Politique de Certification AC Technique

CIRCUIT DE VALIDATION

Date application	Version	Objet	Rédaction	Vérification	Approbation
23/11/2018	1.1	Correction Point de contact et liens de publication	Le 07/11/2018 L.Flament	Le 08/11/2018 F. 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 14:45:27 +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 28/06/2018 L.Flament	Le 29/06/2018 F. Loffredo	
	0.2	intégration des remarques du vérificateur	Le 02/07/2018 L.Flament		
	0.3	séparation PC/DPC, mise à jour OID	Le 10/10/2018 L.Flament		
12/10/2018	1.0	Version approuvée et applicable	Le 10/10/2018 L.Flament	Le 11/10/2018 F. Loffredo	Le 11/10/2018 AA-PEKIN

SOMMAIRE

1. Introduction....10
1.1. Généralités....10
1.2. Identification du document....10
1.3. Définitions et Acronymes....11
1.3.1. Acronymes....11
1.3.2. Définitions....12
1.4. Entités intervenant dans l'AC Technique....14
1.4.1. Autorité de Certification (AC)....14
1.4.1.1. Enregistrement....15
1.4.1.2. Génération des certificats....15
1.4.1.3. Génération d'éléments secrets....15
1.4.1.4. Remise au RC....15
1.4.1.5. Remise au porteur....15
1.4.1.6. Publication des certificats....15
1.4.1.7. Révocation des certificats....15
1.4.1.8. Information sur l'état des certificats....15
1.4.1.9. participants....16
1.4.2. Autorité d'Enregistrement (AE)....16
1.4.3. Responsable de certificats....17
1.4.3.1. RC certificats électroniques de services applicatifs....17
1.4.3.2. RC certificats pour un porteur....17
1.4.4. Porteurs de certificats....17
1.4.5. Utilisateurs de certificats....17
1.4.5.1. Authentification....17
1.4.5.2. Cachet....18
1.4.5.3. Signature....18
1.4.5.4. Authentification et signature....18
1.4.6. Autres participants....18
1.4.6.1. Composantes de l'IGC....18
1.4.6.2. Mandataire de certification....18
1.5. Usages des certificats....19
1.5.1. Domaines d'utilisation applicables....19
1.5.1.1. Bi-clés et certificats....19
1.5.1.2. Bi-clés et certificats d'AC et de composantes....20
1.5.2. Domaines d'utilisation interdits....20
1.6. Gestion de la PC....20
1.6.1. Entité gérant la PC....20
1.6.2. Point de contact....20
1.6.3. Entité déterminant la conformité d'une DPC avec cette PC....20
1.6.4. Procédures d'approbation de la conformité de la DPC....20
2. Responsabilités concernant la mise à disposition des informations devant être publiées....21
2.1. Entités chargées de la mise à disposition des informations....21
2.2. Informations devant être publiées....21
2.3. Délais et fréquences de publication....21
2.4. Contrôle d'accès aux informations publiées....22
3. Identification et Authentification....23
3.1. Nommage....23

3.1.1. Type de noms....23
3.1.2. Nécessité d'utilisation de noms explicites....23
3.1.2.1. Certificat de l'AC Technique....23
3.1.2.2. Certificat de services applicatifs ou porteurs....23
3.1.3. Anonymisation ou Pseudonymisation....24
3.1.4. Règles d'interprétation des différentes formes de nom....24
3.1.5. Unicité des noms....24
3.1.6. Identification, authentification et rôle des marques déposées....24
3.2. Validation initiale de l'identité....24
3.2.1. Certificat porteur....24
3.2.2. Certificat de service applicatif....24
3.2.3. Méthode pour prouver la possession de la clé privée....25
3.2.4. Validation de l'identité d'un organisme....25
3.2.5. Validation de l'identité d'un individu....25
3.2.6. Informations non vérifiées du porteur....25
3.2.7. Validation de l'autorité du demandeur....25
3.3. Identification et validation d'une demande de renouvellement des clés....25
3.3.1. Identification et validation pour un renouvellement courant....25
3.3.2. Identification et validation pour un renouvellement après révocation....25
3.4. Identification et validation d'une demande de révocation....25
4. Exigences opérationnelles sur le cycle de vie du certificat d'AC....27
4.1. Demande de certificat....27
4.1.1. Origine d'une demande de certificat....27
4.1.2. Processus et responsabilités pour l'établissement d'une demande de certificat....27
4.2. Traitement d'une demande de certificat....27
4.2.1. Exécution des processus d'identification et de validation de la demande....27
4.2.2. Acceptation ou rejet de la demande....27
4.2.3. Durée d'établissement du certificat....28
4.3. Délivrance du certificat....28
4.3.1. Actions de l'AC concernant la délivrance du certificat....28
4.3.2. Notification par l'AC de la délivrance du certificat....28
4.4. Acceptation du certificat....28
4.4.1. Démarche d'acceptation du certificat....28
4.4.2. Publication du certificat....28
4.4.3. Notification par l'AC aux autres entités de la délivrance du certificat....28
4.5. Usages de la bi-clé et du certificat....29
4.5.1. Utilisation de la clé privée et du certificat par le RC et le porteur....29
4.5.2. Utilisation de la clé publique et du certificat par l'utilisateur du certificat....29
4.6. Renouvellement d'un certificat....29
4.7. Délivrance d'un nouveau certificat suite à changement de la bi-clé....29
4.7.1. Causes possibles de changement de la bi-clé....29
4.7.2. Origine de la demande....29
4.7.3. Procédures de traitement d'une demande d'un nouveau certificat....29
4.7.4. Notification de l'établissement d'un nouveau certificat....29
4.7.5. Démarches d'acceptation du nouveau certificat....30
4.7.6. Publication du nouveau certificat....30
4.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat....30
4.8. Modification du certificat....30
4.9. Révocation et suspension d'un certificat....30
4.9.1. Causes possibles d'une révocation....30

4.9.1.1. Certificats de services applicatifs....30
4.9.1.2. Certificats de porteurs....30
4.9.1.3. Certificats d'une composante de l'IGC....31
4.9.2. Origine d'une demande de révocation....31
4.9.2.1. Certificats de services applicatifs....31
4.9.2.2. Certificats de porteurs....31
4.9.2.3. Certificats d'une composante de l'IGC....32
4.9.3. Procédure de traitement d'une demande de révocation....32
4.9.3.1. Révocation d'un certificat d'un service applicatif....32
4.9.3.2. Révocation d'un certificat d'un porteur....32
4.9.3.3. Révocation d'un certificat d'une composante de l'IGC....32
4.9.4. Délai accordé pour formuler une demande de révocation....33
4.9.5. Délai de traitement par l'AC d'une demande de révocation....33
4.9.5.1. Révocation d'un certificat de service applicatif ou porteur....33
4.9.5.2. Disponibilité du système de traitement des demandes de révocation....33
4.9.5.3. Révocation d'un certificat d'une composante de l'IGC....33
4.9.6. Exigences de vérification de la révocation par les utilisateurs de certificats....33
4.9.7. Fréquence d'établissement et durée de validité des LCR....33
4.9.8. Délai maximal de publication d'une LCR....33
4.9.9. Exigences sur la vérification en ligne de la révocation et de l'état des certificats....33
4.9.10. Autres moyens disponibles d'information sur les révocations....33
4.9.11. Exigences spécifiques en cas de compromission de la clé privée....33
4.9.12. Causes possibles d'une suspension....34
4.9.13. Origine d'une demande de suspension....34
4.9.14. Procédure de traitement d'une demande de suspension....34
4.9.15. Limites de la période de suspension d'un certificat....34
4.10. Fonction d'information sur l'état des certificats....34
4.10.1. Caractéristiques opérationnelles....34
4.10.2. Disponibilité de la fonction....34
4.10.3. Dispositifs optionnels....34
4.11. Fin de la relation....34
4.11.1. Fin de relation entre le RC et l'AC....34
4.11.2. Fin de relation entre le porteur et l'AC....34
4.12. Séquestre de clé et recouvrement....35
4.12.1. Politique et pratiques de recouvrement par séquestre de clés....35
4.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session....35
5. Mesures de sécurité non techniques....36
5.1. Mesures de sécurité physique....36
5.1.1. Situation géographique et construction des sites....36
5.1.2. Accès physique....36
5.1.3. Alimentation électrique et climatisation....36
5.1.4. Vulnérabilité aux dégâts des eaux....36
5.1.5. Prévention et protection incendie....36
5.1.6. Conservation des supports....37
5.1.7. Mise hors service des supports....37
5.1.8. Sauvegarde hors site....37
5.2. Mesures de sécurité procédurales....37
5.2.1. Rôles de confiance....37
5.2.2. Nombre de personnes requises par tâches....38
5.2.3. Identification et authentification pour chaque rôle....38

5.2.4. Rôles exigeant une séparation des attributions....38
5.2.5. Analyse de risques....39
5.3. Mesures de sécurité vis-à-vis du personnel....39
5.3.1. Qualifications, compétences et habilitations requises....39
5.3.2. Procédures de vérification des antécédents....39
5.3.3. Exigences en matière de formation initiale....39
5.3.4. Exigences et fréquence en matière de formation continue....39
5.3.5. fréquence et séquence de rotation entre différentes attributions....39
5.3.6. Sanctions en cas d'actions non autorisées....39
5.3.7. Exigences vis-à-vis du personnel des prestataires externes....40
5.3.8. Documentation fournie au personnel....40
5.4. Procédures de constitution des données d'audit....40
5.4.1. Type d'événements à enregistrer....40
5.4.2. Fréquence de traitement des journaux d'événements....41
5.4.3. Période de conservation des journaux d'événements....41
5.4.4. Protection des journaux d'événements....41
5.4.5. Procédures de sauvegarde des journaux d'événements....41
5.4.6. Système de collecte des journaux d'événements....41
5.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement....41
5.4.8. Evaluation des vulnérabilités....41
5.5. Archivage des données....41
5.5.1. Types de données à archiver....41
5.5.2. Période de conservation des archives....42
5.5.3. Protection des archives....42
5.5.4. Procédure de sauvegarde des archives....42
5.5.5. Exigences d'horodatage des données....42
5.5.6. Système de collecte des archives....42
5.5.7. Procédure de récupération et de vérification des archives....42
5.6. Changement de clé d'AC....43
5.7. Reprise suite à compromission et sinistre....43
5.7.1. Procédure de remontée et de traitement des incidents et des compromissions....43
5.7.2. Procédure de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données)....43
5.7.3. Procédure de reprise en cas de compromission de la clé privée d'une composante....43
5.7.4. Capacités de continuité d'activités suite à un sinistre naturel ou autre....44
5.8. Fin de vie de l'IGC....44
6. Mesures de sécurité techniques....45
6.1. Génération et installation de bi-clés....45
6.1.1. Génération de bi-clés....45
6.1.1.1. Clés d'AC....45
6.1.1.2. Clés du service applicatif ou du porteur générées par l'AC....45
6.1.1.3. Clés du service applicatif générées par le RC....45
6.1.1.4. Clés du porteur générées par le porteur....45
6.1.2. Transmission de la clé privée au propriétaire....45
6.1.3. Transmission de la clé publique à l'AC....46
6.1.4. Transmission de la clé publique aux utilisateurs de certificats....46
6.1.5. Taille des clés....46
6.1.6. Vérification de la génération des paramètres des bi-clés et de leur qualité....46
6.1.6.1. Clés d'AC....46
6.1.6.2. Clés des services applicatifs....46

6.1.6.3. Clés des porteurs....47
6.1.7. Objectifs d'usage de la clé....47
6.1.7.1. Clés d'AC....47
6.1.7.2. Clés des services applicatifs....47
6.1.7.3. Clés des porteurs....47
6.2. Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques....47
6.2.1. Standards et mesures de sécurité pour les modules cryptographiques....47
6.2.1.1. Module cryptographique de l'AC....47
6.2.1.2. Dispositif de protection des éléments secrets des porteurs....47
6.2.2. Contrôle de la clé privée par plusieurs personnes....47
6.2.3. Séquestre de la clé privée....48
6.2.4. Copie de secours de la clé privée....48
6.2.5. Archivage de la clé privée....48
6.2.6. Transfert de la clé privée vers / depuis le module cryptographique....48
6.2.7. Stockage de la clé privée dans un module cryptographique....48
6.2.8. Méthode d'activation de la clé privée....48
6.2.8.1. Clés privées d'AC....48
6.2.8.2. Clés privées des services applicatifs....48
6.2.8.3. Clés privées des porteurs....48
6.2.9. Méthode de désactivation de la clé privée....48
6.2.9.1. Clés privées d'AC....48
6.2.9.2. Clés privées des services applicatifs....49
6.2.9.3. Clés privées des porteurs....49
6.2.10. Méthode de destruction de la clé privée....49
6.2.10.1. Clés privées d'AC....49
6.2.10.2. Clés privées des services applicatifs....49
6.2.10.3. Clés privées des porteurs....49
6.2.11. Niveau de qualification du module cryptographique....49
6.3. Autres aspects de la gestion des bi-clés....49
6.3.1. Archivage des clés publiques....49
6.3.2. Durée de vie des bi-clés et des certificats....49
6.4. Données d'activation....50
6.4.1. Génération et installation des données d'activation....50
6.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC....50
6.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du service applicatif....50
6.4.1.3. Génération et installation des données d'activation correspondant à la clé privée du porteur....50
6.4.2. Protection des données d'activation....50
6.4.2.1. Protection des données d'activation correspondant à la clé privée de l'AC....50
6.4.2.2. Protection des données d'activation correspondant à la clé privée du service applicatif....50
6.4.2.3. Protection des données d'activation correspondant à la clé privée du service porteur....51
6.4.3. Autres aspects liés aux données d'activation....51
6.5. Mesures de sécurité des systèmes informatiques....51
6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques....51
6.5.2. Niveau de qualification des systèmes informatiques....51
6.6. Mesures de sécurité liées au développement des systèmes....51
6.6.1. Mesures de sécurité liées au développement des systèmes....51
6.6.2. Mesures liées à la gestion de la sécurité....52
6.6.3. Niveau d'évaluation sécurité du cycle de vie des systèmes....52
6.7. Mesures de sécurité réseau....52

6.8. Horodatage / Système de datation....52
7. Profils des certificats, OCSP et des LCR....53
7.1. Profils pour l'AC....53
7.1.1. Profil du certificat de l'« AC Technique »....53
7.1.2. Profils de la Liste des Certificats Révoqués de l'« AC Technique »....54
7.2. Profils pour les services applicatifs....54
7.2.1. Authentification....54
7.2.2. Cachet....55
7.2.3. Authentification IPSec....56
7.2.4. Signature de code....57
7.2.5. Horodatage....57
7.3. Profils pour les porteurs....58
7.3.1. Authentification....58
7.3.2. Authentification IPSec....59
7.3.3. Signature....60
8. Audit de conformité et autres évaluations....62
8.1. Fréquences et / ou circonstances des évaluations....62
8.2. Identités / qualifications des évaluateurs....62
8.3. Relations entre évaluateurs et entités évaluées....62
8.4. Sujets couverts par les évaluations....62
8.5. Actions prises suite aux conclusions des évaluations....62
8.6. Communication des résultats....62
9. Autres problématiques métiers et légales....63
9.1. Tarifs....63
9.2. Responsabilité financière....63
9.3. Confidentialité des informations....63
9.3.1. Périmètre des informations confidentielles....63
9.3.2. Informations hors du périmètre des informations confidentielles....63
9.3.3. Responsabilités en termes de protection des informations confidentielles....63
9.4. Protection des données personnelles....64
9.4.1. Politique de protection des données à caractère personnel....64
9.4.2. Données à caractère personnel....64
9.4.3. Données à caractère non personnel....64
9.4.4. Responsabilité en termes de protection des données à caractère personnel....64
9.4.5. Notification et consentement d'utilisation des données à caractère personnel....64
9.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives....64
9.4.7. Autres circonstances de divulgation d'informations personnelles....64
9.5. Droits sur la propriété intellectuelle et industrielle....64
9.6. Interprétations contractuelles et garanties....64
9.6.1. Autorités de certification....65
9.6.2. Autorité d'enregistrement....65
9.6.3. Responsable de certificat....66
9.6.4. Porteurs de certificats....66
9.6.5. Utilisateurs de certificats....66
9.6.6. Autres participants....66
9.7. Limite de garantie....67
9.8. Limite de responsabilité....67
9.9. Indemnités....67
9.10. Durée et fin anticipée de la validité de la PC....67
9.10.1. Durée de validité....67

9.10.2. Fin anticipée de validité....67
9.10.3. Effets de la fin de validité et clauses restants applicables....68
9.11. Notifications individuelles et communications entre les participants....68
9.12. Amendements à la PC....68
9.12.1. Procédures d'amendements....68
9.12.2. Mécanisme et période d'information sur les amendements....68
9.12.3. Circonstances selon lesquelles l'OID doit être changé....68
9.13. Dispositions concernant la résolution de conflits....68
9.14. Juridictions compétentes....69
9.15. Conformité aux législations et réglementations....69
9.16. Dispositions diverses....69
9.17. Autres dispositions....69
10. Annexe 1 : Exigences de sécurité du module cryptographique....70
10.1. Exigences sur les objectifs de sécurité....70
10.2. Exigences sur la qualification....70
11. Annexe 2 : Exigences de sécurité du dispositif de protection des éléments secrets....71
11.1. Exigences sur les objectifs de sécurité....71
11.2. Exigences sur la qualification....71
12. Annexe 3 : Documents cités en référence....72

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 possède une autorité dénommée « AC Technique » dont le rôle est de signer des certificats pour des entités finales (machines et humaines) pour les besoins du MJ. Le présent document constitue la Politique de Certification (PC) de l'Autorité de Certification « AC Technique ».

l'« AC Technique » est hiérarchiquement rattachée à l'« ACR Infrastructure Justice » et ne délivre des certificats que pour des entêtées finales. Pour ce besoin, l'« AC Technique » est une AC en-ligne.

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

L'objectif de cette politique de certification est de définir les engagements minimums que le Ministère de la Justice respecte dans la délivrance et la gestion des certificats de l'« AC Technique ».

La présente PC est basée sur :

- La PC Type « certificats électroniques de personne » pour un usage d'authentification client/serveur TLS au niveau * du RGS élaboré par l'ANSSI, pour les usages à destination de personnes physiques :
  - Authentification ;
  - Authentification IPSEC ;
  - Signature ;
- La PC Type « certificats électroniques de services applicatifs » pour un usage d'authentification client/serveur TLS au niveau * du RGS élaboré par l'ANSSI, pour les usages suivants à destination de services applicatifs :
  - Authentification ;
  - Cachet Serveur ;
  - Horodatage ;
  - Authentification IPSEC ;
  - Signature de code.

Remarque :

La présente Politique de Certification est valable pour les profils listés ci-dessus, qui correspondent chacun à un OID distinct (cf. Identification du document). Les différences entre profils sont mentionnées explicitement au fil de la PC.

1.2. IDENTIFICATION DU DOCUMENT

La présente PC est dénommée « Politique de Certification de l'AC Technique » et est la propriété du Ministère de la Justice. Elle définit les exigences relatives à l'AC Technique pour des certificats de services applicatifs et porteurs.

Ce document couvre huit politiques de certification pour les différents usages de certificats :

- Personne physique :
  - PC pour les certificats d'authentification, identifiée par l'OID 1.2.250.1.120.3.3.201.1 ;
  - PC pour les certificats de signature, identifiée par l'OID 1.2.250.1.120.3.3.207.1 ;
  - PC pour les certificats d'authentification IPSec, identifiée par l'OID 1.2.250.1.120.3.3.208.1 ;
- Service applicatif :
  - PC pour les certificats d'authentification, identifiée par l'OID 1.2.250.1.120.3.3.202.1 ;
  - PC pour les certificats d'horodatage, identifiée par l'OID 1.2.250.1.120.3.3.203.1 ;
  - PC pour les certificats cachet serveur, identifiée par l'OID 1.2.250.1.120.3.3.205.1 ;
  - PC pour les certificats d'authentification IPSec, identifiée par l'OID 1.2.250.1.120.3.3.209.1 ;
  - PC pour les certificats de signature de code, identifiée par l'OID 1.2.250.1.120.3.3.210.1.

Le présent document peut être identifié par le numéro d'IDentifiant d'Objet (OID) du profil concerné. D'autres éléments, plus explicites, comme le nom, le numéro de version et la date d'application permettent également de l'identifier sans ambiguïté.

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
VC	Validateur de Certificat

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.

Porteur : cf. participants

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

Validateur de certificat (VC) : cf. participants

1.4. ENTITÉS INTERVENANT DANS L'AC TECHNIQUE

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 » et d'AC subordonnées. L'« AC Technique » est l'une d'entre elles dans le cadre de la délivrance de certificats pour des personnes physiques et des services applicatifs. L'« AC Technique » ne délivre que des certificats à des entités finales.

La mise en œuvre opérationnelle de l'« AC Technique » 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'« AC Technique » 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'« AC Technique » :

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 du service provenant soit du RC ou du porteur, soit de la fonction de génération des éléments secrets du service, si c'est cette dernière qui génère la bi-clé du service applicatif ou du porteur.

1.4.1.3. GÉNÉRATION D'ÉLÉMENTS SECRETS

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

1.4.1.4. REMISE AU RC

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

1.4.1.5. REMISE AU PORTEUR

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

1.4.1.6. 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'« AC Technique » ;
- conditions générales d'utilisation de l'« AC Technique » ;
- politiques et pratiques de l'« AC Technique » ;
- toute autre information pertinente, hors informations d'état des certificats.

1.4.1.7. RÉVOCATION DES CERTIFICATS

La révocation des certificats des services applicatifs ou porteurs de l'« AC Technique » est assurée par l'AE qui se charge de la vérification des informations d'identification du Responsable du Certificat ou du porteur et de la validité du formulaire de révocation de certificat d'autorité conformément aux notices décrivant le contenu attendu pour ce dernier. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

1.4.1.8. INFORMATION SUR L'ÉTAT DES CERTIFICATS

Cette fonction gère la mise à disposition aux utilisateurs de certificats des informations sur l'état des certificats des services applicatifs et des porteurs signés par l'« AC Technique » (révoqués, suspendus, etc.). Ce service est rendu

par la publication de la LCR de l'« AC Technique » à intervalles réguliers ou dès lors qu'une opération de révocation est effectuée.

1.4.1.9. PARTICIPANTS

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

- **Porteur :** La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce certificat ;
- **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 porteur et 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, ...). Typiquement, dans une administration, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.
- **Validateur de Certificat (VC) :** Le validateur de certificat est désigné et placé sous la responsabilité de l'AE. Il s'agit d'une personne physique en charge de la validation des demandes émanant des RC.

1.4.2. AUTORITÉ D'ENREGISTREMENT (AE)

l'AE est en charge de la vérification des informations d'identification du Responsable du Certificat, du bénéficiaire dans le cas d'un certificat destiné à une personne physique, de la validité du formulaire de demande de certificat conformément aux notices décrivant le contenu attendu pour ce dernier. Si la demande est valide, elle est transmisse au service de génération des certificats.

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

1. Dans tous les cas :
   - 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 ;
   - L'établissement et la transmission de la demande de certificat à l'« AC Technique »;
   - 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.

2. Certificat pour un service applicatif :
   - La prise en compte et la vérification des informations du service applicatif ainsi que leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
3. Certificat pour un porteur :
   - La conservation et la protection en confidentialité et intégrité des données personnelles d'authentification du porteur ;
   - La prise en compte et la vérification des informations du futur porteur ainsi que leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;

Note : dans le cadre d'un certificat pour un porteur, le RC a un rôle de MC. Il est en charge de la vérification des informations concernant le futur porteur qu'il a sous sa responsabilité hiérarchique pour le compte de l'AE. De son côté l'AE vérifie que le RC est bien autorisé à demander un certificat pour le porteur en question.

1.4.3. RESPONSABLE DE CERTIFICATS

1.4.3.1. RC CERTIFICATS ÉLECTRONIQUES DE SERVICES APPLICATIFS

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 étant attaché au service applicatif et non au RC, en cas de changement de RC, l'entité doit le signaler à l'AC préalablement sauf cas exceptionnel et lui désigner un successeur sans délai.

L'AC révoque les certificats pour lesquels il n'y a plus de RC explicitement identifié.

1.4.3.2. RC CERTIFICATS POUR UN PORTEUR

Dans le cadre de la présente PC, un RC pour un porteur ne peut être qu'une personne physique qui est responsable de la demande d'attribution du certificat du porteur identifié dans ce certificat. Le RC a un lien hiérarchique avec le porteur et effectue pour le compte de l'AE les vérifications concernant l'identité du porteur.

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

1.4.4. PORTEURS DE CERTIFICATS

Dans le cadre de la présente PC, un porteur de certificat ne peut être qu'une personne physique qui utilise sa clé privée et le certificat électronique associé pour ses activités en lien avec l'entité, identifiée dans le certificat électronique, avec laquelle il a une relation contractuelle, hiérarchique ou réglementaire.

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

1.4.5. UTILISATEURS DE CERTIFICATS

1.4.5.1. AUTHENTIFICATION

Un utilisateur (ou accepteur) de certificats électroniques d'authentification serveur peut être notamment :

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

- Une personne accédant à un serveur et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat du serveur, afin d'établir une clé de session partagée entre son poste et le serveur ;
- Un service applicatif accédant à un serveur informatique et qui utilise un certificat et un applicatif de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, et afin d'établir une clé de session partagée entre les deux serveurs.

1.4.5.2.CACHET

Un utilisateur (ou accepteur) de certificats électroniques de cachet peut être notamment :

- Un usager destinataire de données signées par un service applicatif de cachet et qui utilise le certificat électronique du cachet ainsi qu'un module de vérification de cachet afin d'authentifier l'origine de ces données transmises ;
- Un service applicatif destinataire de données provenant d'un autre service applicatif et qui utilise le certificat électronique de cachet et un module de vérification de cachet afin d'authentifier l'origine de ces données transmises ;
- Un service applicatif qui signe des données électroniques.

1.4.5.3.SIGNATURE

Un utilisateur (ou accepteur) de certificats de signature électronique peut être notamment :

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

1.4.5.4.AUTHENTIFICATION ET SIGNATURE

Un utilisateur (ou accepteur) de certificats double usage signature électronique et authentification peut être notamment l'un de ceux identifiés pour les usages séparés de signature électronique et d'authentification (cf. Authentification et Signature).

1.4.6.AUTRES PARTICIPANTS

1.4.6.1.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.

1.4.6.2.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

1.5.1.1. BI-CLÉS ET CERTIFICATS

Les usages des certificats électroniques des services applicatifs sont les suivants :

- **Cachet serveur :**

  Signature électronique de données et la vérification de signature électronique. Ces données peuvent être, par exemple, un accusé de réception suite à la transmission d'informations par un usager à un service applicatif, une réponse automatique à une demande formulée par un usager, un jeton d'horodatage, un code applicatif, un certificat de répondeur OCSP, ou encore une archive.

- **Signature et Chiffrement de clés :**

  Signature électronique de données, vérification de signature électronique, chiffrement et déchiffrement de clés de sessions. Ce double usage est requis par des produits spécifiques, par exemple des produits de téléphonie.

- **Authentification serveur :**

  Authentification du serveur auprès d'autres serveurs ou auprès de personnes, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient protégés (intégrité, confidentialité).

  L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique par le client et chiffrement de cette clé symétrique avec la clé publique du serveur) ou de type Diffie-Hellman (obtention de la clé symétrique via un algorithme combinant la clé privée du client et la clé publique du serveur, et inversement).

Les usages des certificats électroniques des porteurs sont les suivants :

- **Authentification :**

  Authentification du porteur auprès de serveurs ou auprès d'autres porteurs, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient protégés (intégrité, confidentialité).

  L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique et chiffrement de cette clé symétrique avec la clé publique du serveur) ou de type Diffie-Hellman (obtention de la clé symétrique via un algorithme combinant la clé privée du client et la clé publique du serveur, et inversement).

- **Signature :**

  Signature électronique de données. Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

- **Authentification et signature :**

  L'ensemble de ceux identifiés ci-dessus pour les usages séparés d'authentification et de signature.

Les certificats électroniques objets de la présente PC sont utilisés par des services applicatifs ou porteurs pour lesquelles les besoins de sécurité sont moyens eu égard aux risques qui les menacent.

1.5.1.2. Bi-clés et certificats d'AC et de composantes

L'« AC Technique » dispose d'un seul bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur « ACR Infrastructure Justice ». La bi-clé de l'AC permet de signer et de vérifier les différents types d'objets qu'elle génère : certificats des services applicatifs, certificats des porteurs, LCR.

1.5.2. Domaines d'utilisation interdits

L'utilisation des certificats émis par l'« AC Technique » pour des usages autres que ceux prévus dans la présente PC sont interdits. Par conséquent, l'« AC Technique » 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'« AC Technique » respecte également ces restrictions d'usages et impose leur respect par les RC auxquels elle délivre des certificats de service applicatif, les porteurs et les utilisateurs de ces certificats.

A cette fin, l'AC publie à destination des RC, des porteurs 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 RC, porteurs et utilisateurs de certificats.

2.2. INFORMATIONS DEVANT ÊTRE PUBLIÉES

Les informations suivantes sont publiées à destination des RC, porteurs et utilisateurs de certificats sur le site internet public du Ministère de la Justice :

- la présente politique de certification dans sa version en cours de validité :
  - http://www.justice.gouv.fr/igc/sdit/mj_pc_ac-technique.pdf
- le certificat de l'« AC Technique » ;
  - http://www.justice.gouv.fr/igc/sdit/mj_ac-technique.cer
- la LCR de l'« AC Technique » ;
  - http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl
- le certificat de l'« ACR Infrastructure Justice » signataire de l'« AC Technique » :
  - http://www.justice.gouv.fr/igc/sdit/mj_acr-infra_justice.cer
- la LAR de l'« ACR Infrastructure Justice » signataire de l'« AC Technique » :
  - 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_ac-technique.pdf

Certain documents à destination du personnel du Ministère de la Justice (RC, VC, porteurs, ...) 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 CGU, 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 LCR est publiée 24 heures sur 24 et 7 jours sur 7 avec une fréquence de mise à jour toutes les 2 heures durant les heures ouvrées du service de gestion des révocations.

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'AC 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 de niveau « diffusion publique » sont publiées. Des documents comme la DPC, l'offre de service, ...ont des niveaux « diffusion restreinte » ou « diffusion élargie » et la consultation de ces derniers doit faire l'objet d'une demande auprès de l'AA-PEKIN ou est réservée à des personnels du Ministère de la Justice. Le respect de ces niveaux de confidentialité 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'« AC Technique » sont conformes aux spécifications de la norme X.500. Dans chaque certificat X.509v3, le champ « issuer » (AC émettrice, soit l'« AC Technique ») et le champ « subject » (porteur ou service applicatif) sont identifiés par un « Distinguish Name ».

Les noms utilisés dans le certificat de l'« AC Technique » sont définis dans Profils pour l'AC.

3.1.2. NÉCESSITÉ D'UTILISATION DE NOMS EXPLICITES

Les noms utilisés dans les champs « issuer » et « subject » des certificats des porteurs ou services applicatifs et du certificat de l'« AC Technique » sont explicites pour le Ministère de la Justice et toute personne devant les utiliser. Ainsi, ils identifient sans ambiguïté 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.

Dans le cas des porteurs, le CN est construit en utilisant son nom et son prénom.

Dans le cas des services applicatifs, le CN est construit par le RC en fonction des besoins du service. L'AA-PEKIN n'impose pas de règles strictes dans ce cas particuliers, mais veille à un usage ne pouvant pas engendrer de problématiques de sécurité (usage de FQDN de site web public, usage de nom de domaine n'appartenant pas au Ministère de la Justice, …).

3.1.2.1. CERTIFICAT DE L'AC TECHNIQUE

Le format exact du DN du certificat de l'« AC Technique » 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 = AC Technique

3.1.2.2. CERTIFICAT DE SERVICES APPLICATIFS OU PORTEURS

Le format exact du DN d'un certificat d'un service applicatif ou d'un porteur, signé par l'« AC Technique », 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 = AC Technique
Subject DN	C = FR O = Ministere de la Justice OU = 0002 110010014 CN = <identifiant du porteur ou du service applicatif>

3.1.3. ANONYMISATION OU PSEUDONYMISATION

L'anonymisation ou pseudonymisation des certificats des services applicatifs ou des porteurs 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

Le triplet O, OU, CN identifie de manière univoque le titulaire du certificat. Le numéro de série du certificat attribué par l'AC lors de la signature du certificat permet de distinguer les différents certificats que peut posséder un service applicatif ou un porteur.

Durant toute la durée de vie de l'AC, un DN attribué à un service applicatif ou un porteur de certificats ne sera pas attribué à un autre service applicatif ou porteur. Cette exigence est gérée par l'utilisation du CN du service applicatif ou du porteur lors de la création de l'entité au sein de l'IGC. Les entités ne pouvant pas être créées en doublon (impossibilité technique de l'IGC), il est garanti qu'un service applicatif ou un porteur ne pourra pas se voir attribuer le même DN qu'un autre (le CN étant le seul élément non fixe dans le DN).

3.1.6. IDENTIFICATION, AUTHENTIFICATION ET RÔLE DES MARQUES DÉPOSÉES

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

L'AC est responsable de l'unicité des noms des services applicatifs et porteurs 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. CERTIFICAT PORTEUR

L'enregistrement d'un porteur se fait par l'intermédiaire d'un RC de l'entité d'appartenance de ce dernier. Le RC est préalablement enregistré auprès de l'AE.

Lors de la demande de certificat, l'adresse email du porteur est vérifiée au travers de l'envoi d'un email contenant les données d'activation lui permettant ainsi de récupérer et d'utiliser son certificat.

3.2.2. CERTIFICAT DE SERVICE APPLICATIF

L'enregistrement d'un service applicatif pour lequel un certificat doit être délivré se fait via l'enregistrement du RC correspondant. Le RC est préalablement enregistré auprès de l'AE.

Lors de la demande de certificat, l'adresse email du RC est vérifiée au travers de l'envoi de plusieurs emails qui

permettent au RC de transmettre sa demande signée à l'AE et/ou à l'IGC de lui transmettre certaines données d'activation lui permettant ainsi de récupérer et d'utiliser le certificat du serveur.

Il est à noter que dans le cadre de l'IGC PEKIN, les RC sont nommés par l'AA-PEKIN au travers d'une liste exhaustive et nominative qui est diffusée auprès de l'AE pour validation lors du traitement des demandes.

3.2.3. Méthode pour prouver la possession de la clé privée

L'AC s'assure de la détention de la clé privée par le demandeur (RC pour un service applicatif ou porteur) avant de certifier la clé publique. La preuve de possession de la clé privée repose sur la vérification de la signature numérique de la requête de certificat du RC ou du porteur qui doit être au format PKCS#10.

3.2.4. Validation de l'identité d'un organisme

L'identité de l'organisme est préalablement validée par l'AA-PEKIN. L'« AC Technique » ne délivrant que des certificats pour des organismes 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.

3.2.5. Validation de l'identité d'un individu

L'AA-PEKIN nomme est maintient une liste exhaustive et nominative des RC de l'AC. De ce fait, la validation de l'identité d'un RC est explicite et repose sur la connaissance de la personne, de son service de rattachement et de sa position hiérarchique au sein du Ministère de la Justice.

La validation de l'identité d'un porteur est réalisée par le RC du service d'appartenance du porteur. De ce fait, la validation de l'identité d'un porteur repose sur la connaissance de la personne, de son service de rattachement et de sa position hiérarchique au sein du Ministère de la Justice.

Par ailleurs, l'AE dispose d'un accès à l'annuaire du Ministère de la Justice permettant une vérification de l'existence d'un porteur ou d'un RC.

3.2.6. Informations non vérifiées du porteur

Sans objet.

3.2.7. Validation de l'autorité du demandeur

La validation est effectuée en même temps que la procédure de validation de l'identité de la personne physique par l'AE ou par le RC.

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

L'AC n'émet pas de nouveau certificat pour la bi-clé d'un service applicatif ou d'un porteur déjà détenteur d'un certificat. Le renouvellement passe par la génération d'une nouvelle bi-clé et d'une nouvelle demande de certificat. 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.

3.3.1. Identification et validation pour un renouvellement courant

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

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 du certificat d'un service applicatif 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.

La procédure de révocation du certificat d'un porteur 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 ou si cela s'avère impossible, signé manière manuscrite par le porteur. Dans ce cas l'AE, effectuera des vérifications permettant de s'assurer qu'il s'agit bien d'une demande émanant du porteur.

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

4.1. DEMANDE DE CERTIFICAT

4.1.1. ORIGINE D'UNE DEMANDE DE CERTIFICAT

Un certificat peut être demandé par un RC dont dépend le service applicatif ou le porteur, et après consentement préalable du futur porteur dans le cas d'un certificat porteur.

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

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

- FQDN/Nom de service applicatif/CN à utiliser dans le cas d'un certificat serveur/cachet/porteur ;
- les données personnelles d'identification du RC ;
- les données d'identification du bénéficiaire (personne/service en charge de l'installation dans le cas d'un service applicatif)

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 ce service applicatif / porteur ;
- Validation du formulaire, sa signature, les éléments fournis.

Dans le cas de certificat pour un service applicatif, il n'y a pas de vérification par l'AE de l'identité du serveur. S'agissant de services applicatifs internes au Ministère de la Justice, il n'y a pas de nomenclature explicite et commune à tous ces services permettant une vérification. L'identité du serveur est par conséquent de la seule responsabilité du RC qui en est informé et en prend la pleine responsabilité.

Dans le cas de certificat porteur, de même, la vérification de l'identité du porteur est pleinement la responsabilité du RC. Cette vérification est simplifiée de par le fait que le porteur est un membre de l'entité d'appartenance du RC et dans la majorité des cas, le RC est un responsable hiérarchique direct ou indirect du porteur.

4.2.2. ACCEPTATION OU REJET DE LA DEMANDE

En cas de rejet de la demande, l'AE en informe le RC en justifiant le rejet.

4.2.3. Durée d'établissement du certificat

Conformément à l'offre de service PEKIN, la délivrance du certificat doit-être effective dans un délai de 5 jours ouvrés à réception de la demande complète.

4.3. Délivrance du certificat

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

Suite à la validation par l'AE et l'enregistrement de la demande de certificat sur l'IGC par l'AE, l'AC déclenche le processus de génération du certificat et la préparation des différents éléments destinés au RC ou au porteur (bi-clé du service applicatif ou du porteur, dispositif de protection associé, code d'activation, …).

Lorsque l'AC doit générer la bi-clé du service applicatif ou du porteur, le processus de génération du certificat est lié de manière sécurisée au processus de génération de la bi-clé : l'ordonnancement des opérations est assuré ainsi que l'intégrité et l'authentification des échanges entre les composantes de l'IGC. Par ailleurs, la clé privée est transmise de façon sécurisée au RC ou au porteur, en garantissant l'intégrité et la confidentialité.

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

Le certificat complet et exact est mis à disposition du RC ou du porteur qui le télécharge via le lien, l'identifiant et le code d'activation qu'il reçoit par email.

Dans le cas d'une génération de la bi-clé par l'AC :

- pour un service applicatif : le certificat et la bi-clé sont encapsulés par l'IGC dans un PKCS#12 protégé par un mot de passe généré aléatoirement et d'une force suffisante par rapport aux recommandations RGS. Le mot de passe et le PKCS#12 sont fournis au RC par email dans une enveloppe sécurisé par l'utilisation d'un outil de chiffrement qualifié par l'ANSSI et approuvé par le Ministère de la Justice pour cet usage ;
- pour un porteur : le certificat et la bi-clé sont encapsulés par l'IGC dans un PKCS#12 protégé par un mot de passe généré aléatoirement et d'une force suffisante par rapport aux recommandations RGS. Le PKCS#12 est envoyé au porteur par email , le mot de passe est transmis par téléphone au porteur par l'AE.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

Le téléchargement par le RC ou le porteur du certificat mis à disposition par l'AC vaut acceptation de ce dernier dans le cas de l'envoi par email du lien, de l'identifiant et du code d'activation du certificat. l'AC est informé du téléchargement du certificat par le RC ou le porteur.

Dans le cas de la fourniture par l'AC d'un PKCS#12, l'acceptation est tacite à compter de la transmission du PKCS#12 et du mot de passe par email au RC dans le cas d'un service applicatif, et à compter de la transmission du mot de passe par téléphone pour un porteur.

4.4.2. Publication du certificat

Les certificats des services applicatifs et des porteurs ne sont pas directement publiés par l'AC. Un mécanisme sur la plateforme de l'IGC permet néanmoins à un utilisateur de récupérer un certificat en fournissant le DN complet de ce dernier.

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

l'AC informe l'AE de la délivrance du certificat, qui se charge d'en informer le RC ou le porteur 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 RC ET LE PORTEUR

Les RC et les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats décrits au chapitre Domaines d'utilisation applicables. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé et du certificat associé est indiqué dans le certificat lui-même, via les extensions X.509 « Key Usage » et « Extended Key Usage ». Cet usage est également clairement explicité dans la présente PC, ainsi que dans les conditions générales d'utilisation du certificat électronique considéré.

4.5.2. UTILISATION DE LA CLÉ PUBLIQUE ET DU CERTIFICAT PAR L'UTILISATEUR DU CERTIFICAT

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

4.6. RENOUVELLEMENT D'UN CERTIFICAT

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 de certificat sans le renouvellement de la bi-clé correspondante. Ainsi, toute nouvelle demande de certificat 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 DE LA BI-CLÉ

4.7.1. CAUSES POSSIBLES DE CHANGEMENT DE LA BI-CLÉ

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des services applicatifs, des porteurs, et les certificats correspondants, sont renouvelés au moins tous les trois ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du service applicatif ou du porteur.

Note : Dans la suite du présent chapitre, le terme utilisé est "fourniture d'un nouveau certificat". Ce terme recouvre également, dans le cas où elle est générée par l'AC, la fourniture de la nouvelle bi-clé du service applicatif ou du porteur.

4.7.2. ORIGINE DE LA DEMANDE

Toutes les demandes de certificats devant être effectuées par l'intermédiaire d'un formulaire signé par un RC, le déclenchement de la fourniture d'un nouveau certificat, du point de vue de l'AC, est à l'initiative du RC que ce soit pour un porteur ou un service applicatif.

4.7.3. PROCÉDURES DE TRAITEMENT D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

La procédure est identique à un certificat initial (cf. Actions de l'AC concernant la délivrance du certificat).

4.7.4. NOTIFICATION DE L'ÉTABLISSEMENT D'UN NOUVEAU CERTIFICAT

Cf. Notification par l'AC de la délivrance du certificat

4.7.5. Démarches d'acceptation du nouveau certificat

Cf. Démarche d'acceptation du certificat

4.7.6. Publication du nouveau certificat

Cf. Publication du certificat

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

Cf. Notification par l'AC aux autres entités de la délivrance du 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 de la bi-clé) et autres qu'uniquement la modification des dates de validité (cf. Renouvellement d'un certificat).

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

4.9.1.1. Certificats de services applicatifs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un service applicatif :

- les informations du service figurant dans le certificat ne sont plus en conformité avec l'identité du service ou l'utilisation prévue dans le certificat (par exemple, modification du FQDN), ceci avant l'expiration normale du certificat ;
- le RC n'a pas respecté les modalités applicables d'utilisation du certificat ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- le RC n'a pas respecté ses obligations découlant de la présente PC ;
- la clé privée du service applicatif est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- le RC ou une entité autorisée demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du service applicatif et/ou de son support) ;
- l'arrêt définitif du service applicatif ou la cessation d'activité de l'entité du RC de rattachement du service applicatif.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC 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.

4.9.1.2. Certificats de porteurs

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur :

- les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple changement du nom de famille suite à un mariage), ceci

avant l'expiration normale du certificat ;

- le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le porteur n'a pas respecté ses obligations découlant de la présente PC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ;
- la clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- le porteur ou une entité autorisée demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur et/ou de son support) ;
- le décès du porteur ou la cessation d'activité de l'entité du porteur.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC 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.

4.9.1.3. Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'une composante de l'IGC :

- la clé privée de l'AC est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- la décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la présente PC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- la cessation d'activité de l'entité opérant la composante.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC 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

4.9.2.1. Certificats de services applicatifs

La révocation du certificat d'un service applicatif ne peut-être décidé que par :

- le RC ;
- l'AC émettrice du certificat ou son AE ;
- 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.

4.9.2.2. Certificats de porteurs

La révocation du certificat d'un porteur ne peut-être décidé que par :

- le porteur détenteur du certificat ;
- le RC ;

- l'AC émettrice du certificat ou son AE ;
- un représentant légal de l'entité ;
- les autorités judiciaires via une décision de justice.

Le porteur est informé des personnes ou entités susceptibles d'effectuer une demande de révocation pour son certificat.

4.9.2.3. Certificats d'une composante de l'IGC

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

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

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Révocation d'un certificat d'un service applicatif

Les exigences d'identification et de validation d'une demande de révocation sont décrites au chapitre Identification et validation d'une demande de révocation

Une demande de révocation se fait par l'usage du formulaire adéquat adressé à l'AE qui gère la fonction de demande de révocations pour l'AC. Ce formulaire doit notamment contenir les informations :

- RC demandant la révocation ;
- CN (révocation de tous les certificats) **ou** numéro de série (révocation d'un seul certificat) contenu dans le certificat du service applicatif à révoquer ;

Le formulaire signé par le RC est transmis pour validation auprès de l'AE. Une fois la demande authentifiée et contrôlée, l'AE révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est alors diffusée via une LCR signée par l'AC. le RC est informé de la révocation via la résolution d'un ticket correspondant à sa demande.

Note : l'AC ne publie jamais la cause de la révocation d'un certificat dans sa LCR.

4.9.3.2. Révocation d'un certificat d'un porteur

La procédure de révocation d'un certificat porteur est identique à celle d'un service applicatif et passe par le RC de l'entité à laquelle le porteur est rattachée.

Voir Certificats de porteurs pour le détail de la procédure.

4.9.3.3. Révocation d'un certificat d'une composante de l'IGC

Dans le cas où l'« ACR infrastructure Justice » décide de révoquer le certificat de l'« AC Technique » suite à la compromission de la clé privée de l'« AC Technique » ou de l'« ACR infrastructure Justice », cette dernière informe par mail l'ensemble des RC et des porteurs que leurs certificats 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.

4.9.4. Délai accordé pour formuler une demande de révocation

La demande de révocation d'un certificat d'un service applicatif ou d'un porteur 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 par l'AC d'une demande de révocation

4.9.5.1. Révocation d'un certificat de service applicatif ou porteur

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

4.9.5.2. Disponibilité du système de traitement des demandes de révocation

Toute demande de révocation d'un certificat d'un service applicatif ou porteur est traitée dans un délai inférieur à 24 heures (jours ouvrés), ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs (génération et publication d'une nouvelle LCR).

Note : ce délai peut être allongé 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.

4.9.5.3. Révocation d'un certificat d'une composante de l'IGC

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.

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/LAR des certificats de la chaîne de confiance.

4.9.7. Fréquence d'établissement et durée de validité des LCR

La LCR de l'AC est émise toutes les 2 heures sur le créneau journalier 7h00-23h00.

Afin d'assurer une continuité du service dans le cas où un incident sur la publication des LCR survient, la durée de validité de la LCR est fixée à 7 jours.

4.9.8. Délai maximal de publication d'une LCR

La LCR 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.

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 de services applicatifs ou porteurs, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, outre les exigences précisées au chapitre Révocation d'un certificat d'une composante de

l'IGC, la révocation suite à une compromission de la clé privée fait l'objet d'une information clairement diffusée aux RC, entités, utilisateurs du Ministère de la Justice et sur le site internet de l'AC.

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'AC est la consultation publique de son certificat et de sa LCR (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_crl_ac-technique.crl.

l'AC met également à disposition les certificats et LCR/LAR des AC constituant l'ensemble de sa chaine de certification. Ces certificats et LCR/LAR sont 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

4.11.1. Fin de relation entre le RC et l'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC et l'entité de rattachement du service applicatif avant la fin de validité du certificat de cette dernière, quelle qu'en soit la raison, le certificat est révoqué.

De plus, l'AC révoque tout certificat de service applicatif pour lequel il n'y a plus de RC explicitement identifié.

4.11.2. Fin de relation entre le porteur et l'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC et le porteur avant la fin de validité du certificat de ce dernier, quelle qu'en soit la raison, le certificat est révoqué.

4.12. SÉQUESTRE DE CLÉ ET RECOUVREMENT

Le séquestre des clés privées des services applicatifs et des porteurs est interdit dans la présente PC.

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. MESURES DE 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'AC 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'AC dans la présente PC, notamment en matière de disponibilité de ses fonctions de gestion des révocations, de publication et d'information sur l'état de validité des certificats.

5.1.5. PRÉVENTION ET PROTECTION INCENDIE

Les moyens de prévention et de lutte contre les incendies mis en œuvre par le Ministère de la Justice permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC, notamment en matière de

disponibilité de ses fonctions de gestion des révocations, de publication et d'information sur l'état de validité des certificats.

5.1.6. CONSERVATION DES SUPPORTS

Les mesures et moyens de conservation des supports d'informations mis en œuvre par le Ministère de la Justice permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC. En particulier la disponibilité, la confidentialité et l'intégrité des données conservées dans les journaux, les archives et les logiciels 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'AC 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'AC 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 sous 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'IGC 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'AC. 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'« AC Technique » qu'elle met en œuvre. Toute action liée à un certificat émis par l'« AC Technique » est enregistrée et un historique est conservé au sein de la base de données de l'« AC Technique » 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

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'AC (signature ou révocation d'un certificat, signature de la LCR, 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'« AC ».

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'« AC Technique » ;
- Les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les documents justificatifs des actions menées sur l'IGC (création, révocation, …) ;
- les dossiers de demande de certificat, de demande de 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 LCR 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'AC peut accéder à toutes ses archives.

5.6. CHANGEMENT DE CLÉ D'AC

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

Au regard de la date de fin de validité de ce certificat, son renouvellement 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'AC 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'« AC Technique », 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'« AC Technique » 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'« AC Technique » 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)).

Dans le cas de compromission d'une clé d'AC, le certificat correspondant sera immédiatement révoqué (cf. Révocation et suspension d'un certificat). Il en sera de même pour tous les certificats en cours de validité émis par l'AC.

En outre, l'AC respecte les engagements suivants :

- elle informe les RC, les porteurs, les utilisateurs ;
- elle indique que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

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'« AC Technique » :

- le transfert d'activité n'est pas prévu ;
- la cessation d'activité engendrera la révocation des certificats et la publication des LCR conformément aux engagements pris dans la présente PC.

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

- de la récupération et de la destruction de toutes les copies de sauvegarde du HSM de l'AC ;
- de révoquer le certificat de l'AC et dans la mesure du possible, de tous les certificats signés encore valides ;
- de révoquer les certificats des administrateurs de l'AC ;
- de publier une nouvelle LCR contenant tous les certificats révoqués ;
- de la destruction logique et/ou physique de la clé privée de l'AC sur le HSM ;
- d'informer les responsables de certificat, les administrateurs, les utilisateurs de la révocation effective du certificat de l'AC et de l'arrêt du service ;
- d'informer tous les RC, les porteurs, les utilisateurs et les autres composantes de l'IGC de la cessation d'activité ;
- 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

6.1.1.1. CLÉS D'AC

La génération du bi-clé de signature de l'AC est effectuée lors de la cérémonie des clés. Les clés de signature de l'AC 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.

6.1.1.2. CLÉS DU SERVICE APPLICATIF OU DU PORTEUR GÉNÉRÉES PAR L'AC

La génération des clés des services applicatifs ou des porteurs s'effectue dans un dispositif conforme aux exigences précisées dans l'Annexe 2 : Exigences de sécurité du dispositif de protection des éléments secrets. Les clés sont ensuite transférées de manière sécurisée au service applicatif ou au porteur.

6.1.1.3. CLÉS DU SERVICE APPLICATIF GÉNÉRÉES PAR LE RC

Le RC s'engage de manière contractuelle, en acceptant les CGU de l'IGC à :

- générer la clé privée dans un dispositif conforme aux exigences de l'Annexe 2 : Exigences de sécurité du dispositif de protection des éléments secrets ;
- respecter les exigences quant au dispositif qu'il utilise pour générer et stocker sa clé privée.

6.1.1.4. CLÉS DU PORTEUR GÉNÉRÉES PAR LE PORTEUR

Le porteur s'engage de manière contractuelle, en acceptant les CGU de l'IGC à :

- générer la clé privée dans un dispositif conforme aux exigences de l'Annexe 2 : Exigences de sécurité du dispositif de protection des éléments secrets ;
- respecter les exigences quant au dispositif qu'il utilise pour générer et stocker sa clé privée.

6.1.2. TRANSMISSION DE LA CLÉ PRIVÉE AU PROPRIÉTAIRE

Lorsque l'AC génère la bi-clé pour le service applicatif ou le porteur, la clé privée doit être transmise au RC ou au porteur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. La procédure de transmission est décrite au chapitre Notification par l'AC de la délivrance du certificat.

Une fois remise, la clé privée est sous le seul contrôle du RC ou du porteur et n'est ni dupliquée ni conservée par l'AC.

6.1.3. TRANSMISSION DE LA CLÉ PUBLIQUE À L'AC

Lorsque la bi-clé n'est pas générée par l'AC, la demande de certificat au format PKCS#10, contenant la clé publique du service applicatif, est transmise à l'AC par le RC ou le porteur sur la plateforme applicative de cette dernière. Le RC ou le porteur doit utiliser le lien, identifiant et mot de passe qu'il a reçu de l'AC pour s'authentifier sur la plateforme de l'AC et déposer la requête de certificat. L'AC vérifie la signature du PKCS#10 afin de s'assurer que le RC ou le porteur possède bien la clé privée correspondante à la clé publique objet de la demande de certificat. Cette vérification faite, l'AC signe la requête et délivre le certificat.

6.1.4. TRANSMISSION DE LA CLÉ PUBLIQUE AUX UTILISATEURS DE CERTIFICATS

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

la clé publique de l'« AC Technique » est de même diffusée dans un certificat qui est signé par l'« ACR Infrastructure Justice » et qui est intégré sur les postes du MJ et transmis aux AC subordonnées et/ou partenaires du MJ qui le nécessitent.

Par ailleurs, les clés publiques d'AC du MJ, ainsi que leurs valeurs de contrôle, sont diffusées et disponibles pour tout utilisateur sur le site du MJ à l'adresse : http://www.justice.gouv.fr/igc/sdit

6.1.5. TAILLE DES CLÉS

Les clés d'AC, des services applicatifs et des porteurs 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

6.1.6.1. Clés d'AC

Les équipements utilisés pour la génération des bi-clés de l'AC sont des ressources cryptographiques matérielles certifiées et qualifiées par l'ANSSI et respectent donc les normes de sécurité correspondant à la bi-clé (paramètres, algorithmes).

6.1.6.2. Clés des services applicatifs

Lorsque la clé est générée par l'AC, cette dernière utilise un dispositif qui respecte les normes de sécurité correspondant à la bi-clé (paramètres, algorithmes). Lorsque la clé est générée par un RC, ce dernier s'engage à utiliser un dispositif qui respecte les normes de sécurité correspondant à la bi-clé (paramètres, algorithmes). En cas de doute, le RC doit contacter l'AC afin de s'assurer du respect des normes de sécurité du dispositif utilisé.

6.1.6.3. Clés des porteurs

Lorsque la clé est générée par l'AC, cette dernière utilise un dispositif qui respecte les normes de sécurité correspondant à la bi-clé (paramètres, algorithmes). Lorsque la clé est générée par un porteur, ce dernier s'engage à utiliser un dispositif qui respecte les normes de sécurité correspondant à la bi-clé (paramètres, algorithmes). En cas de doute, le porteur doit contacter l'AC afin de s'assurer du respect des normes de sécurité du dispositif utilisé.

6.1.7. Objectifs d'usage de la clé

6.1.7.1. Clés d'AC

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

6.1.7.2. Clés des services applicatifs

L'utilisation de la clé privée du service applicatif et du certificat associé est strictement limitée à l'usage qui est spécifié dans le certificat. Les différents usages possibles pour les services applicatifs sont décrits au chapitre Bi-clés et certificats.

Dans le cadre d'un usage autre que celui spécifié dans le certificat, la responsabilité du RC pourrait être engagée.

6.1.7.3. Clés des porteurs

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à l'usage qui est spécifié dans le certificat. Les différents usages possibles pour les porteurs sont décrits au chapitre Bi-clés et certificats.

Dans le cadre d'un usage autre que celui spécifié dans le certificat, la responsabilité du porteur pourrait être engagée.

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

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1. Module cryptographique de l'AC

Le module cryptographique HSM « Hardware Security Module » utilisé par l'AC, 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.

6.2.1.2. Dispositif de protection des éléments secrets des porteurs

Lorsque le porteur utilise un dispositif pour protéger sa clé privée, ce dispositif doit être conforme avec les exigences de l'Annexe 2 : Exigences de sécurité du dispositif de protection des éléments secrets.

Dans le cas où l'AC fournit le dispositif au porteur, directement ou indirectement, l'AC s'assure que :

- La préparation du dispositif est contrôlée de façon sécurisée ;
- Le dispositif est stocké et distribué de façon sécurisée ;
- La désactivation et réactivation du dispositif est contrôlée de façon sécurisée.

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'AC. 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'AC n'est jamais exportée en clair en dehors du HSM et n'est pas séquestrée.

L'AC ne séquestre pas les clés privées des services applicatifs et des porteurs qu'elle certifie.

6.2.4. Copie de secours de la clé privée

La clé privée de l'AC 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.

L'AC ne fait aucune copie de secours des clés privées des services applicatifs et des porteurs qu'elle certifie.

6.2.5. Archivage de la clé privée

La clé privée de l'AC n'est pas archivée.

Les clés privées des services applicatifs et des porteurs que l'AC certifie ne sont pas archivées.

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

La clé privée de l'AC est générée, activée et stockée dans un HSM.

Quand elle n'est pas stockée dans un HSM ou lors de leur 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 dans des rôles de confiance.

6.2.7. Stockage de la clé privée dans un module cryptographique

La clé privée de l'AC 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

6.2.8.1. Clés privées d'AC

L'activation des clés privées de l'AC 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.

6.2.8.2. Clés privées des services applicatifs

L'activation initiale des clés privées des services applicatifs est contrôlée via des données d'activation qui sont utilisées par le dispositif du porteur. Il est ensuite de la responsabilité du RC de faire appliquer les exigences définies dans l'Annexe 2 : Exigences de sécurité du dispositif de protection des éléments secrets en tenant compte des contraintes d'usage et de disponibilité du service applicatif.

6.2.8.3. Clés privées des porteurs

L'activation des clés privées des porteurs est contrôlée via des données d'activation qui sont utilisées par le dispositif du porteur.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Clés privées d'AC

La désactivation des clés privées de l'AC dans le module cryptographique est automatique lorsque ce dernier est

arrêté ou redémarré. Dans le cas contraire, les clés privées de l'AC sont toujours opérationnelles afin de permettre le maintien du service opérationnel de l'AC.

Lorsqu'une clé privée d'AC n'a plus nécessité d'être active, la désactivation est réalisée par l'AA-PEKIN sur le logiciel de l'IGC.

6.2.9.2. Clés privées des services applicatifs

La méthode de désactivation des clés privées est dépendante du module cryptographique utilisé par le service applicatif.

6.2.9.3. Clés privées des porteurs

La méthode de désactivation des clés privées est dépendante du module cryptographique utilisé par le porteur.

6.2.10. Méthode de destruction de la clé privée

6.2.10.1. Clés privées d'AC

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

6.2.10.2. Clés privées des services applicatifs

Le RC, unique détenteur des clés privées, est le seul à pouvoir les détruire par un effacement ou une destruction physique du dispositif.

Dans le cas d'un dispositif géré par l'AC et pour lequel le RC n'aurait pas le droit d'effacement du contenu, il fera procéder à l'effacement des clés sous sa responsabilité.

6.2.10.3. Clés privées des porteurs

Le porteur, unique détenteur des clés privées, est le seul à pouvoir les détruire par un effacement ou une destruction physique du dispositif.

Dans le cas d'un dispositif géré par l'AC et pour lequel le porteur n'aurait pas le droit d'effacement du contenu, il fera procéder à l'effacement des clés sous sa responsabilité.

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.

Les dispositifs, lorsqu'ils sont physiques sont également certifiés.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Archivage des clés publiques

Les clés publiques de l'AC, des services applicatifs et des porteurs sont archivées dans le cadre de l'archivage des certificats correspondant pendant les périodes de validités des certificats.

6.3.2. Durée de vie des bi-clés et des certificats

Les bi-clés et les certificats des services applicatifs et des porteurs couverts par la présente PC ont une durée de vie maximale de 3 ans.

La durée de validité du certificat de l'AC est de 10 ans et celui de l'AC Racine émettrice est de 24 ans.

La présence PC garantit que l'AC n'émet pas de certificats dont la fin de validité serait postérieure à celle du certificat de l'AC.

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

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

La génération et l'installation des données d'activation du module cryptographique de l'AC se font lors de la phase d'initialisation et de personnalisation de ce module (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'AC 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.

6.4.1.2. Génération et installation des données d'activation correspondant à la clé privée du service applicatif

Lorsque l'AC génère la clé privée du service applicatif, elle génère également les données d'activation qui permettent au RC d'utiliser cette dernière. Ces données sont générées selon une politique stricte qui est en adéquation avec les recommandations de l'ANSSI au moment de la génération. Ces données d'activation sont adressées au RC par email dans un conteneur chiffré à son unique attention.

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

Lorsque l'AC génère la clé privée du porteur, elle génère également les données d'activation qui permettent au porteur d'utiliser cette dernière. Ces données sont générées selon une politique stricte qui est en adéquation avec les recommandations de l'ANSSI au moment de la génération. Ces données d'activation sont adressées au porteur :

- par email lorsque le porteur doit venir demander la génération par l'AC de sa clé privée sur le logiciel de l'IGC (il télécharge alors le PKCS#12 généré par l'AC et protégé avec le mot de passe reçu) ;
- par téléphone lorsque l'AE se charge de demander la génération par l'AC de sa clé privée sur le logiciel de l'IGC. Il reçoit alors le PKCS#12 par email et le mot de passe est communiqué par téléphone.

6.4.2. Protection des données d'activation

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

Les données d'activation 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.

6.4.2.2. Protection des données d'activation correspondant à la clé privée du service applicatif

Lorsque la clé privée est générée par l'AC, les données d'activation des dispositifs de protection des clés privées des services applicatifs, générées par l'AC, sont protégées en intégrité et en confidentialité jusqu'à la remise aux porteurs.

Les données d'activation ne sont pas conservées par l'AC ou si nécessaire, le sont en étant protégées en intégrité et en confidentialité.

6.4.2.3. PROTECTION DES DONNÉES D'ACTIVATION CORRESPONDANT À LA CLÉ PRIVÉE DU SERVICE PORTEUR

Lorsque la clé privée est générée par l'AC, les données d'activation des dispositifs de protection des clés privées des porteurs, générées par l'AC, sont protégées en intégrité et en confidentialité jusqu'à la remise aux porteurs.

Les données d'activation ne sont pas conservées par l'AC ou si nécessaire, le sont en étant protégées en intégrité et en confidentialité.

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

6.6.1. 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.

6.6.2. 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.

6.6.3. 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'AC, mais une datation des évènements qui permet, à partir d'une date fournie par le système d'exploitation de l'AC 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

Tous les certificats émis par l'IGC PEKIN sont au format X.509 v3 et les LCR au format X.509 v2. l'IGC PEKIN n'implémente pas de mécanisme OCSP.

Nous présentons ci-dessous, les profils du certificat et de la LCR de l'AC et les profils des différents certificats qu'elle peut émettre dans le cadre de la présente PC pour les services applicatifs et les porteurs.

7.1. PROFILS POUR L'AC

Les informations de profil du certificat de l'« AC Technique », ainsi que de la LCR qu'elle émet, sont présentés ci-dessous.

7.1.1. PROFIL DU CERTIFICAT DE L'« AC TECHNIQUE »

	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=AC Technique** **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 : 1**
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
	Certificate Policies		**1.2.250.1.120.3.3.1**
	Key Usage	**O**	**Certificate Sign, CRL Sign**

	CRL Distribution Points		**URI : http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl**

7.1.2. PROFILS DE LA LISTE DES CERTIFICATS RÉVOQUÉS DE L'« AC TECHNIQUE »

Les LCR émises par l'« AC Technique » 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 LCR>
	Next Update		<Last Update + 7 jours>
	Issuer DN		**CN=AC Technique** **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) »

7.2. PROFILS POUR LES SERVICES APPLICATIFS

Les informations de profil des certificats pour les services applicatifs, gérés par l'AC dans le cadre de la présente PC, sont présentées ci-dessous.

7.2.1. AUTHENTIFICATION

	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 + 1096 jours>
	Issuer DN		**CN=ACR Technique** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**

	Subject DN		**CN=**<valeur demandée par le RC> **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject Public key Info - Public Key Algorithm - Modulus		**rsaEncryption** <clef publique au format DER (2048 ou 4096 bits)>
	Signature Algorithm		**sha512WithRSAEncryption**
X.509 v3 Extensions	Subject Key Identifier		<SHA-1 de la clé publique du Subject>
	Basic Constraints	**O**	**CA :FALSE**
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
	Certificate Policies		**1.2.250.1.120.3.3.202.1**
	Key Usage	**O**	**Digital Signature, Key Encipherment**
	Extended Key Usage		**Server Authentication**
	CRL Distribution Points		**URI : http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl**

7.2.2. CACHET

	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 + 1096 jours>
	Issuer DN		**CN=ACR Technique** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject DN		**CN=**<valeur demandée par le RC> **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject Public key Info - Public Key Algorithm - Modulus		**rsaEncryption** <clef publique au format DER (2048 ou 4096 bits)>

	Signature Algorithm		**sha512WithRSAEncryption**
X.509 v3 Extensions	Subject Key Identifier		<SHA-1 de la clé publique du Subject>
	Basic Constraints	**O**	**CA :FALSE**
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
	Certificate Policies		**1.2.250.1.120.3.3.205.1**
	Key Usage	**O**	**Digital Signature, Non Repudiation**
	CRL Distribution Points		**URI : http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl**

7.2.3. AUTHENTIFICATION IPSEC

	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 + 1096 jours>
	Issuer DN		**CN=ACR Technique** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject DN		**CN=**<valeur demandée par le RC> **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject Public key Info - Public Key Algorithm - Modulus		**rsaEncryption** <clef publique au format DER (2048 ou 4096 bits)>
	Signature Algorithm		**sha512WithRSAEncryption**
X.509 v3 Extensions	Subject Key Identifier		<SHA-1 de la clé publique du Subject>
	Basic Constraints	**O**	**CA :FALSE**
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
	Certificate Policies		**1.2.250.1.120.3.3.209.1**
	Key Usage	**O**	**Digital Signature, Key Encipherment,** **Key Agreement**
	Extended Key Usage		**Server Authentication, IPSec IKE**

	CRL Distribution Points		**URI : http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl**

7.2.4. SIGNATURE DE CODE

	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 + 1096 jours>
	Issuer DN		**CN=ACR Technique** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject DN		**CN=**<valeur demandée par le RC> **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject Public key Info - Public Key Algorithm - Modulus		 **rsaEncryption** <clef publique au format DER (2048 ou 4096 bits)>
	Signature Algorithm		**sha512WithRSAEncryption**
X.509 v3 Extensions	Subject Key Identifier		<SHA-1 de la clé publique du Subject>
	Basic Constraints	**O**	**CA :FALSE**
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
	Certificate Policies		**1.2.250.1.120.3.3.210.1**
	Key Usage	**O**	**Digital Signature**
	Extended Key Usage		**Code Signing**
	CRL Distribution Points		**URI : http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl**

7.2.5. HORODATAGE

	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 + 1096 jours>
	Issuer DN		**CN=ACR Technique** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject DN		**CN=**<valeur demandée par le RC> **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject Public key Info - Public Key Algorithm - Modulus		**rsaEncryption** <clef publique au format DER (1024, 2048 ou 4096 bits)>
	Signature Algorithm		**sha512WithRSAEncryption**
X.509 v3 Extensions	Subject Key Identifier		<SHA-1 de la clé publique du Subject>
	Basic Constraints	**O**	**CA :FALSE**
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
	Certificate Policies		**1.2.250.1.120.3.3.203.1**
	Key Usage	**O**	**Digital Signature, Non Repudiation**
	Extended Key Usage	**O**	**Time Stamping**
	CRL Distribution Points		**URI : http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl**

7.3. PROFILS POUR LES PORTEURS

Les informations de profil des certificats pour les porteurs, gérés par l'AC dans le cadre de la présente PC, sont présentés ci-dessous.

7.3.1. AUTHENTIFICATION

	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 + 1096 jours>

	Issuer DN		**CN=ACR Technique** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject DN		**CN=**<valeur demandée par le RC> **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject Public key Info - Public Key Algorithm - Modulus		**rsaEncryption** <clef publique au format DER (2048 ou 4096 bits)>
	Signature Algorithm		**sha512WithRSAEncryption**
X.509 v3 Extensions	Subject Key Identifier		<SHA-1 de la clé publique du Subject>
	Basic Constraints	**O**	**CA :FALSE**
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
	Certificate Policies		**1.2.250.1.120.3.3.201.1**
	Key Usage	**O**	**Digital Signature**
	Extended Key Usage		**Client Authentication**
	CRL Distribution Points		**URI : http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl**

7.3.2. AUTHENTIFICATION IPSEC

	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 + 1096 jours>
	Issuer DN		**CN=ACR Technique** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**

	Subject DN		**CN=**<valeur demandée par le porteur> **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject Public key Info - Public Key Algorithm - Modulus		**rsaEncryption** <clef publique au format DER (2048 ou 4096 bits)>
	Signature Algorithm		**sha512WithRSAEncryption**
X.509 v3 Extensions	Subject Key Identifier		<SHA-1 de la clé publique du Subject>
	Basic Constraints	**O**	**CA :FALSE**
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
	Certificate Policies		**1.2.250.1.120.3.3.208.1**
	Key Usage	**O**	**Digital Signature, Key Encipherment,** **Key Agreement**
	Extended Key Usage		**Client Authentication, IPSec IKE**
	CRL Distribution Points		**URI : http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl**

7.3.3. SIGNATURE

	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 + 1096 jours>
	Issuer DN		**CN=ACR Technique** **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**
	Subject DN		**CN=**<valeur demandée par le porteur> **OU=0002 110010014** **O=Ministere de la Justice** **C=FR**

	Subject Public key Info - Public Key Algorithm - Modulus		**rsaEncryption** <clef publique au format DER (2048 ou 4096 bits)>
	Signature Algorithm		**sha512WithRSAEncryption**
X.509 v3 Extensions	Subject Key Identifier		<SHA-1 de la clé publique du Subject>
	Basic Constraints	**O**	**CA :FALSE**
	Authority Key Identifier		<SHA-1 de la clé publique de l'Issuer>
	Certificate Policies		**1.2.250.1.120.3.3.207.1**
	Key Usage	**O**	**Non Repudiation**
	CRL Distribution Points		**URI : http://www.justice.gouv.fr/igc/sdit/mj_crl_ac-technique.crl**

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'AC ;
- Les clés privées de l'AC, des composantes, des services applicatifs et des porteurs ;
- Les données d'activation associées aux clés privées de l'AC, des services applicatifs et des porteurs ;
- 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 services applicatifs et des porteurs ;
- les causes de révocations des certificats ;
- les documents à destination unique des personnels du MJ (formulaires de demandes, notices, offre de service, ...)

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 services applicatifs et des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur) ;
- les dossiers d'enregistrement des RC et des porteurs.

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'AC a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un service applicatif et que le RC correspondant a accepté le certificat ;
- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un porteur et que ce dernier 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 RC et les porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un RC et l'AC ou entre un porteur et l'AC est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC est responsable de la conformité de sa Politique de Certification, avec les exigences émises dans la présente PC. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la présente PC, par elle-même ou l'une de ses composantes. Elle 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'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'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 du service applicatif 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 du service applicatif ;
- Respecter les conditions d'utilisation de la clé privée du service applicatif et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans le certificat du service applicatif ;
- Faire, sans délai, une demande de révocation du certificat du service applicatif 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. PORTEURS DE CERTIFICATS

Le porteur a le devoir de :

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

9.6.5. 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.

9.6.6. AUTRES PARTICIPANTS

Sans objet.

9.7. LIMITE DE GARANTIE

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

- L'identification et l'authentification de l'AC avec son certificat ;
- L'identification et l'authentification des services applicatifs et des porteurs avec les certificats générés par l'AC ;
- 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'AC.

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'AC 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'AC et respecter les engagements avec les services applicatifs et les porteurs. 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.

Les détails sont fournis dans la DPC associée à la présente PC.

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'AC 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'AC 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 LCR) 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'AC 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 : EXIGENCES DE SÉCURITÉ DU DISPOSITIF DE PROTECTION DES ÉLÉMENTS SECRETS

11.1. EXIGENCES SUR LES OBJECTIFS DE SÉCURITÉ

Le dispositif de protection des éléments secrets du service applicatif ou du porteur, utilisé par le service applicatif ou le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- si la bi-clé est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction des clés privées ;
- assurer la confidentialité et l'intégrité des clés privées ;
- assurer la correspondance entre la clé privée et la clé publique ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif ;
- assurer la fonction de sécurité pour le service applicatif ou le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers.

11.2. EXIGENCES SUR LA QUALIFICATION

Le dispositif de protection des clés privées fourni par l'AC ou utilisé par le RC ou le porteur est une solution matérielle ou logicielle respectant les exigences du chapitre Exigences sur les objectifs de sécurité. Dans le cadre de solution logicielle, les exigences pourront être respectées par des mesures de sécurité additionnelles propres à l'environnement dans lequel la clé privée est déployée.

12. ANNEXE 3 : 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)