



**JOURNAUX
OFFICIELS**

Française
Services du Premier Ministre

**POLITIQUES DE CERTIFICATION
DIRECTION DES JOURNAUX OFFICIELS**

**AUTORITE DE CERTIFICATION
JO PUBLICATION**

CERTIFICATS DE SIGNATURE

Version/Révision :	1.0
Date de rédaction :	30/01/2006
Référence physique :	JO_PC_ACPublicationSignature
OID :	1.250.1.144.1.1.2.1

Sommaire

1.	INTRODUCTION	10
1.1.	Présentation générale.....	10
1.2.	Convention d'écriture	10
1.3.	Identification du document	10
1.4.	Entités intervenant dans l'IGC	10
1.4.1.	Autorités de certifications	10
1.4.1.1.	Autorité de certification JO Racine (AC JO Racine)	12
1.4.1.2.	Autorité de certification JO Publication (AC JO Publication).....	13
1.4.1.3.	Autorité de certification JO Infra (AC JO Infra)	13
1.4.1.4.	Autorité de certification JO Codes (AC JO Codes)	13
1.4.1.5.	Autorité de certification JO Rôles (AC JO Roles)	13
1.4.1.6.	Autorité de certification JO Agents (AC JO Agents)	14
1.4.2.	Autorité d'enregistrement	14
1.4.3.	Porteurs de certificats	14
1.4.4.	Utilisateurs de certificats	15
1.5.	Usage des certificats.....	15
1.5.1.	Domaines d'utilisation applicables	15
1.5.1.1.	Bi-clés et certificats des porteurs	15
1.5.1.2.	Bi-clés et certificats d'AC et de composantes	16
1.5.2.	Domaines d'utilisation interdits	16
1.6.	Gestion de la PC	17
1.6.1.	Entité gérant la PC	17
1.6.2.	Point de contact	17
1.6.3.	Entité déterminant la conformité d'une DPC avec cette PC	17
1.6.4.	Procédures d'approbation de la conformité de la DPC.....	17
1.7.	Définitions et acronymes.....	17
1.7.1.	Termes communs à la PRIS	19
1.7.2.	Termes spécifiques ou complétés / adaptés pour la présente PC	20
2.	RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES	22
2.1.	Entités chargées de la mise à disposition des informations	22
2.2.	Informations devant être publiées.....	22
2.3.	Délais et fréquences de publication	22
2.4.	Contrôle d'accès aux informations publiées	23
3.	IDENTIFICATION ET AUTHENTIFICATION.....	24
3.1.	Nommage.....	24
3.1.1.	Types de noms.....	24
3.1.2.	Nécessité d'utilisation de noms explicites	24
3.1.3.	Règles d'interprétation des différentes formes de nom	24
3.1.4.	Unicité de Noms	24
3.1.5.	Identification, authentification et rôle de marques déposées.....	25
3.2.	Validation initiale de l'identité.....	25
3.2.1.	Méthode pour prouver la possession de la clé privée	25
3.2.2.	Validation de l'identité de l'organisme.....	25
3.2.3.	Validation de l'identité d'un individu	25

3.2.3.1.	Enregistrement d'un porteur sans MC	25
3.2.3.2.	Enregistrement d'un MC.....	26
3.2.3.3.	Enregistrement d'un porteur via un MC	26
3.2.4.	Informations non vérifiées du porteur	26
3.2.5.	Validation de l'autorité du demandeur (entité de rattachement).....	26
3.2.6.	Critères d'interopérabilité	26
3.3.	Identification et validation d'une demande de renouvellement des clés.....	26
3.3.1.	Identification et validation pour un renouvellement courant.....	26
3.3.2.	Identification et validation pour un renouvellement après révocation.....	26
3.4.	Identification et validation d'une demande de révocation.....	27
4.	EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	28
4.1.	Demande de certificat.....	28
4.1.1.	Origine d'une demande de certificat	28
4.1.2.	Processus et responsabilités pour l'établissement d'une demande de certificat.....	28
4.2.	Traitement de la demande	28
4.2.1.	Exécution des processus d'identification et de validation de la demande	28
4.2.2.	Acceptation ou rejet de la demande	28
4.2.3.	Durée d'établissement du certificat.....	29
4.3.	Délivrance du certificat.....	29
4.3.1.	Actions de l'AC concernant la délivrance du certif.....	29
4.3.2.	Notification par l'AC de la délivrance du certificat au porteur	29
4.4.	Acceptation du certificat.....	29
4.4.1.	Démarche d'acceptation du certificat.....	29
4.4.2.	Publication du certificat	29
4.4.3.	Notification par l'AC aux autres entités de la délivrance du certificat	29
4.5.	Usages de la bi-clé et du certificat.....	29
4.5.1.	Utilisation de la clé privée et du certificat par le porteur	29
4.5.2.	Utilisation de la clé publique et du certificat par l'utilisateur du certificat ...	30
4.6.	Renouvellement d'un certificat.....	30
4.6.1.	Causes possibles de renouvellement d'un certificat	30
4.6.2.	Origine d'une demande de renouvellement.....	30
4.6.3.	Procédure de traitement d'une demande de renouvellement.....	30
4.6.4.	Notification au porteur de l'établissement du nouveau certificat.....	30
4.6.5.	Démarche d'acceptation du nouveau certificat.....	30
4.6.6.	Publication du nouveau certificat	30
4.6.7.	Notification par l'AC aux autres entités de la délivrance du nouveau certificat.....	30
4.7.	Délivrance d'un nouveau certificat suite à changement de la bi-clé.....	30
4.7.1.	Causes possibles de changement d'une bi-clé.....	30
4.7.2.	Origine d'une demande d'un nouveau certificat.....	31
4.7.3.	Procédure de traitement d'une demande d'un nouveau certificat.....	31
4.7.4.	Notification au porteur de l'établissement du nouveau certificat.....	31
4.7.5.	Démarche d'acceptation du nouveau certificat.....	31
4.7.6.	Publication du nouveau certificat	31
4.7.7.	Notification par l'AC aux autres entités de la délivrance du nouveau certificat.....	31
4.8.	Modification du certificat	31
4.8.1.	Causes possibles de modification d'un certificat	31
4.8.2.	Origine d'une demande de modification d'un certificat	31

4.8.3.	Procédure de traitement d'une demande de modification d'un certificat ...	32
4.8.4.	Notification au porteur de l'établissement du certificat modifié	32
4.8.5.	Démarche d'acceptation du certificat modifié	32
4.8.6.	Publication du certificat modifié	32
4.8.7.	Notification par l'AC aux autres entités de la délivrance du certificat modifié	32
4.9.	Révocation et suspension des certificats.....	32
4.9.1.	Causes possibles d'une révocation	32
4.9.1.1.	Certificats de porteurs	32
4.9.1.2.	Certificats d'une composante de l'IGC	32
4.9.2.	Origine d'une demande de révocation	33
4.9.2.1.	Certificats de porteurs	33
4.9.2.2.	Certificats d'une composante de l'IGC	33
4.9.3.	Procédure de traitement d'une demande de révocation	33
4.9.3.1.	Révocation d'un certificat de porteur.....	33
4.9.3.2.	Révocation d'un certificat d'une composante de l'IGC.....	34
4.9.4.	Délai accordé au porteur pour formuler la demande de révocation	34
4.9.5.	Délai de traitement par l'AC d'une demande de révocation	34
4.9.5.1.	Révocation d'un certificat de porteur.....	34
4.9.5.2.	Révocation d'un certificat d'une composante de l'IGC.....	34
4.9.6.	Exigences de vérification de la révocation par les utilisateurs de certificats	35
4.9.7.	Fréquence d'établissement des LCR.....	35
4.9.8.	Délai maximum de publication d'une LCR	35
4.9.9.	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats.....	35
4.9.10.	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats.....	35
4.9.11.	Autres moyens disponibles d'information sur les révocations	35
4.9.12.	Exigences spécifiques en cas de compromission de la clé privée	35
4.9.13.	Causes possibles d'une suspension	35
4.9.14.	Origine d'une demande de suspension	35
4.9.15.	Procédure de traitement d'une demande de suspension	36
4.9.16.	Limites de la période de suspension d'un certificat	36
4.10.	Fonction d'information sur l'état des certificats	36
4.10.1.	Caractéristiques opérationnelles.....	36
4.10.2.	Disponibilité de la fonction	36
4.10.3.	Dispositifs optionnels	36
4.11.	Fin de la relation entre le porteur et l'AC	36
4.12.	Séquestre de clé et recouvrement.....	36
4.12.1.	Politique et pratiques de recouvrement par séquestre des clés.....	36
4.12.2.	Politique et pratiques de recouvrement par encapsulation des clés de session	36
5.	MESURES DE SECURITE NON TECHNIQUES	37
5.1.	Mesures de sécurité physique	37
5.1.1.	Situation géographique et construction des sites	37
5.1.2.	Accès physique	37
5.1.3.	Alimentation électrique et climatisation.....	37
5.1.4.	Vulnérabilité aux dégâts des eaux	37
5.1.5.	Prévention et protection incendie.....	37
5.1.6.	Conservation des supports	38

5.1.7.	Mise hors service des supports	38
5.1.8.	Sauvegardes hors site	38
5.2.	Mesures de sécurité procédurales	38
5.2.1.	Rôles de confiance.....	38
5.2.2.	Nombre de personnes requises par tâches	39
5.2.3.	Identification et authentification pour chaque rôle	39
5.2.4.	Rôles exigeant une séparation des attributions.....	40
5.3.	Mesures de sécurité vis-à-vis du personnel	40
5.3.1.	Qualifications, compétences et habilitations requises	40
5.3.2.	Procédures de vérification des antécédents	40
5.3.3.	Exigences en matière de formation initiale	40
5.3.4.	Exigences et fréquence en matière de formation continue.....	41
5.3.5.	Fréquence et séquence de rotation entre différentes attributions	41
5.3.6.	Sanctions en cas d'actions non autorisées.....	41
5.3.7.	Exigences vis-à-vis du personnel des prestataires externes.....	41
5.3.8.	Documentation fournie au personnel	41
5.4.	Procédures de constitution des données d'audit.....	41
5.4.1.	Type d'évènements à enregistrer.....	41
5.4.2.	Fréquence de traitement des journaux d'évènements.....	42
5.4.3.	Période de conservation des journaux d'évènements	43
5.4.4.	Protection des journaux d'évènements	43
5.4.5.	Procédure de sauvegarde des journaux d'évènements.....	43
5.4.6.	Système de collecte des journaux d'évènements.....	43
5.4.7.	Notification de l'enregistrement d'un évènement au responsable de l'évènement.....	43
5.4.8.	Evaluation des vulnérabilités.....	43
5.5.	Archivage des données	44
5.5.1.	Types de données à archiver.....	44
5.5.2.	Période de conservation des archives	44
5.5.3.	Protection des archives.....	44
5.5.4.	Procédure de sauvegarde des archives	45
5.5.5.	Exigences d'horodatage des données.....	45
5.5.6.	Système de collecte des archives.....	45
5.5.7.	Procédures de récupération et de vérification des archives	45
5.6.	Changement de clé d'AC	45
5.7.	Reprise suite à compromission et sinistre	45
5.7.1.	Procédures de remontée et de traitement des incidents et des compromissions	45
5.7.2.	Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)	46
5.7.3.	Procédures de reprise en cas de compromission de la clé privée d'une composante.....	46
5.7.4.	Capacités de continuité d'activité suite à un sinistre.....	46
5.8.	Fin de vie de l'IGC.....	46
6.	MESURES DE SECURITE TECHNIQUES	48
6.1.	Génération et installation de bi clés.....	48
6.1.1.	Génération des bi-clés	48
6.1.1.1.	Clés d'AC.....	48
6.1.1.2.	Clés porteurs générées par l'AC	48
6.1.1.3.	Clés porteurs générées par le porteur	48

6.1.2.	Transmission de la clé privée à son propriétaire	48
6.1.3.	Transmission de la clé publique à l'AC	49
6.1.4.	Transmission de la clé publique de l'AC aux utilisateurs de certificats	49
6.1.5.	Tailles des clés	49
6.1.6.	Vérification de la génération des paramètres des bi-clés et de leur qualité	49
6.1.7.	Objectifs d'usage de la clé	49
6.2.	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques	49
6.2.1.	Standards et mesures de sécurité pour les modules cryptographiques	49
6.2.1.1.	Modules cryptographiques de l'AC	49
6.2.1.2.	Dispositifs d'authentification des porteurs	49
6.2.2.	Contrôle de la clé privée par plusieurs personnes	49
6.2.3.	Séquestre de la clé privée	50
6.2.4.	Copie de secours de la clé privée	50
6.2.5.	Archivage de la clé privée	50
6.2.6.	Transfert de la clé privée vers / depuis le module cryptographique	50
6.2.7.	Stockage de la clé privée dans un module cryptographique	50
6.2.8.	Méthode d'activation de la clé privée	50
6.2.8.1.	Clés privées d'AC	50
6.2.8.2.	Clés privées des porteurs	50
6.2.9.	Méthode de désactivation de la clé privée	51
6.2.9.1.	Clés privées d'AC	51
6.2.9.2.	Clés privées des porteurs	51
6.2.10.	Méthode de destruction des clés privées	51
6.2.10.1.	Clés privées d'AC	51
6.2.10.2.	Clés privées des porteurs	51
6.2.11.	Niveau d'évaluation sécurité du module cryptographique	51
6.3.	Autres aspects de la gestion des bi-clés	51
6.3.1.	Archivage des clés publiques	51
6.3.2.	Durées de vie des bi-clés et des certificats	51
6.4.	Données d'activation	52
6.4.1.	Génération et installation des données d'activation	52
6.4.1.1.	VI.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC	52
6.4.1.2.	Génération et installation des données d'activation correspondant à la clé privée du porteur	52
6.4.2.	Protection des données d'activation	52
6.4.2.1.	Protection des données d'activation correspondant à la clé privée de l'AC	52
6.4.2.2.	Protection des données d'activation correspondant aux clés privées des porteurs	52
6.4.3.	Autres aspects liés aux données d'activation	52
6.5.	Mesures de sécurité des systèmes informatiques	52
6.5.1.	Exigences de sécurité technique spécifiques aux systèmes informatiques	52
6.5.2.	Niveau d'évaluation sécurité des systèmes informatiques	53
6.6.	Mesures de sécurité des systèmes durant leur cycle de vie	53
6.7.	Mesures de sécurité liées au développement des systèmes	53
6.7.1.	Mesures liées à la gestion de la sécurité	53
6.7.2.	Niveau d'évaluation sécurité du cycle de vie des systèmes	53
6.8.	Mesures de sécurité réseau	53

6.9.	Horodatage / Système de datation	53
7.	PROFILS DES CERTIFICATS, OCSP ET DES LCR.....	54
7.1.	Profil des certificats	54
7.1.1.	Numéro de version.....	54
7.1.2.	Champs de base	54
7.1.3.	Extensions du certificat de signature des publications	54
7.1.4.	Extensions du certificat de signature des jetons d'horodatage.....	55
7.1.5.	OID des algorithmes	56
7.1.6.	Forme des noms	56
7.1.7.	Contraintes sur les noms	56
7.1.8.	OID des PC	56
7.1.9.	Utilisation de l'extension « contraintes de politique »	57
7.1.10.	Sémantique et syntaxe des qualificants de politique.....	57
7.1.11.	Sémantiques de traitement des extensions critiques de la PC.....	57
7.2.	Profil des LCR.....	57
7.2.1.	Numéro de version.....	57
7.2.2.	Champs de base	57
7.2.3.	Extensions de LCR et d'entrées de LCR	57
8.	AUDIT DE CONFORMITE ET AUTRES EVALUATIONS	59
8.1.	Fréquences et / ou circonstances des évaluations.....	59
8.2.	Identités / qualifications des évaluateurs	59
8.3.	Relations entre évaluateurs et entités évaluées	59
8.4.	Sujets couverts par les évaluations	59
8.5.	Actions prises suite aux conclusions des évaluations	59
8.6.	Communication des résultats.....	60
9.	AUTRES PROBLEMATIQUES METIERS ET LEGALES.....	61
9.1.	Tarifs 61	
9.1.1.	Tarifs pour la fourniture ou le renouvellement de certificats	61
9.1.2.	Tarifs pour accéder aux certificats	61
9.1.3.	Tarifs pour accéder aux informations d'état et de révocation des certificats61	
9.1.4.	Tarifs pour d'autres services	61
9.1.5.	Politique de remboursement	61
9.2.	Responsabilité financière.....	61
9.2.1.	Couverture par les assurances	61
9.2.2.	Autres ressources	61
9.2.3.	Couverture et garantie concernant les entités utilisatrices	61
9.3.	Confidentialité des données professionnelles	61
9.3.1.	Périmètre des informations confidentielles	61
9.3.2.	Informations hors du périmètre des informations confidentielles.....	62
9.3.3.	Responsabilités en terme de protection des informations confidentielles .	62
9.4.	Protection des données personnelles.....	62
9.4.1.	Politique de protection des données personnelles	62
9.4.2.	Informations à caractère personnel	62
9.4.3.	Informations à caractère non personnel	62
9.4.4.	Responsabilité en termes de protection des données personnelles	62
9.4.5.	Notification et consentement d'utilisation des données personnelles.....	62
9.4.6.	Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives	62
9.4.7.	Autres circonstances de divulgation d'informations personnelles	62

9.5.	Droits sur la propriété intellectuelle et industrielle	62
9.6.	Interprétations contractuelles et garanties	63
9.6.1.	Autorités de Certification	63
9.6.2.	Service d'enregistrement	63
9.6.3.	Porteurs de certificats	64
9.6.4.	Utilisateurs de certificats	64
9.6.5.	Autres participants	64
9.7.	Limite de garantie	64
9.8.	Limite de responsabilité	64
9.9.	Indemnités.....	65
9.10.	Durée et fin anticipée de validité de la PC.....	65
9.10.1.	Durée de validité	65
9.10.2.	Fin anticipée de validité.....	65
9.10.3.	Effets de la fin de validité et clauses restant applicables.....	65
9.11.	Notifications individuelles et communications entre les participants	65
9.12.	Amendements à la PC	65
9.12.1.	Procédures d'amendements	65
9.12.2.	Mécanisme et période d'information sur les amendements.....	65
9.12.3.	Circonstances selon lesquelles l'OID doit être changé.....	65
9.13.	Dispositions concernant la résolution de conflits	66
9.14.	Juridictions compétentes	66
9.15.	Conformité aux législations et réglementations	66
9.16.	Dispositions diverses	66
9.16.1.	Accord global	66
9.16.2.	Transfert d'activités	66
9.16.3.	Conséquences d'une clause non valide	66
9.16.4.	Application et renonciation	66
9.16.5.	Force majeure	66
9.17.	Autres dispositions.....	66
10.	ANNEXE 1 : DOCUMENTS CITES EN REFERENCE.....	67
10.1.	Réglementation	67
10.2.	Documents techniques	67
11.	ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC69	
11.1.	Exigences sur les objectifs de sécurité.....	69
11.2.	Exigences sur la certification	69
12.	ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF D'AUTHENTIFICATION	70
12.1.	Exigences sur les objectifs de sécurité.....	70
12.2.	Exigences sur la certification	70
13.	ANNEXE 4 : RESUME DES INFORMATIONS PARTICULIERES A LA PRESENTE PC ..	71

1. INTRODUCTION

1.1. Présentation générale

Ce document constitue la Politique de Certification (PC) de l'Autorité de Certification Journaux officiels *Publication (AC JO Publication)* de la *Direction des Journaux officiels* dans le cadre de l'émission de certificats électroniques **de signature** pour les *composants techniques de l'activité publication* des Journaux Officiels.

Ce document expose le niveau d'exigence que s'engage à respecter et maintenir l'*AC JO Publication*, lors de l'émission, de la gestion du cycle de vie et de la publication de ces certificats.

Il s'appuie sur les préconisations, émises par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) et l'Agence pour le Développement de l'Administration Electronique (ADAE), et présentées dans les PC Type de la Politique de Référencement Intersectorielle de Sécurité version 2 (PRIS v2).

Le niveau de sécurité couvert correspond au niveau 2 étoiles de la PRIS. Néanmoins, l'Infrastructure de gestion de clé (IGC) a été conçue pour couvrir à termes le niveau 3 étoiles.

1.2. Convention d'écriture

Pour repère, tout au long du document la convention d'écriture suivante a été respectée :

- Le texte en police normale et couleur noir reprend les principes énoncés dans les PC Type de la PRIS v2.
- **Le texte en police normale et couleur rouge est spécifique au contexte de la DJO et commun à l'ensemble des PC de la présente IGC**
- *Le texte en police italique et couleur rouge est commun aux PC d'une même AC*
- **Le texte en police gras et couleur rouge est particulier à la présente PC**
- Les paragraphes précédés de la mention **{2 étoiles}** indique qu'il s'agit de spécificités relatives au niveau 2 étoiles de la PRIS v2.

1.3. Identification du document

La présente PC est dénommée « *Politiques de Certification Direction des Journaux officiels – Autorité de Certification JO Publication – Certificats de signature* ».

Le numéro d'OID correspondant à la présente PC : **1.2.250.1.144.1.1.2.1**.

La branche OID est enregistrée auprès de l'AFNOR. Le sixième digit (égal à 1) indique qu'il s'agit d'une PC (la DPC est référencée sous le digit 2). L'avant dernier digit indique l'identifiant spécifique à l'Autorité de Certification concernée et à l'usage des certificats qu'elle émet. Le dernier digit indique la version de la PC.

1.4. Entités intervenant dans l'IGC

1.4.1. Autorités de certifications

La notion d'Autorité de Certification (AC) telle qu'utilisée dans la présente PC est définie au chapitre 1.7.1 ci-dessous.

L'AC en tant qu'autorité 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 : une infrastructure de gestion de clés (IGC).

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats (cf. ci-dessous).

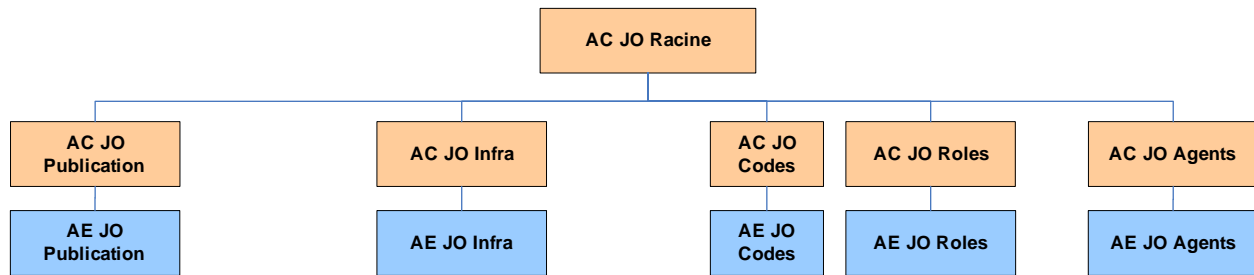
Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine (cf. [ETSI_NQCP]), la décomposition fonctionnelle de l'IGC **DJO** qui est retenue est la suivante :

- **Autorité d'enregistrement (AE)** - Cette fonction vérifie les informations d'identification du futur porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction de génération des certificats (cf. ci-dessous).
- **Fonction de génération des certificats** - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats :
 - Soit en s'appuyant sur les outils propres aux composants techniques ou aux futurs porteurs de certificat
 - Soit en s'appuyant sur les outils de l'IGC (en particulier l'AE)
- **Fonction de remise au porteur** - Cette fonction remet au porteur au minimum son certificat. Les éléments tels que le support de sécurité, le code d'activation (code PIN) et la chaîne de certification sont remis par l'AE.
- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques publiées par l'AC, les certificats d'AC, les conditions d'utilisation et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Lorsque nécessaire, les certificats valides des porteurs sont publiés dans un annuaire de publication de l'IGC.
- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (statut révoqué en particulier). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers qui se matérialise par une Liste de Certificats Révoqués (LCR).

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. Le porteur peut être également un composant technique (routeur, serveur, application) pour certaines AC au sens service que nous qualifierons plus bas.
- **Mandataire de certification (MC)** - Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des porteurs de cette entité (il assure notamment le face-à-face pour l'identification des porteurs lorsque celui-ci est requis). **Dans le cas de la DJO, le mandataire pourra être un agent du service du personnel.**
- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur d'authentification provenant du porteur du certificat.
- **Personne autorisée** - Il s'agit d'une personne autre que le porteur et le mandataire de certification 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, ...). **Dans le cas de la DJO, il peut s'agir d'un responsable de service des systèmes d'information ou d'un responsable hiérarchique du porteur.**

L'organisation fonctionnelle de l'IGC **DJO** est la suivante :



L'ensemble de fonctions assurées par les AC (en tant que service technique) est opéré par le service des systèmes d'information de la **DJO**.

La Déclaration des Pratiques de Certification (DPC) associées aux AC identifiées dans le présent document décrit l'organisation opérationnelle de l'IGC et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrites dans la présente PC (cf. chapitre 5.2.2).

Dans le cadre de leurs fonctions opérationnelles, qu'elles assument directement, les AC décrites ci-après devront assurer les responsabilités suivantes (commun à l'ensemble des PC de l'IGC DJO) :

- Etre une entité légale au sens de la loi française
- Etre en relation par voie contractuelle / hiérarchique / réglementaire l'entité (ou la personne physique) pour laquelle elle a en charge la gestion des certificats des porteurs de cette entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'applications d'échanges dématérialisés, aux porteurs, aux utilisateurs de certificats ... qui mettent en œuvre des certificats dans le cadre de la présente PC
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur
- *Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse. Dans le cadre de la présente PC on s'appuiera sur l'analyse de risque relative à l'application qualifiée comme étant la plus critique (lois et décrets par exemple)*
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité (la journalisation et l'archivage des événements sont des facteurs de qualité et de fiabilité).
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux porteurs et utilisateurs de certificats.

1.4.1.1. Autorité de certification JO Racine (AC JO Racine)

L'AC JO Racine est une composante de l'IGC qui dispose d'une plate-forme lui permettant d'émettre et de gérer deux types de certificats :

- Certificats des AC directement subordonnées de l'IGC **DJO** : AC JO Publication, AC JO Infra, AC JO Codes, AC JO Roles, AC JO Agents – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.1.1.**

- Certificats d'authentification des administrateurs de l'AC JO Racine – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.1.1**.

L'AC JO Racine est dans un premier temps auto-signée. Elle sera prochainement rattachée à l'IGC-A.

1.4.1.2. Autorité de certification JO Publication (AC JO Publication)

L'AC JO Publication est une composante de l'IGC qui dispose d'une plate-forme lui permettant d'émettre et de gérer les types de certificats suivants :

- Certificats de signature pour les publications des Journaux Officiels – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.2.1**.
- Certificats d'authentification pour les serveurs de diffusion – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.3.1**.
- Certificats d'authentification des administrateurs de l'AC JO Publication – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.6.1**.

L'AC Publication est signée par l'AC JO Racine.

1.4.1.3. Autorité de certification JO Infra (AC JO Infra)

L'AC JO Publication est une composante de l'IGC qui dispose d'une plate-forme lui permettant d'émettre et de gérer les types de certificats suivants :

- Certificats d'authentification des composants techniques gérés par la **DJO** (authentification SSL, IPSec ou Windows) – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.4.1**.
- Certificats d'authentification des administrateurs de l'AC JO Infra – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.4.1**.

L'AC Infra est signée par l'AC JO Racine.

1.4.1.4. Autorité de certification JO Codes (AC JO Codes)

L'AC JO Codes est une composante de l'IGC qui dispose d'une plate-forme lui permettant d'émettre et de gérer les types de certificats suivants :

- Certificats de signature de codes mobiles développés par (ou pour) la **DJO** – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.5.1**.
- Certificats d'authentification des administrateurs de l'AC JO Codes – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.6.1**.

L'AC Codes est signée par l'AC JO Racine.

1.4.1.5. Autorité de certification JO Rôles (AC JO Roles)

L'AC JO Roles est une composante de l'IGC qui dispose d'une plate-forme lui permettant d'émettre et de gérer les types de certificats suivants :

- Certificats d'authentification délivrés aux porteurs autorisés à représenter le rôle décrit dans l'objet du certificat
- Certificats d'authentification des administrateurs de l'AC JO Rôles

Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.6.1**.

L'AC Roles est signée par l'AC JO Racine.

1.4.1.6. Autorité de certification JO Agents (AC JO Agents)

L'AC JO Agents est une composante de l'IGC qui dispose d'une plate-forme lui permettant d'émettre et de gérer les types de certificats suivants :

- Certificats d'authentification délivrés aux personnes physiques de la **DJO** ayant été au préalable authentifiées par un MC – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.7.1.**
- Certificats de signature délivrés aux personnes physiques disposant d'un certificat d'authentification émis par l'AC JO Agents – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.8.1.**
- Certificats d'authentification des administrateurs de l'AC JO Codes – Ces certificats sont régis par la PC comportant l'OID **1.2.250.1.144.1.1.7.1.**

L'AC Agents est signée par l'AC JO Racine.

1.4.2. Autorité d'enregistrement

L'Autorité d'enregistrement (AE) doit permettre de vérifier l'identité du futur porteur de certificat. Pour cela, l'AE assure les tâches suivantes :

- Prise en compte et vérification des informations du futur porteur et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant : cette tâche sera déléguée aux AEL et réalisée par un MC (décrit plus bas)
- Etablissement et transmission de la demande de certificat à la fonction de « génération des certificats » de l'AC (cf. paragraphe 1.4.1)
- Archivage des pièces du dossier d'enregistrement (ou l'envoi à l'entité responsable de l'archivage des dossiers)
- Conservation et protection en confidentialité et en intégrité des données personnelles d'authentification du porteur (documents d'identification) ou, le cas échéant, du MC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

L'AE de l'AC JO **Publication** est hébergée et opérée par la **DJO**.

Pour assurer ces tâches, l'AE s'appuie sur une (ou plusieurs) AE locale(s) (AEL) qui assure(nt) les opérations précédemment décrites appliquée à l'émission de certificats **de signature** pour des entités de type **composants techniques de l'activité publication**.

L'AEL est accessible par des personnes autorisées (MC) qui ont été préalablement enregistrées et certifiées.

Cette autorité n'est pas mise en place pour l'AC JO Racine. La signature des autorités subordonnées sera directement sous la responsabilité de l'AC JO Racine, en tant qu'autorité.

1.4.3. Porteurs de certificats

Dans le cadre de la présente PC, un porteur de certificat est un composant technique d'une application spécifique à l'activité publication et d'horodatage de la DJO (application Lois et décrets par exemple). Le certificat est propre au composant technique.

Les opérations d'enregistrement, de renouvellement, de demande de révocation et d'utilisation engage la responsabilité de l'entité (personne, service de la DJO par exemple) qui à la charge de la gestion du certificat et qui veille à ce qu'il soit utilisé dans le respect de la politique de sécurité de l'application concernée.

Le certificat est utilisé par l'application ou des composants de l'application dans le cadre des activités DJO.

Le porteur (ou entité responsable) respecte les conditions qui lui incombent définies dans la présente PC.

1.4.4. Utilisateurs de certificats

La présente PC traitant de certificats **de signature** (cf. chapitre 1.5), un utilisateur de certificats peut être :

- *Un service de la DJO faisant partie du système de publication des documents officiels de la DJO ou utilisateur du système. Ce service est accessible par voie électronique (application, serveur Internet, base de données, etc.), sous la responsabilité d'une personne physique ou morale. Il utilise un certificat et un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message du porteur de certificat (application ou service technique de publication DJO). L'application met en œuvre la politique et les pratiques de sécurité édictées par le responsable d'application.*
- *Un usager accédant à une publication de la DJO, qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur de certificat (l'application) sur le document publié par un service de la DJO*
- *Un abonné accédant au service d'horodatage qui utilise un certificat et un dispositif de demande de jetons d'horodatage.*

Le service de signature permet ainsi de garantir l'intégrité des documents et données signées par le porteur de certificat.

1.5. Usage des certificats

1.5.1. Domaines d'utilisation applicables

1.5.1.1. Bi-clés et certificats des porteurs

La présente PC traite des bi-clés et des certificats à destination des catégories de porteurs identifiés au chapitre 1.4.3, afin que ces porteurs puissent :

- **Signer électroniquement des données (documents ou messages) avec des outils fournis par les Journaux officiels ; la signature est vérifiée par un service des Journaux officiels accessible par voie électronique ou par un service tiers conforme au cadre de signature de la DJO.**
- **Signer électroniquement des données avec des outils fournis par les Journaux officiels ; la signature est vérifiée par un agent ou un usager qui utilise les outils des Journaux officiels ou un outil tier conforme au cadre de signature DJO.**

Les applications principalement concernées sont :

- **La signature des éditions publiées par la DJO (textes Lois et décrets par exemple).**
- **La signature de jetons d'horodatage générés par le système d'horodatage de la DJO.**
- **La signature de messages dans le cadre des échanges entre applications ou services du système de publication DJO**

D'autres usages peuvent être autorisés par l'AC (en tant qu'autorité) dans sa PC, notamment dans des relations autres qu'avec l'Administration, mais sous la responsabilité de l'AC et à conditions que ces autres usages ne remettent pas en cause la conformité aux exigences de la présente PC. Notamment, l'utilisation de la clé privée du porteur et du certificat associé doit rester strictement limitée au **service de signature**.

L'utilisateur du certificat a ainsi l'assurance que le porteur identifié dans le certificat (nom de l'application), représenté par l'entité responsable de l'application, a manifesté son consentement quant au contenu des données signées électroniquement à l'aide de la clé privée correspondante. Le niveau d'assurance correspond au niveau 2 étoiles de la PRIS v2.

{2 étoiles} Les certificats de signature objets de la présente PC sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité pour pouvoir signer indûment des données sont forts (intérêt pour les usurpateurs, effets de la signature, etc.).

Enfin, certaines applications d'échanges dématérialisés peuvent nécessiter des certificats à des fins de validation ou de recette. De tels certificats doivent être identiques aux certificats « de production » fournis et gérés par l'AC. Pour cela, une AC (au sens service) spécifique « de test » doit être mise en place et doit être identique à l'AC « de production ».

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

L'*AC JO Publication* génère et signe différents types d'objets : certificats, *LCR*. Pour signer ces objets, l'AC dispose d'une bi-clé unique. La bi-clé et le certificat de l'AC ne doit être utilisée qu'à ces fins. Ils ne doivent notamment être utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

Conformément au [CWA14167-1], les différentes clés internes à l'IGC sont décomposées suivant les catégories suivantes :

- La (ou les) clé(s) de signature d'AC, utilisée(s) pour signer les certificats générés par l'AC ainsi que les informations sur l'état des certificats (*LCR*)
- Les clés d'infrastructure, utilisées par les systèmes intervenant dans l'IGC à des fins d'authentification, de signature des journaux d'événements, de chiffrement des données échangées ou stockées au sein de l'IGC, etc.
- Les clés de contrôle, assignées au personnel de l'IGC afin de s'authentifier vis-à-vis des différents systèmes, de signer et/ou de chiffrer des messages ou des données échangés, etc.

L'ensemble des clés décrites sont des clés asymétriques.

Les engagements relatifs à ces différents types de clés sont décrits dans la présente PC.

1.5.2. Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 1.5 ci-dessus, selon le niveau **2 étoiles** de la PRISv2 retenu pour la présente PC.

1.6. Gestion de la PC

1.6.1. Entité gérant la PC

L'AC en tant qu'autorité est responsable de la validation et de la gestion de la PC.

1.6.2. Point de contact

Toute demande d'informations concernant ce document devra être transmise à :

Direction des Journaux officiels
Service des systèmes d'information
26, rue Desaix
75015 Paris

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

L'**Autorité Qualifiée en Sécurité des Systèmes d'Information (AQSSI)** nomme les personnes (ou entité) à déterminer la conformité de la DPC avec cette PC.

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

L'approbation de la conformité de la DPC passe par :

- Une présentation des analyses par les personnes (ou entité) désignées pour déterminer la conformité de la DPC
- Une validation des analyses par l'**Autorité Qualifiée en Sécurité des Systèmes d'Information (AQSSI)**
- L'émission d'un certificat de conformité de la DPC par l'**AQSSI**.

1.7. Définitions et acronymes

Les acronymes dans la présente PC sont les suivants :

Sigle	Signification
AC	Autorité de Certification
ADAE	Agence pour le Développement de l'Administration Electronique
AE	Autorité d'Enregistrement
AEL	Autorité d'Enregistrement Locale
AQSSI	Autorité Qualifiée en Sécurité des Systèmes d'Information
AS	Autorité de Sécurité de l'IGC
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DJO	Direction des Journaux officiels
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion de Clés
ISO 9594-8	Norme décrivant, entre autres, le format X509 v3 qui constitue le format normalisé des certificats
JO	Journaux Officiels
JOEA	Journal Officiel Electronique Authentifié
L&D	Lois et décrets

Sigle	Signification
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique
RSA	Rivest Shamir Adelman
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	Codage des caractères définis par Unicode où chaque caractère est codé sur une suite de un à six mots de 8 bits (il n'existe pas actuellement de caractères codés avec plus de 4 mots)
X.509	Format des certificats d'identité recommandé par l'Union Internationale des Télécommunications (UIT).

1.7.1. Termes communs à la PRIS

Terme	Signification
Applications utilisatrices	Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat.
Autorités administratives	Ce terme générique désigne les administrations de l'Etat, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.
Autorité d'horodatage	Autorité responsable de la gestion d'un service d'horodatage (cf. politique d'horodatage type de la PRIS).
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, etc.

Terme	Signification
Produit de sécurité	Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en oeuvre 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.
Promoteur d'application	Un responsable d'un service de la sphère publique accessible par voie électronique.
Qualification des produits de sécurité	Acte par lequel la DCSSI atteste du niveau de sécurité d'un produit de sécurité en s'appuyant sur le schéma français d'évaluation et de certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, schéma défini par le décret [CERTIF].

1.7.2. Termes spécifiques ou complétés / adaptés pour la présente PC

Terme	Signification
Autorité de certification (AC)	Autorité chargée de l'application de la politique de certification. Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat.
Autorité d'enregistrement.	Cf. chapitre 1.4.2.
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 personne physique et portant sur une bi-clé de signature , sauf mention explicite contraire (certificat d'AC, certificat d'une composante, ...).
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 oeuvre opérationnelle d'au moins une fonction de l'IGC.
Déclaration des pratiques de certification (DPC)	Une 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.

Terme	Signification
Dispositif de création de signature	Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour stocker et mettre en oeuvre sa clé privée de signature.
Dispositif de sécurité de création de signature	Dispositif de création de signature répondant aux exigences de l'article 3 du décret [SIG].
Entité	Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.
Fonction de génération des certificats	Cf. chapitre 1.4.1
Fonction de gestion des révocations	Cf. chapitre 1.4.1
Fonction de publication	Cf. chapitre 1.4.1
Fonction de remise au porteur	Cf. chapitre 1.4.1
Fonction d'information sur l'état des certificats	Cf. chapitre 1.4.1
Mandataire de certification	Cf. chapitre 1.4.1
Personne autorisée	Cf. chapitre 1.4.1
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.
Politique de signature	Ensemble de règles pour la création et la validation d'une signature électronique vis-à-vis desquelles la signature peut être déterminée comme valide
Porteur	Cf. chapitre 1.4.1
Usager	Personne physique agissant pour son propre compte ou pour le compte d'une personne morale dans ses relations avec une administration.
Utilisateur de certificat	Cf. chapitre 1.4.1

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

2.1. Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des porteurs et des utilisateurs de certificats, l'AC (en tant qu'autorité) doit mettre en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats (cf. chapitre 1.4.1).

La présente PC précise les méthodes de mise à disposition et les URL correspondantes (annuaire accessible en protocole LDAP, serveur Web de publication).

2.2. Informations devant être publiées

L'AC, en tant qu'autorité, doit publier au minimum les informations suivantes à destination des porteurs et des utilisateurs de certificats :

- Sa politique de certification, couvrant l'ensemble des rubriques du [RFC3647] et conforme à la présente PRISv2
- La liste des certificats révoqués (porteurs et AC)
- Les certificats de l'AC, en cours de validité

Les certificats en cours de validité des AC de la hiérarchie dont dépend la présente AC, les différentes politiques de certification correspondantes et les éventuels documents complémentaires, ceci jusqu'à l'AC Racine

L'AC, en tant que service technique, publie, à destination des porteurs de certificats et le cas échéant, les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.). Elle s'appuie sur l'AE pour assurer cette publication.

De plus, l'AC (hors AC Racine), en tant que service technique, publie également des conditions générales d'utilisation correspondant aux « PKI Disclosure Statement » (PDS) définis par [ETSI_NQCP] et [RFC3647]. La structure des conditions générales est conforme à celle décrite en annexe B de [ETSI_NQCP]. Elle reprennent ainsi, à destination des porteurs et des utilisateurs de certificats, les informations pertinentes de la PC de l'AC (conditions d'usages des certificats, obligations et responsabilités des différentes parties, garanties et limites de garanties de l'AC, etc.).

2.3. Délais et fréquences de publication

Les délais et les fréquences de publication dépendent des informations concernées :

- Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), l'information doit être publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.
- Pour les certificats d'AC, ils doivent être diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants sous délai de **24h**
- Pour les informations d'état des certificats, cf. chapitre 4.9.

Les exigences de disponibilité des systèmes publiant ces informations dépendent des informations concernées :

- Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), les systèmes doivent avoir une disponibilité pendant les **Jours ouvrés** avec une durée maximale d'indisponibilité

par interruption de service (panne ou maintenance) de **8h (jours ouvrées)** et une durée totale maximale d'indisponibilité par mois de **32h (jours ouvrés)**, ceci hors cas de force majeure.

- Pour les certificats d'AC, les systèmes doivent avoir une disponibilité de **24h/24 7j/7** avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de **2h** et une durée totale maximale d'indisponibilité par mois de **8h**, ceci hors cas de force majeure.

Pour les informations d'état des certificats, cf. chapitre IV.10.

A noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une non disponibilité de cette information et que les exigences ci-dessus s'appliquent également à la disponibilité des informations publiées sur ces systèmes.

2.4. Contrôle d'accès aux informations publiées

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

{2 étoiles} L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un **contrôle d'accès fort** (basé sur une authentification au moins à deux facteurs).

L'accès en modification aux systèmes de publication des autres informations doit être strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un **contrôle d'accès de type mots de passe** basé sur une politique de gestion stricte des mots de passe.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. Nommage

3.1.1. Types de noms

Les noms utilisés doivent être conformes aux spécifications de la norme X.500.

Dans chaque certificat X509v3 l'AC émettrice (issuer) et le porteur (subject) sont identifiés par un « Distinguished Name » DN de type X.501 dont le format exact est précisé dans le chapitre 7 décrivant le profil des certificats.

3.1.2. Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats doivent être explicites. Le DN respecte la structure de noms utilisés dans l'annuaire de la **DJO**.

Lorsqu'un pseudonyme est utilisé, il doit être explicitement identifié comme tel dans le DN. L'attribut retenu pour contenir le pseudonyme est « pseudonym ». Dans ce cas les attributs givenName / surname ou commonName ne doivent pas être utilisés.

Dans le cas contraire, le DN du porteur est construit à partir du nom de l'entité responsable (DJO, Service Lois et décrets, ...) de l'application ou du composant logiciel qui sera signé avec le certificat émis. L'AE devra contrôler auprès des responsables de l'application que les informations du DN sont corrects et suffisamment explicites pour désigner l'identité du signataire.

3.1.3. Règles d'interprétation des différentes formes de nom

Aucune exigence n'est stipulée en plus des règles spécifiées ci-dessus.

3.1.4. Unicité de Noms

Afin d'assurer une continuité d'une identification unique du porteur au sein du domaine de l'AC dans ses certificats successifs (renouvellement) et pour éviter toute ambiguïté, le DN du champ « subject » de chaque certificat de porteur doit permettre d'identifier de façon unique le porteur **(ou de l'entité responsable)** correspondant au sein du domaine de l'AC.

Ce DN doit pour cela respecter les exigences suivantes :

- **commonName = Nom du porteur (entité responsable de l'application concernée)**
- **organizationalUnit = Journaux officiels**
- **organization = Gouv**
- **country = FR**

Le format du commonName est explicité ci-dessus.

Le DN sera fourni par le responsable de l'application nécessitant un certificat de signature. Un contrôle sera effectué sur la validité des informations fournies.

3.1.5. Identification, authentification et rôle de marques déposées

Sans objet.

3.2. Validation initiale de l'identité

L'enregistrement d'un porteur peut se faire soit directement auprès de l'AE, soit via un mandataire de certification de l'entité. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

La validation initiale de l'identité d'une entité ou d'une personne physique est ainsi réalisée dans les cas suivants :

- Enregistrement d'un porteur sans MC : validation par l'AE de l'identité « personne morale » de l'entité de rattachement et de l'identité « personne physique » du futur porteur ; ce cas est relativement rare car l'enregistrement des porteurs sera principalement assuré par les MC.
- Enregistrement d'un MC : validation par l'AE de l'identité « personne morale » de l'entité pour lequel le MC interviendra et de l'identité « personne physique » du futur MC.
- Enregistrement d'un porteur via un MC : validation par le MC de l'identité « personne physique » du futur porteur.

Le chapitre 3.2.3 fournit une description détaillée des conditions de validation de l'identité pour chaque cas.

3.2.1. Méthode pour prouver la possession de la clé privée

Lorsque c'est le porteur (**ou le responsable du composant**) qui génère sa bi-clé, il doit alors fournir à l'AC, via le MC le cas échéant, une preuve de possession de sa clé privée correspondant à la clé publique contenue dans la demande de certificat.

Cette preuve est fournie par l'intermédiaire des fonctions de l'AE ou des fonctions de l'outil de génération tiers qui ont permis de délivrer une demande de certificat (requête PKCS#10).

3.2.2. Validation de l'identité de l'organisme

Cf. chapitre 3.2.3

3.2.3. Validation de l'identité d'un individu

3.2.3.1. Enregistrement d'un porteur sans MC

L'identification du futur porteur (**composant technique**) représentant une entité (*la DJO pour les composants logiciels internes*) nécessite, d'une part l'identification de cette entité et, d'autre part l'identification de la personne physique responsable **du composant technique**.

L'enregistrement doit au moins respecter les règles suivantes :

- **La demande de certificat est émise par l'entité (personne physique ou service) responsable de l'application qui demande le certificat de signature**
- **La procédure d'enregistrement est réalisée dans le cadre d'un face-à-face physique avec l'AE et implique les différents acteurs qui partageront le secret d'accès aux clés**
- *L'AE effectue l'enregistrement du certificat dont la demande se présente sous la forme d'un CSR (Certificate Signing Request), au format PKCS#10. L'entité demandeuse s'engage à respecter le cadre de nommage défini dans le cadre de la présente PC*
- **La demande de certificat de signature est validée par l'AE (en tant qu'autorité)**

- **En fin d'enregistrement, les cartes d'accès aux clés, qui sont stockées dans un boîtier cryptographique, sont remises aux différents porteurs**

Le porteur doit être informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation.

3.2.3.2. Enregistrement d'un MC

Ce cas ne concerne pas la présente PC. La délivrance de certificats d'authentification pour les AE et les MC est décrite dans le cadre de la PC AC Roles (OID : 1.2.250.1.144.1.1.6.1)

3.2.3.3. Enregistrement d'un porteur via un MC

L'enregistrement respecte les mêmes règles que l'enregistrement sans MC (paragraphe 3.2.3.1), à la différence que l'AE (en tant qu'autorité) est remplacée par le MC.

Le porteur doit être informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation.

3.2.4. Informations non vérifiées du porteur

Sans objet

3.2.5. Validation de l'autorité du demandeur (entité de rattachement)

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

3.2.6. Critères d'interopérabilité

L'AC gère et documente les demandes d'accords et les accords de reconnaissance avec des AC extérieures au domaine de sécurité auquel l'AC appartient.

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

Le renouvellement de la bi-clé d'un porteur entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la bi-clé correspondante (cf. chapitre 4.6).

3.3.1. Identification et validation pour un renouvellement courant

{2 étoiles} La procédure d'identification et d'authentification du porteur est la même que pour l'enregistrement initial (cf. § 3.2.3.1).

3.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation définitive d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement doit être identique à la procédure d'enregistrement initial ou doit être une procédure offrant un niveau de garantie équivalent.

3.4. Identification et validation d'une demande de révocation

Les demandes de révocation peuvent être faites par téléphone, par courrier, par télécopie ou en face-à-face.

Dans le cas d'une demande en ligne ou par téléphone, le demandeur est formellement authentifié par un jeu de questions / réponses sur des informations propres au demandeur, dont une au moins ne peut réellement être connue que du demandeur

Dans le cas d'une demande par courrier ou par télécopie, la demande doit être signée par le demandeur et l'AE (ou le MC) doit vérifier l'identité du demandeur (vérification de la signature manuscrite par rapport à la signature préalablement signée).

Toute demande de révocation doit être validée par l'AE ou le MC. La validation entraîne la révocation du certificat, l'émission et la publication d'une nouvelle LCR.

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

Un certificat peut être demandé par un représentant légal de l'entité ou un MC dûment mandaté pour cette entité (cf. § 1.4.1), avec dans tous les cas consentement préalable du futur porteur.

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

Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. chapitre 3.2) :

- **Le nom de l'application ou du service pour lesquels est délivré le certificat (nom réel ou pseudonyme)**
- **L'adresse courriel du porteur (responsable de l'application ou du demandeur) ou une adresse institutionnelle**

Les informations et les documents d'enregistrements sont remis par l'entité responsable de l'application à l'AE ou au MC.

4.2. Traitement de la demande

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

Les identités "*personne morale*" sont vérifiées conformément aux exigences du chapitre 3.2.

L'AE, ou le MC le cas échéant, doit effectuer les opérations suivantes :

- Valider l'identité du futur porteur (ou demandeur dans le cas de composants techniques)
- Vérifier la cohérence des justificatifs présentés
- S'assurer que le futur porteur (ou demandeur dans le cas de composants techniques) a pris connaissance des modalités applicables pour l'utilisation du certificat

Dans le cas d'une demande via un MC, celui-ci retransmet, si nécessaire, le dossier à l'AE après avoir effectué les opérations ci-dessus. L'AE doit alors s'assurer que la demande correspond bien au mandat du MC.

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat et, le cas échéant, de la bi-clé vers la fonction adéquate de l'IGC (cf. chapitre 1.4.1).

L'AE conserve ensuite une trace des justificatifs d'identité présentés, sous format électronique ou papier.

4.2.2. Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le porteur, le MC ou le demandeur le cas échéant, en justifiant le rejet.

4.2.3. Durée d'établissement du certificat

La durée d'établissement sera la plus courte possible : de 0 à 7 jours ouvrés (0 signifiant un établissement immédiat).

4.3. Délivrance du certificat

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

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC, en qualité de service technique, déclenche les processus de génération et de préparation des différents éléments destinés au porteur : au minimum, le certificat. La bi-clé associée au certificat, le dispositif d'authentification et les codes d'activation sont fournis / générés lors de la demande de certificat.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 5 et 6 ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre 5.2).

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

{2 étoiles} La remise du certificat est effectuée lors de la phase d'enregistrement, en face-à-face avec l'AE. Le certificat est stocké dans un boîtier cryptographique et protégé par des cartes d'accès selon la méthode Shamir.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'acceptation du certificat est considérée comme tacite et correspond à la récupération du certificat et son intégration dans le support de sécurité (ou le magasin de certificat logiciel sécurisé). Cette opération est réalisée lors du processus d'enregistrement en face-à-face avec l'AE (ou le MC).

Les obligations du porteur et le délai correspondant sont clairement mentionnés dans la présente PC ainsi que dans les conditions générales d'utilisation (cf. chapitre 2.2).

4.4.2. Publication du certificat

Le certificat est publié dans l'annuaire de l'IGC. Il n'est publié qu'à des fins de contrôle de l'identité de l'utilisateur et ne sera accessible que par les applications et utilisateurs autorisés par la DJO.

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

L'AC, en qualité de service technique, informe l'AE de la délivrance du certificat, qui se charge d'en informer le MC le cas échéant.

4.5. Usages de la bi-clé et du certificat

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

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service **de signature** (cf. chapitre 1.5.1.1). Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé du porteur et du certificat associé doit par ailleurs être indiqué dans le certificat lui-même, via les extensions concernant les usages des clés (cf. chapitre 7).

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

Cf. chapitre précédent et chapitre 1.5.

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

La présente PC impose que les certificats et les bi-clés correspondantes aient la même durée de vie, il ne peut donc pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé.

4.6.1. Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2. Origine d'une demande de renouvellement

Sans objet.

4.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4. Notification au porteur de l'établissement du nouveau certificat

Sans objet.

4.6.5. Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6. Publication du nouveau certificat

Sans objet.

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

Sans objet.

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

4.7.1. Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des porteurs, et les certificats correspondants, seront renouvelés tous les **deux ans**.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du porteur (cf. chapitre 4.9, notamment le chapitre 4.9.1.1 pour les différentes causes possibles de révocation).

Nota - 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 porteur.

4.7.2. Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat du porteur peut-être automatique ou bien à l'initiative du porteur (c'est-à-dire le responsable du composant logiciel).

L'entité, via son MC le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un porteur qui lui est rattaché.

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

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 3.3 ci-dessus.

Pour les actions de l'AC, cf. chapitre 4.3.1.

4.7.4. Notification au porteur de l'établissement du nouveau certificat

Cf. chapitre 4.3.2.

4.7.5. Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1.

4.7.6. Publication du nouveau certificat

Cf. chapitre 4.4.2.

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

Cf. chapitre 4.4.3.

4.8. Modification du certificat

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

4.8.1. Causes possibles de modification d'un certificat

Sans objet.

4.8.2. Origine d'une demande de modification d'un certificat

Sans objet.

4.8.3. Procédure de traitement d'une demande de modification d'un certificat

Sans objet.

4.8.4. Notification au porteur de l'établissement du certificat modifié

Sans objet.

4.8.5. Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6. Publication du certificat modifié

Sans objet.

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

Sans objet.

4.9. Révocation et suspension des certificats

4.9.1. Causes possibles d'une révocation

4.9.1.1. 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 le changement d'entité du porteur d'un certificat), ceci avant l'expiration normale du certificat.
- Le porteur n'a pas respecté les modalités applicables d'utilisation du certificat.
- Le porteur et/ou, le cas échéant, le MC / l'entité n'ont pas respecté leurs 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,
- Le porteur ou une entité autorisée (représentant légal de l'entité ou MC par exemple) 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 (pour un certificat).

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 doit être révoqué.

4.9.1.2. Certificats d'une composante de l'IGC

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

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante.

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

4.9.2. Origine d'une demande de révocation

4.9.2.1. Certificats de porteurs

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

- Le porteur (ou le responsable du certificat du porteur) au nom duquel le certificat a été émis
- Le MC
- Un représentant légal ou hiérarchique de l'entité
- L'AC émettrice du certificat ou l'une de ses composantes (AE)

Nota : Le porteur doit être informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat.

4.9.2.2. 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 (la **DJO**), 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 de porteur

Les exigences d'identification et de validation d'une demande de révocation, effectuée hors ligne ou en ligne par la fonction de gestion des révocations, sont décrites au chapitre 3.4.

Les informations suivantes doivent au moins figurer dans la demande de révocation de certificat :

- L'identité du porteur du certificat utilisée dans le certificat (tout ou partie du DN du certificat)
- Le nom du demandeur de la révocation
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série,...)
- Eventuellement, la cause de révocation

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation doit être diffusée au minimum via une LCR. D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'AC (cf. chapitre 4.9.9).

Le demandeur de la révocation doit être informé du bon déroulement de l'opération et de la révocation effective du certificat (soit par une notification en ligne qui se traduit par l'émission d'une nouvelle LCR, soit par une notification par courrier ou par courriel). De plus, si le porteur du certificat n'est pas le demandeur, il doit également être informé de la révocation effective de son certificat.

L'entité (porteur, représentant légal ou hiérarchique), directement ou via son MC le cas échéant (au choix de l'entité), doit être informée de la révocation de tout certificat des porteurs qui lui sont rattachés.

L'opération est enregistrée dans les journaux d'évènements.

Les causes de révocation définitive des certificats ne sont pas publiées. La valeur « unspecified » sera associée à chaque certificat révoqué.

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

La DPC précisera les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC **DJO**.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs certificats ne sont plus valides. Pour cela, la **DJO** pourra par exemple envoyer des récépissés aux AE et aux MC. Ces derniers devront informer les porteurs de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Une notification sera stipulée sur le site de publication de l'IGC.

Afin de faciliter la révocation du certificat de l'AC, il est recommandé que le certificat associé à la clé de l'AC signant les certificats porteurs soit signé par une autre AC et ne soit pas uniquement autosigné (cf. chapitre 1.5.1.2).

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

4.9.4. Délai accordé au porteur pour formuler la demande de révocation

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

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

4.9.5.1. Révocation d'un certificat de porteur

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

La fonction de gestion des révocations doit être disponible **4h**.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de **1h** et une durée maximale totale d'indisponibilité par mois de **4h**.

Toute demande de révocation d'un certificat porteur doit être traitée dans un délai inférieur à **24h**, 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.

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

La révocation d'un certificat d'une composante de l'IGC doit être 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.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR et/ou de réponses OCSP) doit être 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

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

La DJO ne met pas, au moins dans un premier temps, de service OCSP.

4.9.7. Fréquence d'établissement des LCR

La fréquence de publication des LCR est de 24h.

Le besoin de deltaLCR n'a pas été identifié à ce jour.

4.9.8. Délai maximum de publication d'une LCR

Une LCR doit être publiée dans un délai maximum de 30min suivant sa génération.

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

Sans objet

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

Cf. chapitre 4.9.6 ci-dessus.

4.9.11. Autres moyens disponibles d'information sur les révocations

Sans objet

4.9.12. Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de porteur, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, outre les exigences du chapitre 4.9.3.2 ci-dessus, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

4.9.13. Causes possibles d'une suspension

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

4.9.14. Origine d'une demande de suspension

Sans objet.

4.9.15. Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16. Limites de la période de suspension d'un certificat

Sans objet.

4.10. Fonction d'information sur l'état des certificats

4.10.1. Caractéristiques opérationnelles

L'AC, en tant que service, doit fournir aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification.

La fonction d'information sur l'état des certificats doit au moins mettre à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR / LAR. Ces LCR / LAR doivent être des LCR au format V2, publiées au moins dans un annuaire accessible en protocole LDAP V3.

4.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats doit être disponible **24h/24 7j/7**.

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de **2h** et une durée maximale totale d'indisponibilité de **8h**.

4.10.3. Dispositifs optionnels

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

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

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

4.12. Séquestre de clé et recouvrement

Ce document traite des aspects de signature et interdit donc le séquestre des clés privées des porteurs.

Les clés privées d'AC ne doivent pas non plus être séquestrées.

4.12.1. Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

4.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

5. MESURES DE SECURITE NON TECHNIQUES

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter.

La DPC décrit les moyens mis en œuvre pour respecter ces exigences.

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

L'IGC est située dans une des implantations de la DJO.

5.1.2. Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès aux locaux des différentes composantes de l'IGC doivent être contrôlés.

{2 étoiles} Concernant les fonctions de génération des certificats, de génération des éléments secrets du porteur et de gestion des révocations :

- L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique
- L'accès aux machines (serveurs, boîtiers cryptographiques, poste d'administration de l'AC, éléments actifs du réseau) soit limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines (contrôle d'accès par badge, droits associés)

5.1.3. Alimentation électrique et climatisation

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.

Elles permettent également de respecter les exigences de la présente PC, ainsi que les engagements de l'AC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4. Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences de la présente PC, ainsi que les engagements pris par l'AC, en tant qu'autorité, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5. Prévention et protection incendie

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

5.1.6. Conservation des supports

Les supports (papier, disque dur, disquette, CD, etc.) correspondant aux informations relatives à l'activité de l'IGC (fonctions d'exploitation, de sauvegarde, etc.) sont traités et conservés dans une enceinte sécurisée accessibles aux seules personnes autorisées.

Parmi les supports, on distinguera :

- Les cartes contenant une partie du secret d'accès aux clés d'AC qui doivent être conservées dans un coffre personnel à chaque détenteur d'une carte
- Les cartes d'activation des clés du boîtier cryptographique qui sont dupliquées et qui doivent être stockées dans le coffre de l'IGC situé dans la salle machine (de la même manière un coffre placé sur le site de secours contiendra une copie des cartes d'activation)
- Les archives qui doivent être conservées dans le coffre de l'IGC sur le site de production. Une copie de secours est stockée de manière sécurisée sur le site de secours.

5.1.7. Mise hors service des supports

Les supports papier et magnétiques en fin de vie sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité. Les dossiers d'enregistrement devront être conservés au moins pendant la durée de validité du certificat du porteur (en cas de renouvellement, la durée sera prolongée). Les supports magnétiques devront être conservés au moins cinq ans.

Les supports de stockage (disque dur de serveurs) de l'IGC ne sont pas réutilisés à d'autres fins avant destruction complète des informations liées à l'IGC qu'ils sont susceptibles de contenir.

5.1.8. Sauvegardes hors site

{2 étoiles} Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, au moins, mettent en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.).

Les informations sauvegardées hors site doivent respecter 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

Six rôles fonctionnels de confiance sont définis au sein de l'IGC **DJO** :

- **Responsable de sécurité physique** - Il est chargé des contrôles d'accès physiques aux équipements des systèmes de la composante.
- **Responsable de sécurité de l'IGC** - Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il fournit au Responsable de sécurité physique les règles d'accès aux équipements des systèmes de la composante. Il est habilité, par le Responsable de sécurité physique des locaux, à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- **Responsable d'application** - Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

- **Ingénieur système / base de données / réseaux** - Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante qui les concerne. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur** - Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur** - Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière 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.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, on distinguera également les rôles de porteur de parts de secrets d'IGC : cf. chapitres 6.1 et 6.2.

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.

Pour des raisons de sécurité, les fonctions sensibles seront réparties sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC (cf. chapitre 6).

La DPC de l'AC précise quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.).

Dans le cadre de la présente AC, certains rôles seront assurés par les mêmes personnes. La répartition est définie dans le cadre de la DPC.

5.2.3. Identification et authentification pour chaque rôle

Le Responsable de sécurité de l'IGC opérant une composante de l'IGC doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle
- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- Le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes
- Eventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans l'IGC.

Ces contrôles sont décrits dans la DPC de l'AC et sont conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC doit être notifiée par écrit.

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 fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC de l'AC et être conformes à la politique de sécurité de la composante concernée.

{2 étoiles} Concernant les rôles de confiance, les cumuls suivants sont interdits :

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

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 doivent être soumis à une clause de confidentialité vis-à-vis de leur employeur.

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

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

L'AC informe toute personne intervenant dans des rôles de confiance de l'IGC :

- De ses responsabilités relatives aux services de l'IGC
- Des procédures liées à la sécurité du système et au contrôle du personnel

5.3.2. Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC doit mettre 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 ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications doivent être menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (la fréquence recommandée est tous les 3 ans). Le MC (service du personnel en particulier) sera en charge de la conservation des dossiers.

5.3.3. Exigences en matière de formation initiale

Le personnel doit être préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

5.3.4. Exigences et fréquence en matière de formation continue

Le personnel concerné doit recevoir une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Chaque personnel concerné devra assister, au minimum, à une formation de mise à jour suivant chaque modification importante du système.

5.3.6. Sanctions en cas d'actions non autorisées

La **DJO** décide des sanctions à appliquer lorsqu'un exploitant abuse de ses droits ou effectue une opération non conforme à ses attributions.

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 doit également respecter les exigences du présent chapitre 5.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8. Documentation fournie au personnel

Chaque personnel doit disposer au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille.

La documentation adéquate concerne :

- Les PC
- La DPC
- Les procédures internes
- Les documents techniques relatifs aux matériels et logiciels utilisés.

5.4. Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1. Type d'évènements à enregistrer

L'IGC doit permettre, au minimum, de journaliser les évènements suivants, automatiquement dès le démarrage d'un système et sous forme électronique, concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'IGC :

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.)
- Démarrage et arrêt des systèmes informatiques et des applications
- Evènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes

D'autres événements doivent pouvoir aussi être recueillis par le Responsable de sécurité de l'IGC, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- Les accès physiques
- Les actions de maintenance et de changements de la configuration des systèmes
- Les changements apportés au personnel
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...)

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des événements spécifiques aux différentes fonctions de l'IGC doivent également être journalisés, notamment :

- Réception d'une demande de certificat (initiale et renouvellement)
- Validation / rejet d'une demande de certificat
- Evénements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...)
- Génération des certificats des porteurs
- Transmission des certificats aux porteurs et, selon les cas, acceptations / rejets explicites par les porteurs
- Publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.)
- Réception d'une demande de révocation
- Validation / rejet d'une demande de révocation
- Génération puis publication des LCR

Chaque enregistrement d'un événement dans un journal doit contenir au minimum les champs suivants :

- Type de l'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)

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants :

- 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 doivent être effectuées au cours du processus.

En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'évènement.

5.4.2. Fréquence de traitement des journaux d'évènements

Cf. chapitre 5.4.8 ci-dessous.

5.4.3. Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés sur site pendant au moins le délai **1 mois**. Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous le délai **1 mois** (recouvrement possible entre la période de conservation sur site et la période d'archivage).

5.4.4. Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

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

Le système de datation des évènements doit respecter les exigences du chapitre 6.8.

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.5. Procédure de sauvegarde des journaux d'évènements

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

5.4.6. Système de collecte des journaux d'évènements

L'IGC s'appuiera sur les systèmes de collecte internes à chacune de ses composantes.

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

Sans objet.

5.4.8. Evaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC doit être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont contrôlés suivant la fréquence **1 fois par 24h**, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins à une fréquence **1 fois par semaine et dès la détection d'une anomalie**. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) est effectué à une fréquence au moins égale à **1 fois par mois**, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

5.5. Archivage des données

5.5.1. Types de données à archiver

L'archivage permet :

- D'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.
- De conserver les pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques
- les PC
- les DPC
- les accords contractuels avec d'autres AC
- les certificats et LCR tels qu'émis ou publiés
- les récépissés ou notifications (à titre informatif)
- Les engagements signés des MC
- les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement
- les journaux d'évènements des différentes entités de l'IGC

5.5.2. Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé pendant au moins cinq ans, comptés au maximum à partir de l'acceptation du certificat par son porteur.

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AE ou le MC lors de toute sollicitation par les autorités habilitées.

Ce dossier, complété par les mentions consignées par l'AE ou le MC, doit permettre de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC (ou responsable du composant ou de l'application identifiée dans le DN du certificat)..

Certificats et LCR émis par l'AC

Les certificats de clés de porteurs et d'AC, ainsi que les LCR produites, sont archivés pendant au moins cinq ans après l'expiration de ces certificats.

Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 seront archivés pendant cinq ans après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage offrent le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être assurée tout au long de leur cycle de vie.

5.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, sont :

- protégées en intégrité
- accessibles aux personnes autorisées
- accessibles pour relecture et exploitation

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

5.5.4. Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives.

La présente PC ne fournit pas d'exigence particulière concernant la procédure de sauvegarde des archives.

5.5.5. Exigences d'horodatage des données

Cf. chapitre 5.4.4 pour la datation des journaux d'évènements.

Le chapitre 6.8 précise les exigences en matière de datation / horodatage.

5.5.6. Système de collecte des archives

La présente PC ne fournit pas d'exigence particulière sur ce sujet, si ce n'est que le système de collecte des archives, qu'il soit interne ou externe, doit respecter les exigences de protection des archives concernées.

5.5.7. Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à **2 jours ouvrés**, sachant que seule l'AC, en tant qu'autorité, peut accéder à toutes les archives. L'AC peut être représentée par le contrôleur ou le Responsable de sécurité de l'IGC.

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 doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

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

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

5.7. Reprise suite à compromission et sinistre

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

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site internet, récépissé...).

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

Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC, des engagements de l'AC dans sa propre PC, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

Ce plan doit être testé au minimum tous les **2 ans**.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante (cf. chapitre 5.7.2).

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué : cf. chapitre 4.9.

5.7.4. Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC (cf. chapitre 5.7.2).

5.8. Fin de vie de l'IGC

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

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

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

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

1. Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats).
2. Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC. A défaut, les applications concernées refuseront les certificats émis par des AC dont les LCR en cours de validité ne seraient plus accessibles, même si le certificat du porteur est encore valide.

Des précisions quant aux engagements suivants doivent ainsi être annoncées par l'AC dans sa PC :

1. Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire et, au moins, sous le délai **1 mois**.

Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux points 1, 2 et 3 ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans sa PC.

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

1. S'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats
2. Prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante
3. Révoquer son certificat
4. Révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité
5. Informer (par exemple par récépissé) tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre 3.2.3)

6. MESURES DE SECURITE TECHNIQUES

6.1. Génération et installation de bi clés

6.1.1. Génération des bi-clés

6.1.1.1. Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (cf. chapitre 5).

Les clés de signature d'AC doivent être générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre 5.2.1), dans le cadre de « cérémonies de clés ». Ces cérémonies doivent se dérouler suivant des scripts préalablement définis.

L'initialisation de l'IGC et/ou la génération des clés de signature d'AC s'accompagne de la génération de parts de secrets d'IGC (principe de protection Shamir, n sur m). Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.

Concernant la présente AC le partage de secret sur un principe de **3 sur 6**.

6.1.1.2. Clés porteurs générées par l'AC

Les exigences de ce paragraphe ne s'appliquent que si la bi-clé du porteur est générée par l'AC.

La génération des clés des porteurs doit être effectuée dans un environnement sécurisé (cf. chapitre 5).

Les bi-clés des porteurs doivent être générées :

- Soit directement dans le dispositif d'authentification destiné au porteur conforme aux exigences du chapitre 12 ci-dessous pour le niveau de sécurité considéré
- Soit dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré, puis transférées de manière sécurisée dans le dispositif d'authentification destiné au porteur sans que l'AC n'en garde aucune copie.

6.1.1.3. Clés porteurs générées par le porteur

Dans le cas où le porteur génère sa bi-clé, cette génération doit être effectuée dans un dispositif répondant aux exigences du chapitre 12 ci-dessous pour le niveau de sécurité considéré. L'AE doit s'en assurer auprès du porteur, au minimum au travers d'un engagement contractuel clair et explicite du porteur vis-à-vis de l'AE. Cet engagement se traduit par :

- La signature des conditions d'utilisation par exemple
- La remise d'un PKCS#10 dont les informations seront vérifiées par l'AE

6.1.2. Transmission de la clé privée à son propriétaire

Si l'AC génère la bi-clé du porteur (cf. chapitre 6.1.1.2), la clé privée doit être transmise au porteur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité. Cette transmission doit se faire de préférence directement dans le dispositif d'authentification destiné au porteur, ou suivant un moyen équivalent.

6.1.3. Transmission de la clé publique à l'AC

En cas de transmission de la clé publique du porteur vers une composante de l'AC (cas où la bi-clé est générée par le porteur), la clé devra être protégée en intégrité et son origine devra en être authentifiée.

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

Les clés publiques de vérification de signature de l'AC doivent être diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

La clé publique de l'AC sera mise à disposition par la **DJO** sur un site de confiance (interne ou externe) selon les usages. La présente PC sera également accessible depuis ce site.

6.1.5. Tailles des clés

Les clés d'AC et de porteurs doivent respecter les exigences de caractéristiques (tailles, algorithmes, etc.) du chapitre 7.

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

L'équipement de génération de bi-clés doit utiliser des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé (cf. chapitre 7).

6.1.7. Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats et de LCR (cf. chapitre 7).

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature (cf. chapitre 7).

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

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature, ainsi que le cas échéant pour la génération des clés des porteurs, répondent aux exigences du chapitre 11 ci-dessous.

6.2.1.2. Dispositifs d'authentification des porteurs

Les dispositifs d'authentification des porteurs, pour la mise en œuvre de leurs clés privées d'authentification, respectent les exigences du chapitre 12.

6.2.2. Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la bi-clé est traitée au chapitre 6.1.1.1, l'activation de la clé privée au chapitre 6.2.8 et sa destruction au chapitre 6.2.10.

{2 étoiles} Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance (porteurs de secrets d'IGC) et s'appuie sur un boîtier cryptographique mettant en œuvre le partage des secrets Shamir.

6.2.3. Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des porteurs ne doivent en aucun cas être séquestrées.

6.2.4. Copie de secours de la clé privée

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

Pour les clés d'AC, la **DJO** se réserve le droit d'effectuer des copies de secours, dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous, pour des raisons de plan de continuité de l'IGC. En effet, les copies de secours pourront être utilisées en cas de sinistre de l'IGC principale.

En cas d'exportation des clés d'AC, celles-ci devront être chiffrées. Le contrôle des opérations de chiffrement / déchiffrement doit être conforme aux exigences du chapitre 6.2.2.

6.2.5. Archivage de la clé privée

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

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

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

Si l'AC génère les clés privées des porteurs en dehors du dispositif du porteur, le transfert doit se faire conformément aux exigences du chapitre 6.1.1.2 ci-dessus.

Pour les clés privées d'AC, tout transfert doit se faire sous forme chiffrée.

6.2.7. Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC sont stockées dans un module cryptographique répondant au minimum aux exigences du chapitre 11 ci-dessous.

6.2.8. Méthode d'activation de la clé privée

6.2.8.1. Clés privées d'AC

La méthode d'activation des clés privées d'AC dans un module cryptographique doit permettre de répondre aux exigences définies dans le chapitre 11.

{2 étoiles} L'activation des clés privées d'AC dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre 6.4) et doit s'appuyer sur la méthode Shamir retenue pour la présente PC.

6.2.8.2. Clés privées des porteurs

La méthode d'activation de la clé privée du porteur dépend du dispositif utilisé. L'activation de la clé privée du porteur doit au minimum être contrôlée via des données d'activation (cf. chapitre 6.4) et doit permettre de répondre aux exigences définies dans le chapitre 12 pour le niveau de sécurité considéré.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Clés privées d'AC

La désactivation des clés privées d'AC dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc. Une clé privée d'AC peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans le chapitre 11.

6.2.9.2. Clés privées des porteurs

Les conditions de désactivation de la clé privée d'un porteur doivent permettre de répondre aux exigences définies dans le chapitre 12.

6.2.10. Méthode de destruction des clés privées

6.2.10.1. Clés privées d'AC

La méthode de destruction des clés privées d'AC doit permettre de répondre aux exigences définies dans le chapitre 11.

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé doit être systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.10.2. Clés privées des porteurs

En fin de vie de la clé privée d'un porteur, la méthode de destruction de cette clé privée doit permettre de répondre aux exigences définies dans le chapitre 12.

6.2.11. Niveau d'évaluation sécurité du module cryptographique

Les modules cryptographiques de l'AC doivent être évalués au niveau correspondant à l'usage visé, tel que précisé au chapitre 11 ci-dessous.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Archivage des clés publiques

Les clés publiques de l'AC et des porteurs sont archivées dans le cadre de l'archivage des certificats correspondants. Néanmoins, dans le cas de la signature électronique notamment, il revient à l'application d'archiver le certificat du signataire dans l'enveloppe constituant la preuve.

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

Les bi-clés et les certificats des porteurs couverts par la présente PC doivent avoir la même durée de vie, au moins égale à **1 an**, et au maximum de **3 ans**.

La fin de validité d'un certificat d'AC doit être postérieure à la fin de vie des certificats porteurs qu'elle émet. Elle a été définie pour la présente AC à **5 ans**.

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

6.4.1.1. VI.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 d'un module cryptographique de l'IGC sont effectuées lors de la phase d'initialisation et de personnalisation de ce module. Ces données d'activation ne doivent être connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. chapitre 5.2.1).

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

Sans objet.

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 les modules cryptographiques de l'IGC doivent être protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. 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 aux clés privées des porteurs

Sans objet.

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, de nature physique et/ou logique)
- 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. Les mises à jour logicielles et de définition de virus sont contrôlées par la **DJO** et gérées sur un serveur interne auquel l'AC se connecte.
- 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)

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

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

6.5.2. Niveau d'évaluation sécurité des systèmes informatiques

{2 étoiles} Le module cryptographique de l'AC fait l'objet d'une qualification EAL 4+ et DCSSI.

6.6. Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques respectent les objectifs de sécurité définis par la **DJO**.

6.7. Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC doit être documentée et doit respecter dans la mesure du possible des normes de modélisation et d'implémentation. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau doivent être documentées et contrôlées.

6.7.1. Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'IGC doit être signalée à l'AC 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.

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

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

6.8. Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

De plus, les échanges entre composantes au sein de l'IGC peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

6.9. Horodatage / Système de datation

Plusieurs exigences de la présente PC nécessitent la datation par les différentes composantes de l'IGC d'événements liés aux activités de l'IGC (cf. chapitre 5.4).

Pour dater ces événements, les différentes composantes de l'IGC utilisent l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près. Cette exigence n'est plus vraie si un composant est mis hors ligne.

7. PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1. Profil des certificats

7.1.1. Numéro de version

Les certificats émis dans le cadre de l'IGC de la **DJO** respectent la norme X.509 v3.

7.1.2. Champs de base

Les certificats respectent le format de base des certificats définis dans la recommandation x.509v3 et incluent au minimum les champs de base suivants :

Nom du champ	Description	Contenu
Version	Version du certificat X.509	Contient la valeur 2 pour indiquer que le certificat est un certificat x.509v3
SerialNumber	Numéro de série du certificat	Contient une valeur entière pour indiquer le numéro de série du certificat, cette valeur doit être unique pour chaque certificat émis par l' AC JO Publication
Signature	Signature de l'AC pour authentifier : SHA-1 160 bits pour le hashage et RSA pour la signature "sha-1WithRSASignature"	sha1WithRSAEncryption
Issuer	Nom de l'AC	Contient le DN (X.500) de l' AC JO Publication respectant les prescriptions de la PC de l'AC Racine
Validity	Période de validité du certificat	Contient les dates d'activation et d'expiration du certificat
Subject	Nom du porteur	Contient le DN (X.500) de l'application ou de l'entité représentante
Subject Public Key Info	Informations sur la clé publique de l'abonné	Contient l'OID de l'algorithme et la clé publique de l'abonné (longueur de clés = 2048 bits)
Extensions	Liste des extensions	Voir chapitre 7.1.3

7.1.3. Extensions du certificat de signature des publications

Les certificats émis par l'**AC JO Publication** comportent les extensions X.509v3 suivantes :

Extension	Extension critique (O/N)	Description	Valeur
Authority Key Identifier	N	Élément d'identification de la clé publique de l'AC signant le certificat	Identique au champ « <i>SubjectKeyIdentifier</i> » du certificat de l' AC JO Publication
KeyUsage	O	Description des utilisations autorisées de la clé privée	nonRepudiation

Extension	Extension critique (O/N)	Description	Valeur
Extended Key Usage	N	Extensions particulières nécessaires pour certains usages comme l'authentification Windows	
Certificate Policies	N	OID de la PC régissant le certificat et intitulé de la PC	1.2.250.1.144.1.1.2.1
Subject Alternative Name	N	Autres éléments nominatifs associés au porteur, en particulier adresse e-courriel, ou le nom unique de l'utilisateur au sens domaine Windows.	Optionnel (selon les besoins spécifiques de l'application)
Subject Key Identifier	N	Elément d'identification de la clé publique du porteur	Valeur alphanumérique
CRL Distribution Points	O	indique les adresses auxquelles est publiée la LCR de l'AC ayant émis le certificat	Adresses publiques par ordre de priorité : HTTP, LDAP

Si nécessaires d'autres extensions pourront être ajoutées pour le strict usage d'authentification (Authentification IPsec ou Windows en particulier) à condition que :

- Ces extensions ne soient pas critiques et ne perturbent pas l'utilisation du certificat pour d'autres applications
- Les usages restent dans le périmètre fixé par la présente PC

7.1.4. Extensions du certificat de signature des jetons d'horodatage

Les certificats émis par l'**AC JO Publication** comportent les extensions X.509v3 suivantes :

Extension	Extension critique (O/N)	Description	Valeur
Authority Key Identifier	N	Elément d'identification de la clé publique de l'AC signant le certificat	<i>Identique au champ « SubjectKeyIdentifier » du certificat de l'AC JO Publication</i>
KeyUsage	O	Description des utilisations autorisées de la clé privée	DigitalSignature
Extended Key Usage	N	Extensions particulières nécessaires pour certains usages	Id-kp-timeStamping

Extension	Extension critique (O/N)	Description	Valeur
		comme l'authentification Windows	
Certificate Policies	N	OID de la PC régissant le certificat et Intitulé de la PC	1.2.250.1.144.1.1.2.1
Subject Alternative Name	N	Autres éléments nominatifs associés au porteur, en particulier adresse e-courriel, ou le nom unique de l'utilisateur au sens domaine Windows.	Optionnel (selon les besoins spécifiques de l'application)
Subject Key Identifier	N	Elément d'identification de la clé publique du porteur	Valeur alphanumérique
CRL Distribution Points	O	indique les adresses auxquelles est publiée la LCR de l'AC ayant émis le certificat	Adresses publiques par ordre de priorité : HTTP, LDAP

Si nécessaires d'autres extensions pourront être ajoutées pour le strict usage d'authentification (Authentification IPsec ou Windows en particulier) à condition que :

- Ces extensions ne soient pas critiques et ne perturbent pas l'utilisation du certificat pour d'autres applications
- Les usages restent dans le périmètre fixé par la présente PC

7.1.5. OID des algorithmes

Les identificateurs d'algorithmes doivent être inscrits auprès d'un registre (par exemple, un registre international tel que celui de l'ISO).

L'algorithme de hachage utilisé dans le cadre de l'IGC de la **DJO** est SHA-1. L'algorithme de chiffrement utilisé dans le cadre de l'IGC de la **DJO** est RSA.

7.1.6. Forme des noms

Les noms attribués aux porteurs dans le cadre de l'IGC de la **DJO** respectent la norme X.500, comme détaillé au chapitre 3.1.4 de ce document.

7.1.7. Contraintes sur les noms

Les contraintes applicables aux noms inclus dans les certificats émis par l'AC Agents sont exposées au chapitre 3.1.2 de ce document.

7.1.8. OID des PC

L'AC Agents s'assure que les certificats qu'elle délivre contiennent l'OID de la PC qui les gouverne.

Cf. chapitre 1.2

7.1.9. Utilisation de l'extension « contraintes de politique »

La présente PC n'émet pas d'exigence particulière sur ce sujet.

7.1.10. Sémantique et syntaxe des qualifiants de politique

La présente PC n'émet pas d'exigence particulière sur ce sujet.

7.1.11. Sémantiques de traitement des extensions critiques de la PC

Les extensions critiques sont traitées conformément à la norme ISO [9594-8], définissant le cadre applicable aux certificats de clé publique dans le cadre de l'authentification.

7.2. Profil des LCR

7.2.1. Numéro de version

Les LCR émises utilisent la version 2 du format défini dans la norme [9594-8].

7.2.2. Champs de base

Les champs de base des LCR émises par l'*AC JO Publication* sont les suivants :

Champ	Description
Version	Version de la LCR X.509
Signature	Identifiant de l'algorithme utilisé pour produire le sceau d'intégrité de la liste sha1WithRSAEncryption retenu pour la présente PC.
Issuer	Nom de l'AC
This Update	Date d'émission de la LCR
Next Update	Date limite d'émission de cette LCR
Revoked Certificates	Liste d'enregistrement de révocation. On spécifiera pour chaque révocation les valeurs associées aux champs suivants : - User Certificate (numéro de série du certificat révoqué) - Revocation Date (date de révocation du certificat).
CRL Extensions	Extensions générales de la LCR

La LCR dans sa forme finale est l'ensemble des éléments suivants :

Champ	Description
tbsCertlist	L'ensemble des champs décrits ci-dessus
signatureAlgorithm	L'identifiant de l'algorithme utilisé pour produire le sceau d'intégrité de la liste sha1WithRSAEncryption retenu pour la présente PC.
signatureValue	Le résultat de cet algorithme sur l'ensemble des champs de tbsCertList

7.2.3. Extensions de LCR et d'entrées de LCR

Les LCR incluent les champs de base présentés au paragraphe précédent, ainsi que les extensions d'entrée suivantes :

Extension d'entrée	Description
Authority Key Identifier	Identifie la clé publique de l'AC ayant signé la LCR
CRL Number	Donne un nombre croissant séquentiel pour chaque LCR émise
Reason Code	Identifie la cause de révocation du certificat. Sauf spécification particulière, la valeur pour chaque révocation sera « unspecified ».

8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification et, d'autre part, ceux que doit réaliser, ou faire réaliser, l'AC afin de s'assurer que l'ensemble de son IGC, ainsi que le cas échéant le ou les MC, est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

La reconnaissance du respect par l'AC des exigences de la présente PC est effectuée dans le cadre du schéma de qualification des prestataires de services de confiance mis en place et géré par le COFRAC (cf. [PROG_ACCRED]).

La démarche et les exigences liées aux audits de qualification (respectivement de référencement) sont définies dans [PROG_ACCRED] (respectivement [CDC_OAR]) et ne sont donc pas reprises ici.

La suite du présent chapitre ne concerne donc que les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

8.1. Fréquences et / ou circonstances des évaluations

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

En outre, ils procèdent régulièrement à un contrôle de conformité de l'ensemble de son IGC, suivant la fréquence **1 fois tous les 2 ans**.

8.2. Identités / qualifications des évaluateurs

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

8.3. Relations entre évaluateurs et entités évaluées

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

8.4. Sujets couverts par les évaluations

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

8.5. Actions prises suite aux conclusions des évaluations

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

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

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

- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et la DPC.

8.6. Communication des résultats

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

9. AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

Sans objet.

9.1.2. Tarifs pour accéder aux certificats

Sans objet.

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

Sans objet.

9.1.4. Tarifs pour d'autres services

Sans objet.

9.1.5. Politique de remboursement

Sans objet.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

Sans objet.

9.2.2. Autres ressources

Sans objet.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- La partie non-publique de la DPC de l'AC,
- Les clés privées de l'AC, des composantes et des porteurs de certificats
- Les données d'activation associées aux clés privées d'AC et des porteurs
- Tous les secrets de l'IGC
- Les journaux d'événements des composantes de l'IGC
- Le dossier d'enregistrement du porteur
- Les causes de révocations, sauf accord explicite de publication

9.3.2. Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3. Responsabilités en terme de protection des informations confidentielles

L'AC, en tant qu'autorité, est tenue de respecter la législation et la réglementation en vigueur sur le territoire français.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel 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. Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- Les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du porteur)
- Le dossier d'enregistrement du porteur

9.4.3. Informations à caractère non personnel

Sans objet

9.4.4. Responsabilité en termes de protection des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 0 ci-dessous).

9.4.5. Notification et consentement d'utilisation des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 0 ci-dessous).

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

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 0 ci-dessous).

9.4.7. Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5. Droits sur la propriété intellectuelle et industrielle

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

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 présente et les documents qui en découlent
- Respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante)
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre 8) et l'organisme de qualification
- Respecter les accords ou contrats qui les lient entre elles ou aux porteurs
- Documenter leurs procédures internes de fonctionnement
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité

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 porteur donné et que ce porteur a accepté le certificat, conformément aux exigences du chapitre 4.4 ci-dessus ; pour cela l'AC s'appuie sur l'historique conservé des opérations conservée sur la plate-forme technique (statut des certificats, identifiant du valideur, date de validation) ou sur les supports d'archivage selon la période de contrôle.
- Garantir et maintenir la cohérence de sa DPC avec sa PC
- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un porteur et l'AC est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC

L'AC, en tant qu'autorité, est responsable de la conformité de sa Politique de Certification, avec les exigences émises dans les PC Type de la PRIS pour le niveau de sécurité considéré (**2 étoiles**). 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. L'AC s'appuie sur les rôles de confiance décrits au chapitre 5.2.1 pour assurer ces tâches.

De plus, l'AC (en tant qu'autorité) reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des porteurs fournies lors de l'enregistrement d'un certificat (date de naissance, matricule, etc.). Les informations contenues dans le DN du certificat étant publiques, elles ne sont pas considérées comme données personnelles.

Cette règle vaut pour le fonctionnement propre de l'IGC. Toute utilisation par quiconque (acteur ou non de l'IGC) des données personnelles des porteurs est strictement interdite pour quelque usage que ce soit, sauf accord écrit entre les parties (entité tiers / AC).

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes.

9.6.2. Service d'enregistrement

L'AE a pour obligation de :

- Protéger et garantir l'intégrité et la confidentialité de sa clé privée permettant d'accéder aux fonctions d'enregistrement et de gestion du cycle de vie des certificats
- Respecter et appliquer la DPC
- Respecter les accords ou engagements qui la lie aux porteurs
- Documenter ses procédures internes de fonctionnement
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elle s'engage, dans des conditions garantissant qualité et sécurité
- Préserver par tous les moyens disponibles la confidentialité des données personnelles des porteurs de certificats, recueillies dans le cadre de l'enregistrement de ces porteurs

9.6.3. Porteurs de certificats

Le porteur a le devoir de :

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

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

9.6.4. Utilisateurs de certificats

Les utilisateurs utilisant les certificats doivent :

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

9.6.5. Autres participants

Sans objet.

9.7. Limite de garantie

Sans objet.

9.8. Limite de responsabilité

Sans objet.

9.9. Indemnités

Sans objet.

9.10. Durée et fin anticipée de validité de la PC

9.10.1. Durée de validité

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

9.10.2. Fin anticipée de validité

La publication d'une nouvelle version de la PC Type de la PRIS peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer la présente PC. Néanmoins, la DJO évaluera les impacts sur l'IGC et les utilisateurs des certificats (applications, ressources).

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

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

9.10.3. Effets de la fin de validité et clauses restant applicables

Sans objet.

9.11. Notifications individuelles et communications entre les participants

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

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

9.12. Amendements à la PC

9.12.1. Procédures d'amendements

L'AC devra contrôler que tout projet de modification de sa PC reste conforme aux exigences de la PC Type de la PRIS et des éventuels documents complémentaires de la PRIS. En cas de changement important il est recommandé à l'AC de faire appel à une expertise technique pour en contrôler l'impact.

9.12.2. Mécanisme et période d'information sur les amendements

Sans objet.

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 cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

9.13. Dispositions concernant la résolution de conflits

Sans objet.

9.14. Juridictions compétentes

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

9.15. Conformité aux législations et réglementations

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 0 ci-dessous.

9.16. Dispositions diverses

9.16.1. Accord global

Sans objet.

9.16.2. Transfert d'activités

Cf. chapitre 5.8.

9.16.3. Conséquences d'une clause non valide

Sans objet.

9.16.4. Application et renonciation

Sans objet.

9.16.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.

9.17. Autres dispositions

Sans objet.

10. ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1. Réglementation

Renvoi	Document
[CERTIF]	<i>Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.</i>
[CNIL]	<i>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</i>
[LCEN]	<i>Loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie.</i>
[REG_1]	<i>Loi n° 90-1170 du 29 12 90, modifiée par la loi 91-648 du 11 juillet 1991, modifiée par la loi 96-659 du 26 juillet 1996 sur la réglementation des télécommunications, notamment son article 28.</i>
[REG_2]	<i>Décret n°98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie, modifié par le décret n°2002-688 du 2 mai 2002.</i>
[REG_3]	<i>Arrêté du 17 mars 1999 définissant la forme et le contenu du dossier concernant les déclarations ou demandes d'autorisation relatives aux moyens et prestations de cryptologie.</i>
[SIG]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

10.2. Documents techniques

Renvoi	Document
[CWA14167-4]	CWA 14167-4 (2004-02) <i>Cryptographic Module for CSP Signing Operations with Backup – Protection Profile (CMCSO-PP)</i>
[CWA14169]	CWA 14169 (2004-03) <i>Secure Signature Creation Devices "EAL4+" (SSCD)</i>
[CWA14365-2]	CWA 14365-2 (2004-03) <i>Guide on the Use of Electronic Signatures -Part 2: Protection Profile for Software Signature Creation Devices</i>
[DCSSI_ALGO]	<i>Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, DCSSI, version 1.02 du 19 novembre 2004</i> <i>N°2791 SGDN/DCSSI/SDS/Crypto du 19 novembre 2004</i> <i>Cf. www.ssi.gouv.fr</i>

Renvoi	Document
[ETSI_NQCP]	<i>ETSI TS 102 042 V1.1.1 (2002-04)</i> <i>Policy Requirements for Certification Authorities issuing public key certificates</i>
[ETSI_SigPol]	<i>ETSI TR 102 272 - ASN.1 format for signature policies</i> <i>ETSI TR 102 038 - XML format for signature policies</i>
[PC ²]	<i>Procédures et politiques de certification de clés, CISSI, version 2.2 de Janvier 2001.</i>
[PP_AC]	<i>Profil de protection AC</i> <i>Cf. www.ssi.gouv.fr</i>
[PP_AE]	<i>Profil de protection AE</i> <i>Cf. www.ssi.gouv.fr</i>
[PREAMB]	<i>PRIS - Préambule - Version 2.0 du 01/06/2005</i>
[PRES_SIGN]	<i>PRIS - Présentation du service de sécurité "Signature" - Version 2.0 du 01/06/2005</i>
[PROFILS]	<i>PRIS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.0 du 01/06/2005</i>
[PROG_ACCRED]	<i>COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – avril 2005</i>
[QUALIF_STD]	<i>Processus de qualification standard, DCSSI, V 1.0 du 28/07/ 2003 N° 1591/SGDNDCSSI/SDR</i>
[QUALIF_RENF]	<i>Processus de qualification renforcée, DCSSI, V 1.0 du 24/06/04 N° 1549/SGDN/DCSSI/SDR</i>
[RFC3647]	<i>IETF - Internet X.509 Public Key Infrastructure -Certificate Policy and Certification Practice Framework - 11/2003</i>
[Socle_IAS]	<i>Socle commun carte à puce : Identification, Authentification, Signature pour les cartes de l'e-administration</i> <i>Disponible sur demande à l'adresse email pris.adae@pm.gouv.fr</i>

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

11.1. 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, 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
- Etre 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
- Etre 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 privée 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.

{2 étoiles} Le module cryptographique de l'AC doit détecter les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée.

11.2. Exigences sur la certification

{2 étoiles} Le module cryptographique utilisé par l'AC doit, dans les conditions prévues par le décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, être certifié conforme aux exigences du chapitre 11 ci-dessus par le Premier ministre.

{2 étoiles} Le boîtier cryptographique retenu pour la présente AC répond au niveau d'exigence EAL4+

12. ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF D'AUTHENTIFICATION

12.1. Exigences sur les objectifs de sécurité

Le dispositif **de signature**, utilisé par 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 :

- 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 de la clé privée en cas de re-génération de la clé privée
- Garantir la confidentialité et l'intégrité de la clé privée
- Assurer la correspondance entre la clé privée et la clé publique
- Générer une authentification qui ne peut être falsifiée sans la connaissance de la clé privée
- Assurer la fonction d'authentification pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif

12.2. Exigences sur la certification

{2 étoiles} Le dispositif **de signature** utilisé par le porteur doit, dans les conditions prévues par le décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, être certifié conforme aux exigences du chapitre XII.1 ci-dessus par le Premier ministre.

{2 étoiles} Les supports doivent répondre au niveau d'exigence EAL2+. Néanmoins, la DJO se réserve une certaine marge dans le niveau de protection.

13. ANNEXE 4 : RESUME DES INFORMATIONS PARTICULIERES A LA PRESENTE PC

Légende :

- **Normal** : commun à l'ensemble des PC DJO
- *Italique* : commun au PC de la présente AC concernée
- **Gras** : spécificité de la présente PC
- **{2 étoiles}** : spécificité liée au niveau 2 étoiles de la PRIS

Référence	Description	Spécificité de la présente PC
Chapitre INTRODUCTION		
[INT_PROPRIETAIRE]	Nom explicite du propriétaire de la présente PC	Direction des Journaux officiels
[INT_PROPRIETAIRE_ABREV]	Nom abrégé du propriétaire de la présente PC	DJO
[INT_ENTITE]	Entité(s) à laquelle s'adresse la présente PC	<i>composants techniques de l'activité publication</i>
[INT_CERT_TYPE]		de signature
[INT_PC_NOM]	Nom complet de la PC	<i>Politiques de Certification Direction des Journaux officiels – Autorité de Certification JO Publication –</i> Certificats de signature
[INT_AC_ABREV]	Nom abrégé de l'AC	<i>AC JO Publication</i>
[INT_PC_OID]	Numéro OID de la présente PC	1.2.250.1.144.1.1.2.1
[INT_PORTEUR_CERT]	Nature du porteur de certificat	<p><i>Dans le cadre de la présente PC, un porteur de certificat est un composant technique d'une application spécifique à l'activité publication et d'horodatage de la DJO (application Lois et décrets par exemple). Le certificat est propre au composant technique.</i></p> <p><i>Les opérations d'enregistrement, de renouvellement, de demande de révocation et d'utilisation engage la responsabilité de l'entité (personne, service de la DJO par exemple) qui à la charge de la gestion du certificat et qui veille à ce qu'il soit utilisé dans le respect de la politique de sécurité de l'application concernée.</i></p> <p><i>Le certificat est utilisé par l'application ou des composants de l'application dans le cadre des activités DJO.</i></p> <p><i>Le porteur (ou entité responsable) respecte les conditions qui lui incombent définies dans la présente PC.</i></p>
[INT_UTILISATEUR_CERT]	Utilisateur de certificats émis par la présente PC	<ul style="list-style-type: none"> • <i>Un service de la DJO faisant partie du système de publication des documents officiels de la DJO ou utilisateur du système. Ce service est accessible par voie électronique (application, serveur Internet, base de données, etc.), sous la responsabilité d'une personne physique ou morale. Il utilise un certificat et un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message du porteur de certificat (application ou service technique de publication DJO). L'application met en œuvre la politique et les pratiques de sécurité édictées par le responsable</i>

Référence	Description	Spécificité de la présente PC
		<p>d'application.</p> <ul style="list-style-type: none"> • <i>Un usager accédant à une publication de la DJO, qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur de certificat (l'application) sur le document publié par un service de la DJO</i> • <i>Un abonné accédant au service d'horodatage qui utilise un certificat et un dispositif de demande de jetons d'horodatage.</i> <p>Le service de signature permet ainsi de garantir l'intégrité des documents et données signées par le porteur de certificat.</p>
[INT_MC]	Mandataire de certification	Dans le cas de la DJO, le mandataire pourra être un agent du service du personnel.
[INT_PERSAUT]	Personne autorisée	Dans le cas de la DJO, il peut s'agir d'un responsable de service des systèmes d'information ou d'un responsable hiérarchique du porteur.
[INT_ANA_RISQUE]	Particularité des AC Codes, Publication et Rôle pour lesquelles une analyse de risque de l'application permettra de déterminer les objectifs de sécurité de l'IGC.	<ul style="list-style-type: none"> • <i>Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse. Dans le cadre de la présente PC on s'appuiera sur l'analyse de risque relative à l'application qualifiée comme étant la plus critique (lois et décrets par exemple)</i>
[INT_PC_ACR_OID]	Numéro OID de la PC AC JO Racine	1.2.250.1.144.1.1.1.1
[INT_PC_ACPUBLICATION1_OID]	Numéro OID de la PC AC JO Publication – certificats de signature	1.2.250.1.144.1.1.2.1
[INT_PC_ACPUBLICATION2_OID]	Numéro OID de la PC AC JO Publication – certificats d'authentification	1.2.250.1.144.1.1.3.1
[INT_PC_ACINFRA_OID]	Numéro OID de la PC AC JO Infra – certificats d'authentification	1.2.250.1.144.1.1.4.1
[INT_PC_ACCODES_OID]	Numéro OID de la PC AC JO Codes – certificats de signature de code	1.2.250.1.144.1.1.5.1
[INT_PC_ACROLES2_OID]	Numéro OID de la PC AC JO Roles – certificats d'authentification	1.2.250.1.144.1.1.6.1
[INT_PC_ACAGENTS1_OID]	Numéro OID de la PC AC JO Agents – certificats d'authentification	1.2.250.1.144.1.1.7.1
[INT_PC_ACAGENTS2_OID]	Numéro OID de la PC AC JO Agents – certificats de signature	1.2.250.1.144.1.1.8.1
[INT_USAGE_PORTEUR1]	Usage des bi-clés et certificats	<ul style="list-style-type: none"> • Signer électroniquement des données (documents ou messages) avec des outils fournis par les Journaux officiels ; la

Référence	Description	Spécificité de la présente PC
		<p>signature est vérifiée par un service des Journaux officiels accessible par voie électronique ou par un service tiers conforme au cadre de signature de la DJO.</p> <ul style="list-style-type: none"> • Signer électroniquement des données avec des outils fournis par les Journaux officiels ; la signature est vérifiée par un agent ou un usager qui utilise les outils des Journaux officiels ou un outil tier conforme au cadre de signature DJO.
[INT_USAGE_PORTEUR2]	Applications concernées	<ul style="list-style-type: none"> • La signature des éditions publiées par la DJO (textes Lois et décrets par exemple). • La signature de jetons d'horodatage générés par le système d'horodatage de la DJO. • La signature de messages dans le cadre des échanges entre applications ou services du système de publication DJO.
[INT_USAGE_PORTEUR3]	Type service	service de signature
[INT_USAGE_PORTEUR4]	Assurance de l'identité du porteur et de ses droits	L'utilisateur du certificat a ainsi l'assurance que le porteur identifié dans le certificat (nom de l'application), représenté par l'entité responsable de l'application, a manifesté son consentement quant au contenu des données signées électroniquement à l'aide de la clé privée correspondante. Le niveau d'assurance correspond au niveau 2 étoiles de la PRIS v2.
[INT_USAGE_PORTEUR5]	Niveau de sécurité PRISv2 considéré	{2 étoiles} Les certificats de signature objets de la présente PC sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité pour pouvoir signer indûment des données sont forts (intérêt pour les usurpateurs, effets de la signature, etc.).
[INT_LCR_LAR]	Emission ou non de LCR / LAR	LCR
[INT_CONTACT]	Point de contact PC	Direction des Journaux officiels Service des systèmes d'information 26, rue Desaix 75015 Paris
[INT_CONFORMITEP C]	Entité habilitée à déterminer la conformité DPC/PC	Autorité Qualifiée en Sécurité des Systèmes d'Information (AQSSI)
INT_CONFORMITEP C_ABREV]	Abréviation de l'entité habilitée à déterminer la conformité DPC/PC	AQSSI
[PUB_INFOPUBLIEES]	Informations spécifiques publiées par la présente AC	<ul style="list-style-type: none"> • Les certificats en cours de validité des AC de la hiérarchie dont dépend la présente AC, les différentes politiques de certification correspondantes et les éventuels documents complémentaires, ceci jusqu'à l'AC Racine
[PUB_T_DIFF_AC]	Délai de diffusion préalable des certificats d'AC (conforme PRIS 2 étoiles)	24h
[PUB_T_INF_DISP]	Disponibilité de la fonction	Jours ouvrés

Référence	Description	Spécificité de la présente PC
	de publication des informations (hors informations d'état des certificats).	
[PUB_T_INF_INDISP]	Durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de publication (conforme PRIS 2 étoiles)	8h (jours ouvrées)
[PUB_T_INF_MAX]	Durée maximale totale d'indisponibilité par mois de la fonction de publication. (conforme PRIS 2 étoiles)	32h (jours ouvrés)
[PUB_T_AC_DISP]	Disponibilité des systèmes publiant les certificats d'AC. (conforme PRIS 2 étoiles)	24h/24 7j/7
[PUB_T_AC_INDISP]	Durée maximale d'indisponibilité par interruption (panne ou maintenance) des systèmes publiant les certificats d'AC. (conforme PRIS 2 étoiles)	2h
[PUB_T_AC_MAX]	Durée maximale totale d'indisponibilité par mois des systèmes publiant les certificats d'AC. (conforme PRIS 2 étoiles)	8h
[PUB_CA_INFO]	Critères de contrôle d'accès aux informations publiées relatifs au niveau 2 étoiles de la PRISv2.	<p>{2 étoiles} L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).</p> <p>L'accès en modification aux systèmes de publication des autres informations doit être strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un contrôle d'accès de type mots de passe basé sur une politique de gestion stricte des mots de passe.</p>
[ID_COMPOSITION_D N]	Composition du DN permettant d'identifier le porteur	<p>Dans le cas contraire, le DN du porteur est construit à partir du nom de l'entité responsable (DJO, Service Lois et décrets, ...) de l'application ou du composant logiciel qui sera signé avec le certificat émis. L'AE devra contrôler auprès des responsables de l'application que les informations du DN sont corrects et suffisamment explicites pour désigner l'identité du signataire.</p>
[ID_UNICITE_NOMS1]		<ul style="list-style-type: none"> • commonName = Nom du porteur (entité responsable de l'application concernée) • organizationalUnit = Journaux officiels • organization = Gouv • country = FR
[ID_UNICITE_NOMS2]		Le format du commonName est explicité ci-dessus.

Référence	Description	Spécificité de la présente PC
		<i>Le DN sera fourni par le responsable de l'application nécessitant un certificat de signature. Un contrôle sera effectué sur la validité des informations fournies.</i>
[ID_ENREG_SANSMC 2]	Entité que représentent les agents interne de la DJO	<i>(la DJO pour les composants logiciels internes)</i>
[ID_ENREG_SANSMC 2]	Règles d'enregistrement dans le cas d'un enregistrement sans MC	<p>L'enregistrement doit au moins respecter les règles suivantes :</p> <ul style="list-style-type: none"> • La demande de certificat est émise par l'entité (personne physique ou service) responsable de l'application qui demande le certificat de signature • La procédure d'enregistrement est réalisée dans le cadre d'un face-à-face physique avec l'AE et implique les différents acteurs qui partageront le secret d'accès aux clés • <i>L'AE effectue l'enregistrement du certificat dont la demande se présente sous la forme d'un CSR (Certificate Signing Request), au format PKCS#10. L'entité demandeuse s'engage à respecter le cadre de nommage défini dans le cadre de la présente PC</i> • La demande de certificat de signature est validée par l'AE (en tant qu'autorité) • En fin d'enregistrement, les cartes d'accès aux clés, qui sont stockées dans un boîtier cryptographique, sont remises aux différents porteurs
[ID_ENREG_MC]	Règles d'enregistrement dans le cas d'un enregistrement de MC	<i>Ce cas ne concerne pas la présente PC. La délivrance de certificats d'authentification pour les AE et les MC est décrite dans le cadre de la PC AC Roles (OID : 1.2.250.1.144.1.1.6.1).</i>
[ID_ENREG_AVECMC]	Règles d'enregistrement dans le cas d'un enregistrement de porteur via MC	<i>L'enregistrement respecte les mêmes règles que l'enregistrement sans MC (paragraphe 3.2.3.1), à la différence que l'AE (en tant qu'autorité) est remplacée par le MC.</i>
[ID_RENOUV]	Règles de renouvellement courant	{2 étoiles} <i>La procédure d'identification et d'authentification du porteur est la même que pour l'enregistrement initial (cf. § 3.2.3.1).</i>
[OP_PROC_DEMAND ECERTIF]	Processus et responsabilités relatifs à la demande d'un certificat	<ul style="list-style-type: none"> • Le nom de l'application ou du service pour lesquels est délivré le certificat (nom réel ou pseudonyme) • L'adresse courriel du porteur (responsable de l'application ou du demandeur) ou une adresse institutionnelle <p>Les informations et les documents d'enregistrements sont remis par l'entité responsable de l'application à l'AE ou au MC.</p>
[OP_IDENTITE]	Identité du porteur	<i>"personne morale"</i>

Référence	Description	Spécificité de la présente PC
	(personne physique / personne morale).	
[OP_DUREE_ETSCE RTIF]	Durée d'établissement du certificat	0 à 7 jours ouvrés (0 signifiant un établissement immédiat)
[OP_DELIVRANCE_C ERTIF]	Condition de délivrance du certificat	{2 étoiles} La remise du certificat est effectuée lors de la phase d'enregistrement, en face-à-face avec l'AE. Le certificat est stocké dans un boîtier cryptographique et protégé par des cartes d'accès selon la méthode Shamir.
[OC_ACCEPT_CERTI F]	Conditions d'acceptation du certificat	<i>L'acceptation du certificat est considérée comme tacite et correspond à la récupération du certificat et son intégration dans le support de sécurité (ou le magasin de certificat logiciel sécurisé). Cette opération est réalisée lors du processus d'enregistrement en face-à-face avec l'AE (ou le MC).</i> Les obligations du porteur et le délai correspondant sont clairement mentionnés dans la présente PC ainsi que dans les conditions générales d'utilisation (cf. chapitre 2.2).
[OP_PUB_CERTIF]	Publication du certificat	Le certificat est publié dans l'annuaire de l'IGC. <i>Il n'est publié qu'à des fins de contrôle de l'identité de l'utilisateur et ne sera accessible que par les applications et utilisateurs autorisés par la DJO.</i>
[OP_DUREEVALIDITE CERTIF]	Durée de validité d'un certificat de porteur	deux ans
[OP_ORIG_DEMAND E]	Origine de la demande d'un nouveau certificat.	<i>Le déclenchement de la fourniture d'un nouveau certificat du porteur peut-être automatique ou bien à l'initiative du porteur (c'est-à-dire le responsable du composant logiciel).</i> <i>L'entité, via son MC le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un porteur qui lui est rattaché.</i>
[OP_T_REV_DISP]	Disponibilité du service de révocation	24h/24 7j/7
[OP_T_REV_INDISP]	Durée d'indisponibilité du service de révocation	1h
[OP_T_REV_MAX]	Durée total d'indisponibilité du service de révocation	4h
[OP_T_REV_TRAIT]	Délai de traitement des demandes de révocation	24h
[OP_F_PUB_LCR]	Fréquence de publication des LCR	24h
[OP_T_PUB_LCR]	Délai maximum de publication des LCR	30min
[OP_T_ETAT_DISP]	Disponibilité de la fonction d'information sur l'état des certificats	24h/24 7j/7
[OP_T_ETAT_INDISP]	Durée d'indisponibilité maximale de la fonction d'information sur l'état des certificats	2h
[OP_T_ETAT_MAX]	Durée d'indisponibilité totale de la fonction d'information	8h

Référence	Description	Spécificité de la présente PC
[OP_SEQUESTRE]	sur l'état des certificats Conditions de séquestres des clés privées	Ce document traite des aspects de signature et interdit donc le séquestre des clés privées des porteurs. Les clés privées d'AC ne doivent pas non plus être séquestrées.
[OP_PRAT_SEQUESTRE1]	Politique et pratiques de recouvrement par séquestre des clés	Sans objet.
[OP_PRAT_SEQUESTRE2]	Politique et pratiques de recouvrement par encapsulation des clés de session	Sans objet.
[SEC_SITUATION]	Situation géographique et construction des sites	L'IGC est située dans une des implantations de la DJO.
[SEC_ROLE_CONF]	Rôles de confiance de l'IGC	<i>Dans le cadre de la présente AC, certains rôles seront assurés par les mêmes personnes. La répartition est définie dans le cadre de la DPC.</i>
[SEC_ROLE_CONF_NONCUMUL]	Rôles de confiance non cumulables	{2 étoiles} Concernant les rôles de confiance, les cumuls suivants sont interdits : <ul style="list-style-type: none"> responsable de sécurité et ingénieur système / opérateur contrôleur et tout autre rôle ingénieur système et opérateur
[SEC_T_JOUR_SITE]	Durée de conservation des journaux d'évènements	1 mois
[SEC_F_JOUR_ECH]	Fréquence de contrôle des journaux d'évènements	1 fois par 24h
[SEC_F_JOUR_ANA]	Analyse complète des journaux d'évènements	1 fois par semaine et dès la détection d'une anomalie
[SEC_F_JOUR_RAP]	Fréquence de rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles	1 fois par mois
[SEC_T_REC_ARCH]	Délai de récupération des archives	2 jours ouvrés
[SEC_F_TEST_PLAN]	Fréquence de test du plan de continuité d'activité de l'IGC	2 ans
[SEC_T_CESS]	Délai de cessation d'activité d'une composante de l'IGC	1 mois
[SECT_SHAMIR]	Principe de partage de secret Shamir (n sur m)	3 sur 6
[SECT_USAGE_CLE]	Objectifs d'usage de la clé	L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature (cf. chapitre 7).
[SECT_SEQUESTRE]	Séquestre des clés privées d'AC et de certificats de porteurs	Ni les clés privées d'AC, ni les clés privées des porteurs ne doivent en aucun cas être séquestrées.
[SECT_T_PORT_MIN]	Durée de vie minimum des bi-clés des porteurs	1 an

Référence	Description	Spécificité de la présente PC
[SECT_T_PORT_MAX]	Durée maximum des bi-clés des porteurs	3 ans
[SECT_T_C_AC_MAX]	Durée de vie maximum d'un certificat d'AC	5 ans
[PP_DN_AGENT]	Type d'entité	Contient le DN (X.500) de l'application ou de l'entité représentante
[PP_KEYUSAGE]	Key Usage du certificat de porteur	nonRepudiation
[PP_KEYUSAGE_HORO]	Key Usage du certificat de porteur	digitalSignature
[PP_EXT_KEYUSAGE]	Extended Key Usage du certificat de porteur	
[PP_EXT_KEYUSAGE_HORO]	Extended Key Usage du certificat de porteur	Id-kp-timeStamping
[PP_SUBJALTNNAME]	Subject Alternative Name du certificat de porteur	Optionnel (selon les besoins spécifiques de l'application)
[AUD_F_CONFORM]	Fréquence du contrôle de conformité	1 fois tous les 2 ans
[AUT_NIV_PRIS]	Niveau de sécurité de la PRIS considéré	2 étoiles