Subject DN	C = FR O = Ministere de la Justice OU = 0002 110010014 CN = ACR Infrastructure Justice

3.1.2.2. CERTIFICAT D'AC SUBORDONNÉE

Le format exact du DN d'un certificat d'AC subordonnée, signé par l'« ACR Infrastructure Justice », est le suivant pour les champs « issuer » et « subject » :

Champ du certificat	Valeur
Issuer DN	C = FR O = Ministere de la Justice OU = 0002 110010014 CN = ACR Infrastructure Justice

Subject DN	C = FR O = Ministere de la Justice OU = 0002 110010014 CN = <identifiant de l'AC subordonnée>

3.1.3. Pseudonymisation des AC

La pseudonymisation des certificats d'AC de l'IGC PEKIN est interdite.

3.1.4. Règles d'interprétation des différentes formes de nom

Aucune interprétation n'est faite sur le nom des certificats.

3.1.5. Unicité des noms

L'« ACR Infrastructure Justice » assure l'unicité des noms distinctifs des ACs générés dans son domaine. Des moyens organisationnels et techniques sont mis en œuvre afin de faciliter l'assurance de garantie de cette unicité (vérification durant le processus d'enregistrement, création de l'AC sur la base de son CN, impossibilité d'enregistrement d'un CN en doublon).

En cas de litige sur l'utilisation d'un nom pour un certificat d'AC subordonnée, l'« ACR Infrastructure Justice » a la responsabilité de résoudre le litige en question et est seule décisionnaire dans ce cas précis.

3.1.6. Identification, authentification et rôle des marques déposées

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

L'« ACR Infrastructure Justice » est responsable de l'unicité des noms d'AC subordonnées pour les certificats qu'elle délivre, et par conséquent responsable de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession de la clé privée

La bi-clé de l'« ACR Infrastructure Justice » et le certificat associé sont générés lors de la Cérémonie des Clés de l'« ACR Infrastructure Justice » et sont stockés conformément à la procédure [PCC]. Pour chaque AC subordonnée, la bi-clé de l'AC subordonnée et le certificat associé sont également générés lors de la Cérémonie des Clés de cette AC subordonnée.

La preuve de possession de la clé privée de l'AC subordonnée repose sur la vérification de la signature numérique de la requête de certificat de l'AC subordonnée qui doit être au format PKCS#10.

3.2.2. Validation de l'identité d'un organisme

L'identité de l'organisme est préalablement validée par l'AA-PEKIN. L'« ACR Infrastructure Justice » ne délivrant que des certificats pour des AC subordonnées du Ministère de la Justice, la validation de l'identité de l'organisme demandeur est simplifiée et repose sur des vérifications internes au Ministère de la Justice.

3.2.3. Validation de l'identité d'un individu

Sans objet pour l'« ACR Infrastructure Justice » qui ne délivre que des certificats d'AC.

3.2.4. INFORMATIONS NON VÉRIFIÉES DU PORTEUR

Sans objet pour l'« ACR Infrastructure Justice » qui ne délivre que des certificats d'AC.

3.2.5. VALIDATION DE L'AUTORITÉ DU DEMANDEUR

La validation est effectuée en même temps que la procédure d'acceptation de rattachement à l'« ACR Infrastructure Justice » d'une AC subordonnée.

3.2.6. CERTIFICATION CROISÉE D'AC

L'AA-PEKIN gère et documente les demandes d'accords de reconnaissance avec des AC extérieures au domaine de l'IGC PEKIN du Ministère de la Justice.

3.3. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLÉS

3.3.1. IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT

Il n'est pas prévu de renouvellement des clés de l'« ACR Infrastructure Justice » dans cette version de la PC. Le renouvellement du bi-clé d'une AC subordonnée entraine automatiquement la génération et la fourniture d'un nouveau certificat d'AC. De plus, un nouveau certificat ne pourra être émis que pour un nouveau bi-clé. A cet effet, une vérification applicative interdit explicitement la génération de deux certificats pour une même clé publique que l'entité soit identique ou différente.

3.3.2. IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT APRÈS RÉVOCATION

La procédure est identique à celle d'une demande initiale, cf. Validation initiale de l'identité

3.4. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RÉVOCATION

La procédure de révocation d'un certificat d'AC subordonnée doit être effectuée à l'aide du formulaire de demande de révocation adéquat et dument renseigné et adressé au service de révocation des certificats par voie électronique. Ce formulaire doit par ailleurs être signé électroniquement par un RC identifié et faisant autorité pour l'AC subordonnée en question. S'agissant d'un certificat d'AC subordonnée, le service de révocation des certificats effectue un contre appel pour validation de la demande et identification du demandeur.

4. EXIGENCES OPÉRATIONNELLES SUR LE CYCLE DE VIE DU CERTIFICAT D'AC

Sauf mention explicite, ce chapitre ne concerne que les certificats d'AC subordonnées signés par l'« ACR Infrastructure Justice ».

4.1. DEMANDE DE CERTIFICAT

4.1.1. ORIGINE D'UNE DEMANDE DE CERTIFICAT

Lorsqu'une nouvelle AC subordonnée doit être crée, un formulaire de demande de certificat d'AC, précisant à minima son nom, l'usage, la délégation de gestion, l'AC signataire et des informations sur le demandeur, est renseigné par l'AA de cette AC subordonnée.

4.1.2. PROCESSUS ET RESPONSABILITÉS POUR L'ÉTABLISSEMENT D'UNE DEMANDE DE CERTIFICAT

L'établissement de la demande d'un certificat d'une AC subordonnée est sous la responsabilité de l'AA de cette autorité. Le formulaire de demande doit être signé par un RC qui a autorité pour cette AC subordonnée et transmis à l'AE de l'IGC PEKIN pour traitement.

La demande de certificat doit être effectuée en utilisant les formulaires adéquats mis à disposition par l'« ACR Infrastructure Justice ». Ces formulaires contiennent à minima les informations suivantes :

- CN à utiliser pour l'AC ;
- les données personnelles d'identification du RC ;
- les données d'identification du bénéficiaire (personne responsable de l'usage de l'AC après sa délivrance)

Le formulaire de demande est établi soit directement par le RC à partir des éléments fournis par son entité, soit par son entité. Il est dans tous les cas signé par le RC et transmis à l'AE.

Par ailleurs, l'AE doit s'assurer de disposer d'une information permettant de contacter le RC du certificat et de valider ses autorisations de demande de certificats.

4.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

4.2.1. EXÉCUTION DES PROCESSUS D'IDENTIFICATION ET DE VALIDATION DE LA DEMANDE

L'AE effectue les opérations suivantes lors du traitement d'une demande de certificat qui lui est transmise :

- Validation de l'identité de l'entité ;
- Validation de l'identité du RC signataire de la demande ;
- Validation de l'autorisation d'émettre un certificat par le RC signataire ;
- Validation de l'autorisation d'émettre un certificat pour cette AC ;
- Validation du formulaire, sa signature, les éléments fournis.

4.2.2. ACCEPTATION OU REJET DE LA DEMANDE

l'AA-PEKIN, en fonction des informations présentes dans la demande validée par l'AE, approuve, rejette ou réclame des informations complémentaires permettant de prendre une décision définitive sur l'approbation ou le rejet de la demande. En cas d'acceptation, l'AA-PEKIN organise une Cérémonie des Clés pour la création du

certificat d'AC subordonnée demandé.

4.2.3. Durée d'établissement du certificat

S'agissant de certificat d'AC et par conséquent requérant la réalisation d'une cérémonie des clés, à réception de la demande, la durée d'établissement est de 10 jours ouvrés.

4.3. Délivrance du certificat

4.3.1. Actions de l'AC concernant la délivrance du certificat

Le certificat de l'« ACR Infrastructure Justice » tout comme les certificats d'AC subordonnée qu'elle signe, sont générées lors d'une cérémonie des clés.

Au préalable à cette cérémonie des clés, l'AA-PEKIN vérifie le contenu des documents fournis par l'AA de l'AC subordonnée et crée un document de gestion de la Cérémonie des Clés reprenant toute les étapes nécessaires à la création du certificat de l'AC subordonnée et de la bi-clé si nécessaire (cas de la délégation de gestion). Ce document sera suivi étape par étape lors de la Cérémonie des Clés.

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

Le certificat est remis à l'AA de l'AC subordonnée à la fin de la Cérémonie des Clés.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

A la fin de la cérémonie des clés, il est de la responsabilité de l'AA de l'AC subordonnée de vérifier que le certificat est conforme à la demande. Un Procès Verbal de fin de cérémonie des clés est signée par l'AA attestant la conformité de la cérémonie des clés vis à vis du document de gestion de la cérémonie des clés et valant acceptation du certificat généré durant cette dernière.

4.4.2. Publication du certificat

La publication du certificat d'AC subordonnée délivré par l'« ACR Infrastructure Justice » est de la responsabilité de l'AA de l'AC subordonnée (exception du cas de la délégation de gestion qui transfert la responsabilité de publication à l'AA-PEKIN).

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

l'AA-PEKIN informe l'AE de la délivrance du certificat, qui se charge d'en informer le RC le cas échéant.

4.5. Usages de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat par le porteur

Nous distinguons ici le cas de l'« ACR Infrastructure Justice » elle-même et le cas des AC subordonnées.

4.5.1.1. Clé privée et certificat de l'« ACR Infrastructure Justice »

L'utilisation de la clé privée de l'« ACR Infrastructure Justice » et du certificat associé est limité aux conditions d'usage, génération de certificats d'AC et de LAR, définies pour l'« ACR Infrastructure Justice » dans la présente PC (cf. Usages des certificats). Cette utilisation est conforme à l'utilisation spécifique décrite dans le contenu du certificat (paramètre « keyUsage »).

L'utilisation de la clé privée de l'« ACR Infrastructure Justice » et du certificat associé n'est autorisée que pendant la période de validité du certificat associé (cf. Durée d'établissement du certificat).

La clé privée de l'« ACR Infrastructure Justice » est toujours stockée dans un HSM et n'être mise en œuvre que par l'intermédiaire de ce dernier. Les sauvegardes de la clé privée de l'« ACR Infrastructure Justice » doivent être stockées chiffrées avec une clé uniquement présente dans le HSM.

4.5.1.2. Clé privée et certificat d'une AC subordonnée

L'utilisation de la clé privée d'une AC subordonnée et du certificat associé est limité aux conditions d'usage définies pour cette AC subordonnée dans la présente PC (cf. Usages des certificats). Cette utilisation doit être conforme à l'utilisation spécifique décrite dans le contenu du certificat (paramètre « keyUsage »).

L'utilisation de la clé privée d'une AC subordonnée et du certificat associé n'est autorisée que pendant la période de validité du certificat associé.

La clé privée d'une AC subordonnée doit toujours être stockée dans un HSM et n'être mise en œuvre que par l'intermédiaire de ce dernier. Les sauvegardes de la clé privée de cette AC subordonnée doivent être stockées chiffrées avec une clé uniquement présente dans le HSM.

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

Les UC ne doivent utiliser les certificats d'AC subordonnée et le certificat de '« ACR Infrastructure Justice » qu'à des fins de validation d'une chaîne de confiance et strictement respecter les usages autorisés des certificats. Dans le cas contraire, la responsabilité des UC pourraient être engagée.

Les UC doivent notamment valider les certificats en prenant en compte des LAR/LCR des AC subordonnées et de la LAR de l'« ACR Infrastructure Justice ».

4.6. Renouvellement d'un certificat d'AC

Conformément à [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).

La présente PC interdit le renouvellement et toute nouvelle demande de certificat pour une AC subordonnée ou l'« ACR Infrastructure Justice » entraine la vérification préalable à toute délivrance que la bi-clé soit différente des bi-clés déjà utilisées (unicité du couple DN/clé publique).

4.7. Délivrance d'un nouveau certificat suite à changement du bi-clé

Les bi-clés doivent être périodiquement renouvelés :

- selon les recommandations émises par l'ANSSI en matière de cryptanalyse, afin de minimiser les possibilités d'attaques cryptographiques, ;
- pour que l'« ACR Infrastructure Justice » puisse continuer à délivrer des certificats d'AC subordonnées d'une durée constante ;
- en cas de compromission, suspicion de compromission, vol, dysfonctionnement ou perte des moyens de reconstruction de la clé privée de l'« ACR Infrastructure Justice » ou d'une AC subordonnée.

La délivrance d'un nouveau certificat suit la même procédure que lors de la première génération (cf. Demande de certificat).

4.8. MODIFICATION DU CERTIFICAT

Conformément à [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. Délivrance d'un nouveau certificat suite à changement du bi-clé) et autres qu'uniquement la modification des dates de validité (cf. Renouvellement d'un certificat d'AC).

La modification d'un certificat n'est pas autorisée dans la présente PC.

4.9. RÉVOCATION ET SUSPENSION D'UN CERTIFICAT

La suspension d'un certificat n'est pas autorisée dans la présente PC, nous ne traitons ici que le cas de la révocation.

4.9.1. CAUSES POSSIBLES D'UNE RÉVOCATION

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat de l'« ACR Infrastructure Justice » ou du certificat d'une AC subordonnée :

- demande motivée par une AC subordonnée ;
- suspicion de compromission, compromission, perte ou vol de la clé privée de l'AC ;
- décision de changement d'AC de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de l'AC avec celles annoncées dans la PC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant l'AC ;
- utilisation du certificat par une AC subordonnée portant préjudice à l'« ACR Infrastructure Justice » ;
- les informations présentes dans le certificat d'une AC subordonnée ne sont plus exactes ;
- découverte d'une erreur dans la procédure d'enregistrement de l'AC subordonnée.

Lorsqu'une des circonstances ci-dessus se réalise et que l'« ACR Infrastructure Justice » en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné est révoqué.

4.9.2. ORIGINE D'UNE DEMANDE DE RÉVOCATION

La révocation du certificat de l'« ACR Infrastructure Justice » ou du certificat d'une AC subordonnée ne peut-être décidé que par :

- le RC ;
- l'entité responsable de l'AC ;
- le responsable de l'IGC PEKIN ;
- un représentant légal de l'entité ;
- les autorités judiciaires via une décision de justice.

Le RC est informé des personnes ou entités susceptibles d'effectuer une demande de révocation pour le certificat dont il a la responsabilité

4.9.3. PROCÉDURE DE TRAITEMENT D'UNE DEMANDE DE RÉVOCATION

Dans le cas où l'« ACR infrastructure Justice » décide de révoquer le certificat d'une AC subordonnée suite à la

compromission de la clé privée de l'AC ou de l'« ACR infrastructure Justice », cette dernière informe par mail l'AC subordonnée que l'ensemble des certificats qu'elle a délivré ne sont plus valides, car l'un des certificats de la chaîne de certification n'est plus valide. Cette information sera relayée également directement auprès des entités.

Par ailleurs, le contact identifié sur le site de l'ANSSI (http://www.ssi.gouv.fr) est immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification du Ministère de la Justice.

Dans le cas où une AC subordonnée demande la révocation de son certificat, elle renseigne, signe et transmet le formulaire de demande de révocation et le transmet à l'AE pour traitement. Les informations à fournir sont celles présentes dans le formulaire.

S'agissant d'une AC, l'AE se charge de la validité de la demande, notamment le RC signant la demande et transmet la demande à l'AA-PEKIN pour traitement effectif de la révocation.

4.9.4. Délai accordé à l'AA d'une AC pour formuler une demande de révocation

La demande de révocation d'un certificat d'une AC doit être effectuée sans délai dès la détection d'un événement décrit dans les causes de révocation (cf. Causes possibles d'une révocation).

4.9.5. Délai de traitement d'une demande de révocation

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

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. 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, et que cette liste est accessible au téléchargement.

La révocation d'un certificat de signature de l'AC (signature de certificats et de LCR) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé. A noter, qu'un délai peut être nécessaire en cas de circonstances exceptionnelles comme l'indisponibilité du système, du service, ou d'autres éléments, qui échappe aux contrôles de l'AA-PEKIN. Dans tous les cas, toutes les mesures possibles sont prises afin de permettre la révocation du certificat dans les plus brefs délais.

4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats

Les utilisateurs de certificats sont tenus de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Cette vérification se fait par la consultation des LCR des AC subordonnées et de la LAR de l'« ACR Infrastructure Justice ».

4.9.7. Fréquence d'établissement de la LAR

La LAR de l'« ACR Infrastructure Justice » est émise tous les ans. En cas de révocation d'un certificat d'AC subordonnée, une nouvelle LAR est émise (cf. Délai de traitement d'une demande de révocation).

4.9.8. Délai maximal de publication de la LAR

La LAR est publiée et disponible au téléchargement dans un délai maximal de 30 minutes suivant sa génération.

4.9.9. Exigences sur la vérification en ligne de la révocation et de l'état des certificats

La présente PC ne comprend pas de système de vérification en ligne.

cf. Exigences de vérification de la révocation par les utilisateurs de certificats

4.9.10. Autres moyens disponibles d'information sur les révocations

La présente PC ne comprend pas d'autres moyens d'information sur les révocations.

4.9.11. EXIGENCES SPÉCIFIQUES EN CAS DE COMPROMISSION DE LA CLÉ PRIVÉE

Pour les certificats d'AC subordonnée, outre les exigences précisées au chapitre Procédure de traitement d'une demande de révocation, l'AA de l'AC en cause doit clairement diffusée l'information de révocation de la clé privée de l'AC sur le site internet de l'AC et par tout autres moyens qu'elle jugera opportun. Par ailleurs, l'AA de l'AC doit mettre en œuvre les processus permettant de garantir l'interruption immédiate et définitive de l'usage de la clé privée compromise et du certificat associé.

4.9.12. CAUSES POSSIBLES D'UNE SUSPENSION

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

4.9.13. ORIGINE D'UNE DEMANDE DE SUSPENSION

Sans objet.

4.9.14. PROCÉDURE DE TRAITEMENT D'UNE DEMANDE DE SUSPENSION

Sans objet.

4.9.15. 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

Le seul service d'état des certificats proposés pour l'« ACR Infrastructure Justice » est la consultation publique de son certificat et de sa LAR (au format V2). Cette dernière est accessible sur le site web public du Ministère de la Justice à l'adresse http://www.justice.gouv.fr/igc/sdit/mj_arl-infrastructure.crl.

Dans le cas d'AC subordonnée géré par délégation, les certificats et les LAR/LCR (au format V2) de ces AC subordonnées sont également accessibles sur le site web public du Ministère de la Justice à l'adresse http://www.justice.gouv.fr/igc/sdit/.

4.10.2. DISPONIBILITÉ DE LA FONCTION

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24 et 7 jours sur 7. Cette fonction peut avoir une interruption de service (panne ou maintenance) de 2 heures maximum et une durée maximale totale d'indisponibilité mensuelle de 8 heures.

4.10.3. DISPOSITIFS OPTIONNELS

La présente PC n'inclut pas de dispositifs optionnels.

4.11. FIN DE LA RELATION ENTRE LE L'AC SUBORDONNÉE ET L'« ACR INFRASTRUCTURE JUSTICE »

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'« ACR Infrastructure Justice » et une AC subordonnée avant la fin de validité du certificat de cette dernière, quelle qu'en soit la raison, le certificat est révoqué.

Cette fin de relation doit par ailleurs être compatible avec les engagements pris par l'« ACR Infrastructure

Justice » vis-à-vis des différentes AC subordonnées aux quelles l'« ACR Infrastructure Justice » a délivré des certificats.

4.12. SÉQUESTRE DE CLÉ ET RECOUVREMENT

La bi-clé de l'« ACR Infrastructure Justice » au même titre que les bi-clés des AC subordonnées pour lesquelles elle émet des certificats, n'est pas séquestrée.

Des copies de sauvegardes sécurisés sont effectués afin de pallier à une panne technique d'un HSM. Ce point est traité dans Copie de secours de la clé privée.

4.12.1. POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR SÉQUESTRE DE CLÉS

Sans objet.

4.12.2. POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR ENCAPSULATION DES CLÉS DE SESSION

Sans objet.

5. MESURES DE SÉCURITÉ NON TECHNIQUES

5.1. SÉCURITÉ PHYSIQUE

5.1.1. SITUATION GÉOGRAPHIQUE ET CONSTRUCTION DES SITES

Le site d'exploitation de l'IGC PEKIN est installé dans des locaux du Ministère de la Justice, situés sur le territoire national. La construction des sites respecte les règlements et normes en vigueur. Les caractéristiques ont été définies selon les résultats de l'analyse de risques menée par le Ministère de la Justice.

Les opérations cryptographiques sur l'« ACR Infrastructure Justice » sont réalisées sur des HSM physiquement placés au sein du data center appartenant et sous contrôle du Ministère de la Justice. Les HSM sont par ailleurs à l'intérieur d'une zone réservée au sein de ce data center.

5.1.2. ACCÈS PHYSIQUE

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

Le Ministère de la Justice 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 Ministère de la Justice a défini un périmètre de sécurité physique où sont installés les serveurs et HSM. La mise en œuvre de ce périmètre permet de respecter la séparation des rôles de confiance comme prévu dans la présente PC. Ce périmètre de sécurité doit garantir, en cas de mise en œuvre dans des locaux en commun, que les fonctions et informations hébergées sur les serveurs et HSM de l'IGC ne sont accessibles qu'aux seules personnes ayant des rôles de confiance reconnus et autorisés.

Les équipements de l'IGC PEKIN étant physiquement dans un site classifié du Ministère de la Justice, les détails de la sécurité physique de ce site et par conséquent de l'IGC PEKIN, sont des informations non publiques et uniquement accessibles à des personnes habilitées et après vérification de la nécessité d'accès à ces informations.

Ces points seront précisés dans la DPC.

5.1.3. ALIMENTATION ÉLECTRIQUE ET CLIMATISATION

Afin d'assurer la disponibilité des systèmes informatiques de l'IGC, des systèmes de génération et de protection des installations électriques sont mis en œuvre par le Ministère de la Justice. Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements 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 Ministère de la Justice permettent de respecter les exigences et les engagements pris par l'« ACR Infrastructure Justice » 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 Ministère de la Justice permettent de

respecter les exigences et les engagements pris par l'« ACR Infrastructure Justice » 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'informations mis en œuvre par le Ministère de la Justice permettent de respecter les exigences et les engagements pris par l'« ACR Infrastructure Justice » dans la présente PC. En particulier la disponibilité, la confidentialité et l'intégrité des données conservées dans les journaux, les archives et les logiciels utilisés par l'AC sont assurées.

Les zones de conservation des supports d'informations sont protégées contre les risques d'incendie, d'inondation et de détérioration.

Les documents papiers sont conservées par l'« ACR Infrastructure Justice » dans des locaux fermés à clé et/ou stockés dans des coffres forts dont les codes ne sont connus que par des personnes habilités.

Par ailleurs, des mesures de protection contre l'obsolescence et la détérioration des supports sont prises en compte afin de garantir un accès aux données durant toute la durée de rétention.

5.1.7. MISE HORS SERVICE DES SUPPORTS

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

5.1.8. SAUVEGARDE HORS SITE

En complément de sauvegardes sur site, L'IGC PEKIN réalise des sauvegardes hors site en s'appuyant sur les procédures d'exploitation interne existantes du Ministère de la Justice. Ces sauvegardes sont organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, conformément aux exigences de la présente PC et aux engagements de l'« ACR Infrastructure Justice » en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats.

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

5.2. MESURES DE SÉCURITÉ PROCÉDURALES

5.2.1. RÔLES DE CONFIANCE

Les personnes auxquelles sont attribués des rôles de confiance de l'IGC sont toutes des personnes habilitées du Ministère de la Justice.

Les personnes ayant un rôle 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 de confiance qu'on distingue sont les suivants :

- « Responsable de sécurité » 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 est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc ;
- « Responsable d'application » 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 ;

- « Ingénieur système » 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 ;
- « Opérateur » chargé, dans le cadre de ses attributions, de l'exploitation des applications pour les fonctions mises en œuvre par la composante ;
- « Contrôleur » personne désignée par le HFDS du Ministère de la Justice, dont le rôle est de procéder régulièrement à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante ;
- «Détenteur de secrets » personne ayant pour rôle d'assurer la confidentialité, l'intégrité et la disponibilité des secrets qui lui sont confiés.

5.2.2. NOMBRE DE PERSONNES REQUISES PAR TÂCHES

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents. Les opérations nécessitant l'intervention de plusieurs personnes et les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc) seront précisées dans la DPC.

5.2.3. IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE RÔLE

Chaque entité intervenant dans la cadre de l'« ACR Infrastructure Justice » doit faire vérifier l'identité et les autorisations de tout membre de son personnel 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 les systèmes concernés par le rôle ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- qu'un compte soit ouvert à son nom dans ces systèmes, si nécessaire de par son rôle ;
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

5.2.4. RÔLES EXIGEANT UNE SÉPARATION DES ATTRIBUTIONS

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des services offerts. Les attributions associées à chaque rôle sont décrites dans la DPC de l'« ACR Infrastructure Justice ». La DPC précise comment et sous quelles conditions des rôles peuvent être cumulés par un même exploitant.

La séparation des rôles suivants est respectée :

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

Par ailleurs, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur ;
- contrôleur et tout autre rôle ;
- ingénieur système et opérateur.

5.2.5. Analyse de risques

Le Ministère de la Justice procède à une analyse de risques afin d'identifier les menaces sur l'IGC PEKIN. Cette analyse est revue périodiquement et en cas de changement structurels significatifs de l'IGC.

5.3. Mesures de sécurité vis-à-vis du personnel

5.3.1. Qualifications, compétences et habilitations requises

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

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

Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des procédures de sécurité en vigueur au sein de l'IGC PEKIN.

l'AA-PEKIN et le responsable de la sécurité informent toute personne intervenant dans des rôles de confiance de l'IGC PEKIN :

- de ses responsabilités relatives aux services de l'IGC PEKIN ;
- des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

5.3.2. Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC PEKIN met en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante. Ces personnels sont notamment habilités à un niveau suffisant permettant de garantir une vérification des antécédents adéquate.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (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.

Les personnels ont eu connaissance et compris les implications des opérations dont ils ont la responsabilité.

5.3.4. Exigences et fréquence en matière de formation continue

Chaque évolution dans les systèmes, les procédures ou l'organisation fait l'objet d'information ou de formation aux intervenants lorsque cette évolution impacte le mode de fonctionnement initial.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Sans objet

5.3.6. SANCTIONS EN CAS D'ACTIONS NON AUTORISÉES

Les sanctions appliquées en cas d'abus de droits ou d'actions non autorisées, font l'objet d'un traitement commun entre le RSSI et le DRH du Ministère de la Justice.

5.3.7. EXIGENCES VIS-À-VIS DU PERSONNEL DES PRESTATAIRES EXTERNES

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC PEKIN est soumis aux mêmes règles que le personnel du Ministère de la Justice. Les règles, procédures et exigences des chapitres § 5.3.1 à § 5.3.4 et § 5.3.6 sont applicables.

5.3.8. DOCUMENTATION FOURNIE AU PERSONNEL

Le 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 et de sécurité de la composante au sein de laquelle il travaille.

5.4. PROCÉDURES DE CONSTITUTION DES DONNÉES D'AUDIT

5.4.1. TYPE D'ÉVÉNEMENTS À ENREGISTRER

L'IGC PEKIN enregistre les évènements liés aux services et à la protection de l'« ACR Infrastructure Justice » qu'elle met en œuvre. Toute action liée à un certificat émis par l'« ACR Infrastructure Justice » est enregistrée et un historique est conservé au sein de la base de données de l'« ACR Infrastructure Justice » ou de la base de données de l'AE.

De plus, les événements suivants font l'objet d'un enregistrement par l'application de l'IGC PEKIN :

- acceptation ou refus de connexion à l'application ;
- demande ou génération de certificat ;
- demande de révocation ou révocation de certificat ;
- génération de la LCR ;
- ajout ou suppression des personnels autorisés à intervenir sur l'application ;
- modification des droits des personnels autorisés à intervenir sur l'application ;
- modification des paramètres de configuration de l'application ;
- plus généralement, toute opération réalisée sur l'application.

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

- Type d'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;
- Date et heure de l'évènement ;
- Résultat de l'évènement (échec ou réussite) ;

De plus, lorsqu'elles existent, les informations suivantes sont enregistrées :

- Destinataire de l'opération ;
- Nom du demandeur de l'opération ou référence du système effectuant la demande ;

- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'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 PEKIN, à l'exception des actions manuelles pour lesquelles des journaux papier sont utilisés (accès physique, cérémonie des clés, ...).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée.

5.4.2. Fréquence de traitement des journaux d'événements

l'« ACR Infrastructure Justice » étant une AC racine, dont les clés sont offline, il n'y a pas de fréquence spécifiquement établie pour le traitement des journaux. Ces derniers sont traités à l'occasion d'opérations effectuées sur l'« ACR Infrastructure Justice » (signature ou révocation d'un certificat, signature de la LAR, ajout, suppression, modification d'un administrateur, …) ou systématiquement en cas de remontée d'événement anormal ou de dysfonctionnement d'une fonctionnalité de l'IGC.

5.4.3. Période de conservation des journaux d'événements

Les enregistrements des journaux sont conservés :

- 1 an pour les événements système ;
- sans limitation de durée pour les événements générés par l'application de l'IGC ou de l'AE.

5.4.4. Protection des journaux d'événements

Les journaux d'événements de l'application IGC sont accessibles uniquement au personnel autorisé de l'IGC est sont en lecture seule depuis l'application.

Les journaux d'événement système du serveur d'application IGC sont accessibles uniquement aux administrateurs autorisés du Ministère de la Justice et nécessite un accès avec un compte à privilèges sur le serveur faisant tourner l'application IGC.

5.4.5. Procédures de sauvegarde des journaux d'événements

Les journaux d'événements sont sauvegardés quotidiennement par delta avec la sauvegarde précédente et hebdomadairement dans leur globalité.

5.4.6. Système de collecte des journaux d'événements

Un système de collecte des journaux d'événements système est en place afin d'assurer l'archivage de ces derniers. Il respecte le niveau de sécurité relatif à l'intégrité, la disponibilité et la confidentialité des données.

5.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement

Les personnels agissant sur l'IGC PEKIN sont informés que toutes les opérations qu'ils effectuent sur cette dernière sont tracées. De ce fait, ils sont de facto notifiés de l'enregistrement de leurs actions.

5.4.8. Evaluation des vulnérabilités

Le contrôle des journaux d'événements système est continu et quotidien afin de permettre une anticipation des vulnérabilités, et des remontées d'alerte en cas de vulnérabilités.

Le contrôle des journaux des événements fonctionnels est réalisé à la demande en cas de litige, ou pour analyse de comportement de l'« ACR Infrastructure Justice ».

5.5. ARCHIVAGE DES DONNÉES

5.5.1. TYPES DE DONNÉES À ARCHIVER

L'archivage permet d'assurer la pérennité des journaux constitués au profit de l'IGC PEKIN. Il permet également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données de l'« ACR Infrastructure Justice » qui sont archivées sont les suivantes :

- les logiciels et les fichiers de configuration des équipements informatiques ;
- la PC et la DPC de l'« ACR Infrastructure Justice » ;
- Les certificats et LAR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les dossiers de demande de certificat, de demande de révocation ;
- les documents justificatifs des actions menées sur l'IGC (création, révocation, …) ;
- les journaux d'événements.

5.5.2. PÉRIODE DE CONSERVATION DES ARCHIVES

Les durées d'archivage des différentes données sont les suivantes :

- PC et DPC : durée de vie de l'AC ;
- documents organisationnels de cérémonies des clés : durée de vie de l'AC ;
- dossiers de demande de certificat : 7 ans ;
- certificats émis par l'AC : 5 ans après son expiration ;
- dernière LAR émis par l'AC : 5 ans après son expiration ;
- journaux d'événements : 7 ans après leur génération.

5.5.3. PROTECTION DES ARCHIVES

Pendant toute la durée de leur conservation, les archives et leurs sauvegardes sont :

- protégées en intégrité ;
- accessibles aux personnes autorisées (protection en confidentialité) ;
- disponibles à la lecture et l'exploitation (protection en disponibilité).

Les moyens mis en œuvre pour la protection des archives sont détaillés dans la DPC de la présente PC.

5.5.4. PROCÉDURE DE SAUVEGARDE DES ARCHIVES

Des sauvegardes régulières sont réalisées par les personnels de confiance du Ministère de la Justice. L'AA-PEKIN s'assure de la mise en place et du maintien des mesures requises afin d'assurer l'intégrité et la disponibilité des archives de l'« ACR Infrastructure Justice », conformément aux exigences de la présente PC.

5.5.5. EXIGENCES D'HORODATAGE DES DONNÉES

L'horodatage des données journalisées est automatique. Pour cela, les composants de l'IGC sont synchronisés sur

un même serveur synchronisé avec l'heure universelle.

5.5.6. Système de collecte des archives

Un système de collecte des archives est en place et respecte le niveau de sécurité relatif à l'intégrité, la disponibilité et la confidentialité des données.

5.5.7. Procédure de récupération et de vérification des archives

Toute demande de récupération d'archive (papier et électronique) doit être adressée à l'AA-PEKIN. La récupération et la vérification des archives sont effectuées dans un délai d'une semaine. Il est à noter que seul l'« ACR Infrastructure Justice » peut accéder à toutes ses archives.

5.6. Changement de clé d'AC

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

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

Dès qu'une nouvelle bi-clé d'« ACR Infrastructure Justice » est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.

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

5.7. Reprise suite à compromission et sinistre

5.7.1. Procédure de remontée et de traitement des incidents et des compromissions

Des procédures (sensibilisation, formation du personnel notamment) et des moyens de remontée et de traitement des incidents (analyse des différents journaux d'événements notamment) sont mis en oeuvre.

Dans le cas d'un incident majeur tel que la perte, la suspicion de compromission, la compromission ou le vol de la clé privée de l'« ACR Infrastructure Justice », l'événement déclencheur est la constatation de l'incident au niveau de la composante concernée. Cette dernière doit immédiatement informer l'AC par tout moyen à sa disposition. Le cas de l'incident majeur est impérativement traité dès sa détection et la publication de l'information de révocation du certificat, si nécessaire, est effectuée dans la plus grande urgence par tout moyen utile et disponible. Par ailleurs, le contact identifié sur le site de l'ANSSI (http://www.ssi.gouv.fr) est immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification du Ministère de la Justice.

Dans le cas d'une insuffisance de sécurité, pour son utilisation prévue restante, dans l'algorithme ou de ses paramètres associés utilisés par l'« ACR Infrastructure Justice » pour son propre certificat ou le certificat d'une AC subordonnée, l'« ACR Infrastructure Justice » :

- informera les AC subordonnées pour lesquelles elle a délivré des certificats ;
- révoquera les certificats concernés.

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

Conformément à la Politique de Sécurité du MJ, l'« ACR Infrastructure Justice » est intégrée dans le Plan de

Continuité d'Activité (PCA) du MJ afin de répondre aux exigences de disponibilité de ses fonctions sensibles, et découlant :

- de la présente PC ;
- des engagements en termes de qualité de service des différentes composantes de l'IGC, notamment pour ce qui concerne les fonctions liées à la publication et/ou liées à la révocation des certificats.

Ce plan est testé au minimum une fois tous les 3 ans.

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

5.7.3.1. Compromission de l'« ACR Infrastructure Justice »

1. Tous les certificats d'AC subordonnées émis par l'« ACR Infrastructure Justice » sont révoqués ;
2. Le certificat de l'« ACR Infrastructure Justice » est immédiatement révoqué ;
3. Il n'est pas prévu de procédure de reprise (régénération du certificat d'« ACR Infrastructure Justice ») ;
4. Tous les certificats des AC subordonnées deviennent invérifiables. Leurs PC respectives doivent préciser la gestion et les implications de ce cas de figure ;
5. l'AA de l'« ACR Infrastructure Justice » décide du transfert ou de la cessation d'activité de l'IGC ou de la génération d'un nouveau certificat d'« ACR Infrastructure Justice » puis de nouveaux certificats d'AC subordonnée.

5.7.3.2. Compromission d'une AC subordonnée

A la demande de l'AA de l'AC subordonnée, le certificat correspondant est immédiatement révoqué suivant la procédure décrite dans Procédure de traitement d'une demande de révocation. La procédure de renouvellement du certificat de l'AC subordonnée est détaillée dans Renouvellement d'un certificat d'AC.

5.7.4. Capacités de continuité d'activités suite à un sinistre naturel ou autre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC (cf. Procédure de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)).

5.8. Fin de vie de l'IGC

Une ou plusieurs Composantes de l'IGC PEKIN peuvent être amenées à cesser leur activité ou à les transférer à une autre entité.

Par définition :

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

Dans le cas de l'« ACR Infrastructure Justice » :

- le transfert d'activité n'est pas prévu ;
- la cessation d'activité qui serait totale s'agissant d'une AC racine, engendrera la révocation des certificats et la publication des LCR conformément aux engagements pris dans la présente PC (cf. Compromission de l'« ACR Infrastructure Justice »).

En cas d'arrêt du service, l'AC s'assurera :

- de la récupération et de la destruction de toutes les copies de sauvegarde du HSM de l'« ACR Infrastructure Justice » ;
- de révoquer le certificat de l'« ACR Infrastructure Justice » et dans la mesure du possible, de tous les certificats des AC subordonnées signés et encore valides ;
- de révoquer les certificats des administrateurs de l'« ACR Infrastructure Justice » ;
- de publier une nouvelle LAR contenant tous les certificats révoqués ;
- de la destruction logique et/ou physique de la clé privée de l'« ACR Infrastructure Justice » sur le HSM ;
- d'informer les responsables de certificat, les administrateurs, les utilisateurs de la révocation effective du certificat de l'« ACR Infrastructure Justice » et de l'arrêt du service ;
- d'informer immédiatement le contact identifié sur le site de l'ANSSI (http://www.ssi.gouv.fr).

6. MESURES DE SÉCURITÉ TECHNIQUES

6.1. GÉNÉRATION ET INSTALLATION DE BI-CLÉS

6.1.1. GÉNÉRATION DE BI-CLÉS

La génération du bi-clé de signature de l'« ACR Infrastructure Justice » et des AC subordonnées qu'elle signe est effectuée lors de la cérémonie des clés. Les clés de signature de l'« ACR Infrastructure Justice » et des AC subordonnées qu'elle signe sont générées et mises en œuvre dans un module cryptographique ayant une certification Critères Communs au niveau EAL4+ et une qualification au niveau renforcé délivrée par l'ANSSI.

La cérémonie de clés se déroule 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 MJ. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie.

La cérémonie se déroule suivant un processus préalablement défini et donne lieu à la génération du bi-clé de signature de l'AC et éventuellement d'autres bi-clés nécessaire au bon fonctionnement de l'IGC. Des parts de secrets sont également générées. Les parts de secrets sont des des données permettant de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la (ou des) clé(s) privée(s) d'AC sauvegardée(s) lors de la cérémonie de clés.

Suite à leur génération, les parts de secrets sont remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Les parts de secrets sont confinées dans des cartes à puce et remises à des porteurs à raison d'une part maximale pour une AC. Chaque part de secrets est être mise en œuvre par son porteur. Ce dernier peut le cas échéant, en accord avec le responsable de l'IGC, notamment en cas d'indisponibilité au moment où la cérémonie des clés doit être opérée, transférer temporairement ou définitivement cette part de secret à un personnel désigné.

6.1.2. TRANSMISSION DE LA CLÉ PRIVÉE AU PROPRIÉTAIRE

La présente PC ne prévoit pas de transmission de clé privée.

La clé privée de l'« ACR Infrastructure Justice » est générée dans la plate-forme de l'« ACR Infrastructure Justice ». Elle est sauvegardée durant la cérémonie des clés, et n'est pas transmise. Elle reste exclusivement la propriété de l'AA-PEKIN.

La clé privée d'une AC subordonnée est générée par l'AC subordonnée lors d'une cérémonie des clés de celle-ci. Cette génération doit être effectuée dans un dispositif répondant aux exigences Annexe 1 : Exigences de sécurité du module cryptographique de la présente PC. L'« ACR Infrastructure Justice » s'assure du respect de ces exigences, auprès de l'AC subordonnée, au travers d'un engagement contractuel clair et explicite de l'AC subordonnée vis-à-vis de l'« ACR Infrastructure Justice ».

6.1.3. TRANSMISSION DE LA CLÉ PUBLIQUE À L'« ACR INFRASTRUCTURE JUSTICE »

La clé publique d'une AC subordonnée est transmise à l'« ACR Infrastructure Justice » dans le cadre de la certification de cette AC subordonnée. Cette transmission suit la procédure décrite dans le document correspondant.

6.1.4. TRANSMISSION DE LA CLÉ PUBLIQUE DE L'« ACR INFRASTRUCTURE JUSTICE » AUX UTILISATEURS DE CERTIFICATS

La clé publique de l'« ACR Infrastructure Justice » est diffusée dans un certificat d'AC Racine qui est un auto-signé.

Un certificat racine auto-signé ne permet pas de garantir par lui-même que la clé publique correspondante

appartient bien à l'AC considérée. Sa diffusion doit s'accompagner de la diffusion, via des sources de confiance, de l'empreinte numérique du certificat, et éventuellement de la clé publique, ainsi que d'une déclaration qu'il s'agit bien de la clé publique de l'AC Racine.

La clé publique de l'« ACR Infrastructure Justice », ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration d'appartenance) doivent pouvoir être récupérées aisément par les utilisateurs de certificats.

L'IGC PEKIN étant privée, la clé publique et le certificat de l'« ACR Infrastructure Justice » sont intégrés sur les postes du MJ et transmis aux AC subordonnées et/ou partenaires du MJ qui le nécessitent.

6.1.5. Taille des clés

Les clés de l'« ACR Infrastructure Justice » et des AC subordonnées doivent respecter les exigences de caractéristiques (tailles, algorithmes, etc.) du document [PES].

Tous les certificats sont signés en utilisant l'algorithme de hachage SHA-512.

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 de l'« ACR Infrastructure Justice » et des AC subordonnées sont des ressources cryptographiques matérielles certifiées et/ou qualifiées par l'ANSSI et respectent donc les normes de sécurité correspondant à la bi-clé (paramètres, algorithmes).

l'« ACR Infrastructure Justice » impose un taille de 4096 bits pour sa clé et les clés des AC subordonnées qu'elle signe.

6.1.7. Objectifs d'usage de la clé

L'utilisation de la clé privée de l'« ACR Infrastructure Justice » et du certificat associé est strictement limitée à la signature de certificats d'AC subordonnées et de LAR.

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

Le module cryptographique HSM « Hardware Security Module » utilisé par l'« ACR Infrastructure Justice », pour la génération et la mise en œuvre de ses clés privées, est un matériel ayant une certification Critères Communs au niveau EAL4+ et qualification au niveau renforcé délivrée par l'ANSSI.

l'« ACR Infrastructure Justice » s'assure de la sécurité des HSM utilisés tout au long de leur cycle de vie. En particulier, l'AC met en place les procédures nécessaires pour garantir :

- l'intégrité des HSM durant leur transport depuis le fournisseur;
- l'intégrité des HSM durant leur stockage précédant la cérémonie des clés ;
- que les opérations d'activation, de sauvegarde et de restauration des clés de signature sont réalisées sous le contrôle de deux personnels ayant des rôles de confiance ;
- que le HSM fonctionne correctement ;
- que les clés contenues dans le HSM sont bien détruites lorsque celui-ci est dé-commissionné.

6.2.2. CONTRÔLE DE LA CLÉ PRIVÉE PAR PLUSIEURS PERSONNES

L'activation de la clé privée d'AC est contrôlée par une personne détenant des données d'activation et qui est dans un rôle de confiance. La personne de confiance activant la clé privée d'AC s'authentifie de manière forte sur le logiciel de l'« ACR Infrastructure Justice ». La clé privée est activée dans un boîtier cryptographique afin qu'elle puisse être utilisée par les seuls rôles de confiance qui peuvent émettre des certificats.

6.2.3. SÉQUESTRE DE LA CLÉ PRIVÉE

La clé privée de l'« ACR Infrastructure Justice » n'est jamais exportée en clair en dehors du HSM et n'est pas séquestrée.

L'« ACR Infrastructure Justice » ne séquestre pas les clés privées des AC subordonnées qu'elle certifie.

6.2.4. COPIE DE SECOURS DE LA CLÉ PRIVÉE

La clé privée de l'« ACR Infrastructure Justice » est sauvegardée sous le contrôle de plusieurs personnes à des fins de disponibilité. Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles. Les sauvegardes sont sur un site délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'AC. Les sauvegardes sont stockées dans un coffre fort physique.

6.2.5. ARCHIVAGE DE LA CLÉ PRIVÉE

La clé privée de l'« ACR Infrastructure Justice » n'est pas archivée.

6.2.6. TRANSFERT DE LA CLÉ PRIVÉE VERS / DEPUIS LE MODULE CRYPTOGRAPHIQUE

La clé privée de l'« ACR Infrastructure Justice » est générée, activée et stockée dans un HSM.

Quand elle n'est pas stockée dans un HSM ou lors de son transfert, la clé privée de l'AC est chiffrée au moyen de l'algorithme AES. La clé privée de l'AC chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence et l'authentification de plusieurs personnes ayant des rôles de confiance.

6.2.7. STOCKAGE DE LA CLÉ PRIVÉE DANS UN MODULE CRYPTOGRAPHIQUE

La clé privée de l'« ACR Infrastructure Justice » stockée dans un HSM est protégée avec le même niveau de sécurité que celui dans lequel elle a été générée.

Le stockage de secours est précisé au chapitre Copie de secours de la clé privée.

6.2.8. MÉTHODE D'ACTIVATION DE LA CLÉ PRIVÉE

L'activation de la clé privée de l'« ACR Infrastructure Justice » dans le module cryptographique est contrôlée via des données d'activation et fait intervenir une personne ayant un rôle de confiance au sein de l'AA-PEKIN.

6.2.9. MÉTHODE DE DÉSACTIVATION DE LA CLÉ PRIVÉE

La désactivation de la clé privée de l'« ACR Infrastructure Justice » dans le module cryptographique est de la responsabilité de la personne ayant effectuée l'activation de la clé. Cette personne s'assure et garantie que la clé privée est désactivée après son usage.

6.2.10. MÉTHODE DE DESTRUCTION DE LA CLÉ PRIVÉE

La clé privée de l'« ACR Infrastructure Justice » est détruite quand elle n'est plus utilisée ou quand le certificat auquel elle correspond est expiré ou révoqué. 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.

6.2.11. NIVEAU DE QUALIFICATION DU MODULE CRYPTOGRAPHIQUE

Le module cryptographique utilisé par l'« ACR Infrastructure Justice » est certifié au niveau EAL4+ selon les critères communs (norme ISO 15408) et qualifié renforcé par l'ANSSI.

6.3. AUTRES ASPECTS DE LA GESTION DES BI-CLÉS

6.3.1. ARCHIVAGE DES CLÉS PUBLIQUES

La clé publique de l'« ACR Infrastructure Justice » est archivée dans le cadre de l'archivage de son certificat correspondant pendant la période de validité du certificat.

Les clés publiques des AC subordonnées sont également archivées dans le cadre de l'archivage des certificats correspondant pendant la période de validité des certificats.

6.3.2. DURÉE DE VIE DES BI-CLÉS ET DES CERTIFICATS

La durée de vie du certificat de l'« ACR Infrastructure Justice » est de 24 ans.

La durée de vie du certificat d'une AC subordonnée sera établie entre l'AA-PEKIN et l'AA de l'AC subordonnée en fonction des besoins exprimés.

Dans tous les cas, la présente PC garantit que l'AC subordonnée ne pourra pas avoir une date de fin postérieure à la date d'expiration du certificat de l'« ACR Infrastructure Justice » qui est le 21 novembre 2037.

6.4. DONNÉES D'ACTIVATION

6.4.1. GÉNÉRATION ET INSTALLATION DES DONNÉES D'ACTIVATION

La génération et l'installation des données d'activation du module cryptographique de l'« ACR Infrastructure Justice » se font lors de la phase d'initialisation et de personnalisation de ce module (cérémonie des clés du module cryptographique). Ces données d'activation sont transmises aux porteurs de secrets de manière à en garantir la confidentialité et l'intégrité. De même, la génération et l'installation des données d'activation de la clé privée de l'« ACR Infrastructure Justice » sont générées durant une cérémonie de clés. Elles permettent d'activer la clé privée lorsque nécessaire.

l'AA-PEKIN s'assure de la confidentialité et de la disponibilité de ces données d'activation qui sont confiées à des responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués.

6.4.2. PROTECTION DES DONNÉES D'ACTIVATION

Les données d'activation qui sont générées par l'AC pour son module cryptographique sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire qui est effectuée durant la cérémonie des clés. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

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 de l'AC. Il répond au moins aux objectifs de sécurité suivants :

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

Quand un composant d'AC est hébergé sur une plateforme évaluée au regard d'exigences d'assurance de sécurité, il est utilisé dans sa version certifiée. Au minimum le composant utilise la même version de système d'exploitation que celle sur lequel le composant a été certifié. Les composants d'AC sont configurés de manière à limiter les comptes et services aux seuls éléments nécessaires pour supporter les services d'AC.

6.5.2. Niveau de qualification des systèmes informatiques

Sans objet

6.6. Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre une fonction de l'IGC PEKIN est documentée. La configuration du système des composantes de l'IGC PEKIN ainsi que toute modification et mise à niveau sont documentées.

6.6.1. Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC doit être signalée à l'AA-PEKIN pour validation. Elle doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

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

Sans objet

6.7. Mesures de sécurité réseau

Les mesures mises en place répondent à la stratégie de gestion des risques du Ministère de la Justice pour les systèmes d'information.

Les communications réseau véhiculant des informations confidentielles font l'objet de mesures de protection

contre l'écoute des informations.

Des passerelles de sécurité sont mises en place afin de protéger la composante locale du système d'information des accès non autorisés.

6.8. HORODATAGE / SYSTÈME DE DATATION

Il n'y a pas d'horodatage utilisé par l'« ACR Infrastructure Justice », mais une datation des évènements qui permet, à partir d'une date fournie par le système d'exploitation de l'« ACR Infrastructure Justice » de séquencer les événements. La date fournie par le système d'exploitation est automatiquement maintenue par la synchronisation avec un serveur NTP « Network Time Protocol ».

7. PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1. PROFILS DES CERTIFICATS

Les certificats émis par l'IGC PEKIN sont au format X.509 v3. Les informations de profil du certificat de l'« ACR Infrastructure Justice », ainsi que de la LAR qu'elle émet, sont présentés ci-dessous. Les informations relatives au certificat de chaque AC subordonnée sont fournies dans la PC de cette AC. Néanmoins, le gabarit utilisé par l'« ACR Infrastructure Justice » pour produire ces certificats d'AC subordonnées est fourni ci-après.

l'IGC PEKIN n'implémente pas de mécanisme OCSP.

7.1.1. PROFIL DU CERTIFICAT DE L'« ACR INFRASTRUCTURE JUSTICE »

	Champ	*Critique*	*Valeur*
Champ de base	Version		**2** (version 3)
	Serial Number		Généré par le logiciel de l'IGC.
	NotBefore		<Date de la signature du certificat> format YYMMDDhhmmssZ
	NotAfter		<NotBefore + 8760jours> format YYMMDDhhmmssZ
	Issuer DN		**CN=ACR Infrastructure Justice** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject DN		**CN=ACR Infrastructure Justice** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject Public key Info - Public Key Algorithm - Modulus		 **rsaEncryption** <clef publique au format DER (4096 bits)>
	Signature Algorithm		**sha512WithRSAEncryption**
X.509 v3 Extensions	Subject Key Identifier		<SHA-1 de la clé publique du Subject>
	Basic Constraints	**O**	**CA:TRUE**
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
	Certificate Policies		**1.2.250.1.120.3.1.1.1**
	Key Usage	**O**	**Certificate Sign, CRL Sign**

7.1.2. PROFIL DU CERTIFICAT D'UNE AC SUBORDONNÉE

	Champ	*Critique*	*Valeur*
Champ de base	Version		**2** (version 3)
	Serial Number		<Généré par le logiciel de l'IGC>
	NotBefore		<Date de la signature du certificat>
	NotAfter		<NotBefore + 3652 jours>
	Issuer DN		**CN=ACR Infrastructure Justice** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject DN		**CN=** <Défini avec l'AC Subordonnée> **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject Public key Info - Public Key Algorithm - Modulus		 **rsaEncryption** <clef publique au format DER (4096 bits)>
	Signature Algorithm		**sha512WithRSAEncryption**
X.509 v3 Extensions	Subject Key Identifier		<SHA-1 de la clé publique du Subject>
	Basic Constraints	**O**	**CA :TRUE** **Pathlen :** <Défini avec l'AC Subordonnée>
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
	Certificate Policies		<OID de l'AC subordonnée>
	Key Usage	**O**	**Certificate Sign, CRL Sign**
	CRL Distribution Points		**URI : http://www.justice.gouv.fr/igc/sdit/mj_arl-infrastructure.crl**

7.2. PROFILS DE LA LISTE DES AUTORITÉS RÉVOQUÉS DE L'« ACR INFRASTRUCTURE JUSTICE »

Les LAR émises par l'« ACR Infrastructure Justice » sont au format X.509 v2, et respecte le profil suivant

	Champ	*Critique*	*Valeur*

Champ de base	Version		**1** (version 2)
	Last Update		<Date de la signature de la LAR>
	Next Update		<Last Update + 365 jours>
	Issuer DN		**CN=ACR Infrastructure Justice** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Signature Algorithm		**sha512WithRSAEncryption**
X.509 v3 Extensions	CRL Number		<Généré par le logiciel de l'IGC, incrémental>
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
Certificats révoqués	Revoked Certificates :		
	- Serial Number		<numéro de série du certificat révoquée>
	- Revocation Date		<date de révocation du certificat>
	- Reason Code		valeur non présente car « non spécifié (0) »

8. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

8.1. Fréquences et / ou circonstances des évaluations

Un contrôle de conformité à la PC peut-être demandé par l'AA-PEKIN.

8.2. Identités / qualifications des évaluateurs

Le contrôle d'une composante est effectué par un ou plusieurs 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

Les auditeurs sont désignés par l'AA-PEKIN mais ne doivent pas appartenir à cette dernière ou être des personnes ayant des rôles opérationnels au sein de l'IGC.

8.4. Sujets couverts par les évaluations

Les contrôles de conformité porte sur une composante ou l'ensemble de l'IGC et à pour objectif de vérifier le respect des engagements et pratiques définis dans :

- la présente politique de certification ;
- la déclaration des pratiques de certification associée à la présence PC ;
- les services de certification mis en œuvre qui découle de la PC et de la DPC.

8.5. Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AA-PEKIN un avis, ayant les conséquences suivantes :

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

8.6. Communication des résultats

Les résultats des contrôles de conformité sont communiqués à la composante contrôlée ainsi qu'à l'AA-PEKIN.

9. AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

9.1. TARIFS

Sans objet.

9.2. RESPONSABILITÉ FINANCIÈRE

Sans objet.

9.3. CONFIDENTIALITÉ DES INFORMATIONS

9.3.1. PÉRIMÈTRE DES INFORMATIONS CONFIDENTIELLES

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

- La partie non publique de la DPC de l'« ACR Infrastructure Justice » ;
- Les clés privées de l'« ACR Infrastructure Justice », des composantes et des AC subordonnées ;
- Les données d'activation associées aux clés privées de l'« ACR Infrastructure Justice » et des AC subordonnées ;
- Tous les secrets de l'IGC, notamment les informations techniques liées à la gestion des HSM ;
- Les journaux d'évènements des composantes de l'IGC ;
- Les rapports d'audits ;
- Les dossiers d'enregistrement des AC subordonnées ;
- Les causes de révocations des certificats ;

9.3.2. INFORMATIONS HORS DU PÉRIMÈTRE DES INFORMATIONS CONFIDENTIELLES

Sans objet.

9.3.3. RESPONSABILITÉS EN TERMES DE PROTECTION DES INFORMATIONS CONFIDENTIELLES

De manière générale les informations confidentielles ne sont accessibles qu'aux personnes concernées par de telles informations ou qui ont l'obligation de conserver et/ou traiter de telles informations.

Le Ministère de la Justice s'engage à traiter les informations confidentielles recueillies dans le respect des lois et règlements en vigueur sur le territoire français.

Dès lors que les informations confidentielles sont soumises à un régime particulier régi par un texte législatif et réglementaire, le traitement, l'accès, la modification de ces informations sont effectués conformément aux dispositions des textes en vigueur.

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au chapitre Périmètre des informations confidentielles, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage. De plus, lorsque ces données sont échangées, l'AC en garantit l'intégrité.

L'AC respecte la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut être amenée à mettre à disposition les dossiers d'enregistrement des RC, services applicatifs ou porteurs à des tiers dans le cadre de procédures légales.

9.4. PROTECTION DES DONNÉES PERSONNELLES

9.4.1. POLITIQUE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

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

9.4.2. DONNÉES À CARACTÈRE PERSONNEL

Les données considérées comme personnelles sont au moins les suivantes :

- les causes de révocation des certificats des AC subordonnées (qui sont considérées comme confidentielles sauf accord explicite de l'AA de l'AC) ;
- les dossiers d'enregistrement des AC.

9.4.3. DONNÉES À CARACTÈRE NON PERSONNEL

Sans objet.

9.4.4. RESPONSABILITÉ EN TERMES DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

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

9.4.5. NOTIFICATION ET CONSENTEMENT D'UTILISATION DES DONNÉES À CARACTÈRE PERSONNEL

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

9.4.6. CONDITIONS DE DIVULGATION D'INFORMATIONS PERSONNELLES AUX AUTORITÉS JUDICIAIRES OU ADMINISTRATIVES

De par sa nature, le Ministère de la Justice applique les lois en vigueur sur le territoire français, dans le cadre de la divulgation d'informations personnelles.

9.4.7. AUTRES CIRCONSTANCES DE DIVULGATION D'INFORMATIONS PERSONNELLES

Sans objet.

9.5. DROITS SUR LA PROPRIÉTÉ INTELLECTUELLE ET INDUSTRIELLE

La fourniture de service par le Ministère de la Justice ne saurait être considérée comme entraînant la cession d'un quelconque doit de propriété intellectuelle ou industrielle. La législation et de la réglementation en vigueur sur le territoire français s'appliquent le cas échéant.

9.6. INTERPRÉTATIONS CONTRACTUELLES ET GARANTIES

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

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent ;

- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante) ;
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC ;
- respecter les accords ou contrats qui les lient entre elles ou aux porteurs ;
- documenter leurs procédures internes de fonctionnement ;
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1. AUTORITÉS DE CERTIFICATION

L'« ACR Infrastructure Justice » a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour une AC subordonnée et que cette dernière a accepté le certificat ;
- Garantir et maintenir la cohérence de sa DPC avec sa PC ;
- Mettre en œuvre et suivre les différentes exigences décrites dans la présente PC lors du traitement d'une demande de certificat ou de révocation ;
- Mettre à disposition 24h/24 7j/7 les informations sur l'état des certificats non expirés ;
- Prendre toutes les mesures raisonnables pour s'assurer que les AC subordonnées sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre une AC subordonnée et l'« ACR Infrastructure Justice » est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'« ACR Infrastructure Justice ».

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

L'« ACR Infrastructure Justice » reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AA-PEKIN.

9.6.2. AUTORITÉ D'ENREGISTREMENT

L'autorité d'enregistrement a le devoir de :

- Instruire les demandes de certificat conformément aux pratiques de la présente PC ;
- Valider l'exactitude des informations fournies ;
- Valider le rôle de confiance du demandeur ;
- Informer l'AC des demandes de certificat en attente ;
- Traiter sans délai les demandes de révocation.

9.6.3. RESPONSABLE DE CERTIFICAT

Le RC a le devoir de :

- Communiquer des informations exactes et à jour lors de sa demande ou du renouvellement du certificat ;
- Interrompre immédiatement et définitivement l'usage des clés privées en cas de compromission.
- Protéger la clé privée de l'AC subordonnée dont il a la responsabilité par des moyens appropriés à son environnement ;
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à la base de certificats de l'AC subordonnée ;
- Respecter les conditions d'utilisation de la clé privée de l'AC subordonnée et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans le certificat de l'AC subordonnée ;
- Faire, sans délai, une demande de révocation du certificat de l'AC subordonnée dont il est responsable auprès de l'AE en cas de compromission ou de suspicion de compromission de sa clé privée (ou de ses données d'activation).

9.6.4. UTILISATEURS DE CERTIFICATS

Les utilisateurs (personnes ou applications) utilisant les certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Contrôler que le certificat signé par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- Pour chaque certificat de la chaine de certification, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (date de validité, statut de révocation) ;
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

9.6.5. AUTRES PARTICIPANTS

Sans objet.

9.7. LIMITE DE GARANTIE

L'« ACR Infrastructure Justice » garantit au travers de ses services d'IGC :

- L'identification et l'authentification de l'« ACR Infrastructure Justice » avec son certificat ;
- L'identification et l'authentification des AC subordonnées avec les certificats d'AC générés par l'« ACR Infrastructure Justice » ;
- La gestion des certificats correspondants et des informations de validité des certificats selon la présente PC.

Aucune autre garantie ne peut être mise en avant par l'« ACR Infrastructure Justice ».

9.8. LIMITE DE RESPONSABILITÉ

Le Ministère de la Justice ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation, des LAR/CRL ainsi que de tout autre équipement ou logiciel mis à disposition.

Le Ministère de la Justice décline en particulier sa responsabilité pour tout dommage résultant :

- d'un emploi des bi-clés pour un usage autre que ceux prévus ;
- de l'usage de certificats révoqués ou expirés ;
- d'un cas de force majeur tel que défini par les tribunaux français.

Le Ministère de la Justice décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le RC.

Le Ministère de la Justice ne pourra pas être tenu pour responsable pour les dommages résultant de réclamation de tiers, de perte de clientèle, d'arrêt de travail ou de tout autre dommage, notamment indirects ou engendrant une perte commerciale.

9.9. INDEMNITÉS

Sans objet.

9.10. DURÉE ET FIN ANTICIPÉE DE LA VALIDITÉ DE LA PC

9.10.1. DURÉE DE VALIDITÉ

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

9.10.2. FIN ANTICIPÉE DE VALIDITÉ

L'« ACR Infrastructure Justice » peut être amené à publier une nouvelle version de la présente PC en cas de besoin d'évolutions.

Le délai de mise en conformité sera arrêté en fonction de la nature et de l'importance des évolutions apportées à la PC et/ou d'un changement de réglementation en vigueur.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

9.10.3. EFFETS DE LA FIN DE VALIDITÉ ET CLAUSES RESTANTS 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

Sans objet.

9.12. AMENDEMENTS À LA PC

9.12.1. PROCÉDURES D'AMENDEMENTS

Tout projet de modification de la présente PC doit rester conforme aux exigences de la politique de sécurité de l'IGC PEKIN, de la PC de l'« ACR Infrastructure Justice » et respecter les engagements avec les AC subordonnées. En cas de changement important, l'AA-PEKIN pourra faire appel à une expertise technique pour en contrôler l'impact.

La procédure d'amendement devra intégrer l'information et les délais d'information concernant les amendements.

La présente PC fera l'objet d'une revue annuelle, pouvant entraîner ou non un amendement.

9.12.2. MÉCANISME ET PÉRIODE D'INFORMATION SUR LES AMENDEMENTS

L'AC communique via son site internet http://www.justice.gouv.fr/igc/sdit l'évolution de la PC au fur et à mesure de ses amendements.

Les seules modifications que l'AA-PEKIN peut opérer sur la PC en vigueur sans notification sont les changements mineurs comme, par exemple, les corrections rédactionnelles et typographiques, les clarifications ou les corrections d'erreurs manifestes. L'AA-PEKIN est seule juge pour déterminer si une modification est mineure ou non.

Pour une modification non mineure, la nouvelle PC sera mise en ligne par avance, avec une indication de la date d'effet.

Lorsqu'une nouvelle version de la PC est mise en ligne, tous les utilisateurs de l'IGC PEKIN sont informés de la nature, de la date et de l'heure du changement, par une publication sur le site web du Ministère de la Justice.

9.12.3. CIRCONSTANCES SELON LESQUELLES L'OID DOIT ÊTRE CHANGÉ

L'OID de la PC de l'« ACR Infrastructure Justice » étant inscrit dans les certificats qu'elle émet, toute évolution de la PC ayant un impact majeur sur les certificats déjà émis se traduit par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

En particulier, l'OID de la PC de l'« ACR Infrastructure Justice » évoluera dès lors qu'un changement majeur intervient dans les exigences de sa PC.

9.13. DISPOSITIONS CONCERNANT LA RÉSOLUTION DE CONFLITS

Sans objet.

9.14. JURIDICTIONS COMPÉTENTES

La présente PC est soumise au droit français. Tout litige relatif à la validité, l'interprétation, l'exécution de la présente PC sera soumis à la législation et de la réglementation en vigueur sur le territoire français.

9.15. CONFORMITÉ AUX LÉGISLATIONS ET RÉGLEMENTATIONS

La présente PC est conforme aux exigences énoncées dans les textes législatifs et réglementaires français.

9.16. DISPOSITIONS DIVERSES

Sans objet.

9.17. AUTRES DISPOSITIONS

Sans objet.

10. ANNEXE 1 : EXIGENCES DE SÉCURITÉ DU MODULE CRYPTOGRAPHIQUE

10.1. EXIGENCES SUR LES OBJECTIFS DE SÉCURITÉ

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques et des LAR) doit répondre 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 créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

10.2. EXIGENCES SUR LA QUALIFICATION

Le module cryptographique utilisé par l'« ACR Infrastructure Justice » et les AC subordonnées doit être qualifié au niveau renforcé, selon le processus décrit dans le [RGS], et être conforme aux Exigences sur les objectifs de sécurité. Pour se faire, il doit notamment avoir une certification Critères Communs dont la cible de sécurité est conforme au profil de protection [CWA14167-4] (ou [CWA14167-2] s'il y a une fonction de sauvegarde des clés privées de l'AC).

11. ANNEXE 2 : DOCUMENTS CITÉS EN RÉFÉRENCE

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
[CWA14167-4]	CWA14167-4 (2003-10) Cryptographic Module for CSP Signing Operations - Protection Profile (CMCSO-PP). PP certifié EAL4+.
[CWA14167-2]	CWA 14167-2 (2003-10) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP). PP certifié EAL4+.
[PCC]	Procédure de Cérémonie des clés – Ministère de la Justice - version 1.0
[PES]	Procédure d'Exploitation de Sécurité – Ministère de la Justice version 1.2
[RGS]	Référentiel Général de Sécurité – Version 2.0
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version mars 2000 (complétée par les correctifs techniques n° 1 d'octobre 2001, n° 2 d' avril 2002 et n° 3 d'avril 2004)