POLITIQUE DE CERTIFICATION

AUTORITE DE CERTIFICATION CDC - LEGALIA

GABARIT AUTHENTIFICATION

OU

GABARIT SIGNATURE

Version	Date	Description	Auteurs	Société
1.0	23/11/2009	Définition des noms d'AC	Alain BOUILLE	Caisse des Dépôts
1.1	02/04/2010	Changement d'OID	Cédric CLEMENT	Caisse des Dépôts
1.2	28/05/2010	Mise à jour après les premiers déploiements	Cédric CLEMENT	Caisse des Dépôts
1.3	22/07/2010	Unification des PC authentification ou signature	Cédric CLEMENT	Caisse des Dépôts
1.4	01/12/2010	Mise à jour suite à l'audit RGS	Cédric CLEMENT	Caisse des Dépôts
1.5	30/10/2012	Mise à jour suite à l'audit externe	Vincent COUILLET	Caisse des Dépôts
1.6	15/11/2013	Précisions sur processus	Vincent COUILLET	Caisse des Dépôts
1.7	15/03/2014	Mise à jour suite à l'audit RGS	Vincent COUILLET	Caisse des Dépôts

Classification du document	Référence
Diffusion publique	OID authentification : 1.2.250.1.5.1.1.1.2.2 OID signature : 1.2.250.1.5.1.1.1.3.2

SOMMAIRE

1 INTRODUCTION

1.1 Présentation générale

La Caisse des Dépôts et Consignations (CDC) s'est positionnée comme prestataire de service de certification électronique à destination de ses collaborateurs (Groupe Caisse des Dépôts) et de ses Clients, en offrant des services supports à la confiance numérique, de manière à leur permettre généralement de sécuriser l'ensemble de leurs échanges. Les certificats des collaborateurs et des Clients de la CDC sont générés par différentes Autorités de Certification, dépendant de l'Autorité de Certification racine « CDC - RACINE ». L'ensemble constitue une hiérarchie de certification.

La présente politique de certification définit les exigences relatives à l'AC CDC - LEGALIA pour des certificats Porteurs de type Entreprise et/ou Administration ayant un profil **Authentification** (OID 1.2.250.1.5.1.1.1.2.2) ou un profil **Signature** (OID 1.2.250.1.5.1.1.1.3.2).

Ce document a été établi sur la base de la Politique de Certification type de l'Etat afin que l'Autorité de Certification CDC - LEGALIA soit en conformité avec le Référentiel Général de Sécurité (RGS).

La Déclaration des Pratiques de Certification est mise à disposition sur demande auprès de l'Autorité de Certification ou de l'Autorité d'Enregistrement.

1.2 Identification du document

Profil Authentification

Pour les certificats d'authentification, le numéro d'OID du présent document est **1.2.250.1.5.1.1.1.2.2**. Le numéro d'OID de ce document répond aux principes de nommage suivants :

- Iso(**1**)
- member-body(**2**)
- f(**250**)
- type-org(**1**)
- cdc (**5**)
- Direction des Risques et du Contrôle Interne (**1**)
- Programme de confiance numérique (**1**)
- Politiques de Certification (**1**)
- Politique de Certification CDC - LEGALIA - Authentification (**2**)
- Version (**2**)

Profil Signature

Pour les certificats de signature, le numéro d'OID du présent document est **1.2.250.1.5.1.1.1.3.2**. Le numéro d'OID de ce document répond aux principes de nommage suivants :

- Iso(**1**)
- member-body(**2**)
- f(**250**)
- type-org(**1**)
- cdc (**5**)
- Direction des Risques et du Contrôle Interne (**1**)
- Programme de confiance numérique (**1**)

- Politiques de Certification (**1**)
- Politique de Certification CDC - LEGALIA - Signature (**3**)
- Version (**2**)

La présente politique de certification s'applique aux usages [Authentification] (OID 1.2.250.1.5.1.1.1.2.2) et [Signature] (OID 1.2.250.1.5.1.1.1.3.2) sauf si spécifié.

1.3 Entités intervenant dans l'IGC

1.3.1 Autorité de certification

L'Autorité de Certification est la Caisse des Dépôts et Consignations (CDC), dûment représentée par son responsable, le Directeur Général de la CDC. Dans le cadre de cette activité, il peut, s'il le souhaite, déléguer cette fonction à une personne de son choix. Notamment, le RSSI de la CDC dispose de cette délégation. Le RSSI de la CDC est le Responsable de l'Autorité de Certification.

L'Autorité de Certification est en charge de l'application de la présente Politique de Certification. L'AC est responsable des certificats signés en son nom et de l'ensemble de l'infrastructure à clés publiques (IGC) qu'elle a mise en place.

En particulier, l'AC a la responsabilité des fonctions suivantes :

- Mise en application de la Politique de Certification,
- Enregistrement des Porteurs,
- Emission des certificats,
- Gestion des certificats,
- Information sur l'état des certificats (publication de la Liste des Certificats Révoqués (LCR) et service de réponse en ligne (OCSP)),
- Journalisation et archivage des événements et informations relatives au fonctionnement de l'IGC.

L'AC assure ces fonctions directement ou en les déléguant, ou en les sous-traitant, pour tout ou partie. Dans tous les cas, l'AC en garde la responsabilité vis-à-vis des entités externes (utilisateurs, porteurs…).

1.3.2 Autorité d'enregistrement

Une AE assure les fonctions suivantes :

- Gestion des demandes de certificats ;
- Déclenchement de la génération des certificats auprès de l'OSC ;
- Vérification de l'identité des futurs Mandataires de Certification et validation de leur nomination ;
- Vérification de l'identité des futurs Porteurs ;
- Validation des dossiers d'enregistrement ;
- Validation des demandes de révocation de certificats ;
- Participation au renouvellement des certificats ;
- Archivage des dossiers d'enregistrement ;
- Support niveau 2 pour les Porteurs.

L'Autorité d'Enregistrement (AE) gère le cycle de vie des certificats sous la responsabilité de l'AC. Elle valide les demandes des Porteurs. Elle est garante de l'identité des Porteurs à qui elle délivre des certificats.

Plusieurs AE peuvent être opérées, chacune sur un périmètre distinct en fonction des besoins liés à leur activité ou à leur métier.

Les obligations réciproques entre l'Autorité de Certification et l'Autorité d'Enregistrement sont décrites dans une « Convention AC – AE » signée par le responsable de l'Autorité de Certification et par le représentant de l'Entité en charge de l'AE.

L'organisation, les processus et les outils de chaque AE sont identiques.

Les Opérateurs d'Enregistrement peuvent différer entre chaque AE. Ils sont nommés par le Responsable d'Application.

1.3.3 Porteurs de certificats

Un Porteur de certificat (ou Abonné) est une personne physique, agissant dans le cadre de ses activités professionnelles en tant que collaborateur, client ou partenaire, qui détient un certificat de l'AC CDC - LEGALIA. Ce certificat sert pour l'authentification lors de l'accès à des ressources métier ou pour réaliser de la signature électronique dans le cadre d'usages métier.

1.3.4 Utilisateurs de certificats

Les utilisateurs de certificats sont les services d'authentification, de signature électronique et de validation de signature qui exploitent les certificats des Porteurs. Il s'agit des applications utilisatrices.

1.3.5 Autres participants

1.3.5.1 Composantes de l'IGC

Les composantes techniques permettant d'opérer les fonctions de l'IGC sont présentées dans la DPC.

1.3.5.2 Opérateur de Service de Certification (OSC)

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

Elle est techniquement responsable de :

- La génération des certificats
- La publication de la LCR
- La mise à disposition du service OCSP

1.3.5.3 Mandataire de certification

Le Mandataire de Certification est désigné par et placé sous la responsabilité du Client. 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). Il peut également être impliqué dans le processus de demande ou de révocation de certificat pour le compte des Porteurs.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats des Porteurs

Les certificats émis par l'AC CDC - LEGALIA sont utilisables exclusivement pour des opérations d'authentification ou de signature réalisées par les Utilisateurs de certificats tels que définis au paragraphe §1.3.4. Tout autre usage est effectué sous la seule responsabilité du Porteur de certificats.

L'AC CDC - LEGALIA n'émet pas de certificats pour d'autres populations et pour d'autres usages. Les certificats des autres composantes de l'Infrastructure à Gestion de Clés sont émis par d'autres autorités de certification.

Une autorité de certification spécifique délivre des certificats de test, portant la mention « TEST » au niveau de leur DN.

Les bi-clés associées aux certificats des Porteurs sont au format dit « matériel » : les bi-clés sont protégées dans un support physique. Le support physique, qualifié renforcé (gamme « MultiApp ID IAS ECC sur composant NXP »), est personnel et propre au Porteur. Il garantit la sécurité des échanges relatifs à l'utilisation de la bi-clé depuis le support physique (cf. § 6.2.1)

1.4.1.2 Bi-clés et certificats d'AC et de composantes

Le certificat de l'AC CDC - LEGALIA est émis par l'AC CDC RACINE et est utilisable exclusivement pour :

- Signer des certificats Porteurs ;
- Signer des LCRs.

1.4.2 Domaines d'utilisation interdits

Les certificats de la présente PC ne peuvent pas être utilisés en dehors d'opérations d'authentification ou de signature, effectuées dans le contexte d'applications explicitement autorisées par la CDC, ou ayant été préalablement autorisées par les représentants de l'AC. La CDC ne saurait être responsable de l'usage d'un certificat par un Porteur, sur une application non explicitement autorisée.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

La gestion de la PC est de la responsabilité de la CDC à travers la Direction du Risque et du Contrôle Interne (DRCI).

1.5.2 Point de contact

Les demandes d'information ou questions concernant l'Autorité de Certification sont à adresser au Responsable de l'application :

- Par courrier : Caisse des Dépôts - Responsable offre certificats électroniques – DRCI – 56, rue de Lille – 75356 PARIS 07 SP
- Par courriel : igc@caissedesdepots.fr

Pour contacter l'Autorité d'Enregistrement :

- Par courrier : Caisse des Dépôts – AE « CDC – LEGALIA » - DSB – 15, quai Anatole France – 75356 PARIS 07 SP
- Par courriel : ae-dbr@caissedesdepots.fr
- Par téléphone : +33 (1) 58 50 58 58

Les points de contact sont également précisés dans les formulaires constitutifs du contrat ainsi que dans les Conditions Générales de Vente.

1.5.3 Entité déterminant la conformité d'une DPC avec cette PC

La CDC est en charge des opérations internes de contrôle de conformité de la DPC à la PC.

1.5.4 Procédures d'approbation de la conformité de la DPC

L'approbation de la conformité de la DPC à la Politique de certification est prononcée par le Responsable de l'Autorité de Certification.

1.6 Définition et acronymes

1.6.1 Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CEN	Comité Européen de Normalisation
CISSI	Commission Interministérielle pour la SSI
CRL	*Certificate Revocation List*
DN	*Distinguished Name*
DPC	Déclaration des Pratiques de Certification
ETSI	*European Telecommunications Standards Institute*
HSM	*Harware Security Module*
IGC	Infrastructure de Gestion de Clés.
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
OC	Opérateur de Certification
OCSP	*Online Certificate Status Protocol*
OID	*Object Identifier*
OSC	Opérateur de Service de Certification
PC	Politique de Certification
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Electronique
RSA	Rivest Shamir Adelman
RSSI	Responsable de la Sécurité du Système d'Information
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSCD	*Secure Signature Creation Device*
URL	*Uniform Resource Locator*

1.6.2 Définitions

Agent - Personne physique agissant pour le compte d'une autorité administrative.

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 ou des besoin d'authentification ou de cachet du serveur auquel le certificat est rattaché.

Authentification - Processus permettant de vérifier l'identité déclarée d'une personne ou de tout autre entité, ou de garantir l'origine de données reçues.

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 de certification (AC) - Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ « issuer » du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre I.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

Autorité d'enregistrement - 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 adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC (cf. ci-dessous). L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du Porteur lors du renouvellement du certificat de celui-ci.

AE Déléguée – Autorité d'Enregistrement gérant les Porteurs d'un périmètre donné.

Autorité d'horodatage - Autorité responsable de la gestion d'un service d'horodatage. (cf. politique d'horodatage type [RGS_A_12]).

Bi-clé - Une bi clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques.

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 d'authentification ou de signature sauf mention explicite contraire (certificat d'AC, certificat d'une composante…).

Chaîne de confiance - Ensemble des Certificats nécessaires pour valider la généalogie d'un Certificat d'un Porteur de Certificat.
Dans une architecture horizontale simple, la chaîne se compose du Certificat de l'Autorité de Certification qui a émis le certificat et de celui du Porteur de Certificat.

Client - Personne morale qui contracte avec la CDC afin de bénéficier de ses services de certification électronique. Le Client peut mandater un ou plusieurs MC pour la gestion des certificats des Porteurs.

Comité de Pilotage de l'AC – instance de pilotage de l'Autorité de Certification. Elle comprend 5 personnes qui jouent un rôle de sécurité.

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

Conditions Générales d'Utilisation (CGU) – Récapitulatif de l'usage autorisé d'un certificat et des obligations du Porteur, conformément à la Politique de Certification de l'AC. Les CGU doivent être connues du Porteur.

« Convention AC – AE » - document définissant les obligations réciproques entre l'Autorité de Certification et une Entité opérant une AE.

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.

Dispositif d'authentification – Il s'agit du dispositif matériel et/ou logiciel utilisé par le Porteur pour stocker et mettre en œuvre sa clé privée d'authentification.

Dispositif sécurisé de création de signature électronique (SSCD) - Matériel ou logiciel, destinés à mettre en application les données de création de signature électronique, qui satisfait aux exigences définies par la règlementation

Dossier d'enregistrement – ensemble de documents permettant à l'AE de valider la demande d'enregistrement d'un futur Porteur. Le dossier d'enregistrement de l'AC CDC - LEGALIA d'un Porteur comprend le formulaire de demande signé, une photocopie du titre d'identité du futur Porteur certifiée « conforme à l'original » ainsi que les Conditions Générales d'Utilisation signées. A noter que le dossier d'enregistrement d'un Mandataire de Certification contient des pièces supplémentaires (décrites au paragraphe 3.2.3.3).

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.

Fenêtre de renouvellement – période de temps pendant laquelle un certificat peut être renouvelé. Elle démarre quelques mois avant la date d'expiration du certificat. La valeur de la fenêtre de renouvellement est définie dans la présente PC (paragraphes 4.6 et 4.7).

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

Fonction de génération des éléments secrets du Porteur - Cette fonction génère les éléments secrets à destination du Porteur, si l'AC a en charge une telle génération, et les prépare en vue de leur remise au Porteur (par exemple, personnalisation de la carte à

puce destinée au Porteur, courrier sécurisé avec le code d'activation, etc.). De tels éléments secrets peuvent être, par exemple, directement la bi-clé du Porteur, les codes (activation / déblocage) liés au dispositif de stockage de la clé privée du Porteur ou encore des codes ou clés temporaires permettant au Porteur de mener à distance le processus de génération / récupération de son certificat.

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 de publication - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux Porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses Porteurs.

Fonction de remise au Porteur - Cette fonction remet au Porteur au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif du Porteur, clé privée du Porteur, codes d'activation,…).

Fonction d'information sur l'état des certificats - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) et éventuellement également selon un mode requête / réponse temps réel (OCSP).

Formulaire de demande - Formulaire requis pour l'enregistrement d'un Porteur. Il doit être rempli et signé par le futur Porteur. Il contient des informations sur l'identité et l'organisation du Porteur.

Fournisseur de service cryptographique (ou ***CryptoServiceProvider*** **– CSP**) – Programme permettant d'utiliser les fonctions cryptographiques du support d'un certificat.

HSM (*Hardware Security Module*) - Boîtier cryptographique matériel dans lequel sont stockées les clés publiques et privées des Autorités de Certification.

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.

Liste de Certificats Révoqués (LCR) - Liste contenant les identifiants des certificats révoqués ou invalides.

Mandataire de certification - 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).

Motif de révocation – Circonstance pouvant être à l'origine de la révocation d'un certificat. Les motifs de révocation sont détaillés au paragraphe 4.9.1.

OID - Identificateur numérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.

Opérateur d'enregistrement – Représentant de l'AE ayant des fonctions à la gestion opérationnelle des certificats et notamment les actions liées à la vérification et à la saisie des informations (aussi appelé Gestionnaire d'AE).

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, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du Porteur ou d'un responsable des ressources humaines.

Politique de certification (PC) - Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les Porteurs et les utilisateurs de certificats.

Porteur de certificat - 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.

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

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

Promoteur d'application - Un responsable d'un service de la sphère publique accessible par voie électronique.

Qualification d'un prestataire de services de certification électronique - Le [DécretRGS] décrit la procédure de qualification des PSCO. Un PSCE étant un PSCO particulier, la qualification d'un PSCE est un acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC Type pour un niveau de sécurité donné et correspondant au service visé par les certificats.

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

est décrite dans le [DécretRGS]. Le [RGS] précise les trois processus de qualification : qualification de niveau élémentaire, qualification de niveau standard et qualification de niveau renforcé.

Renouvellement d'un Certificat - Opération effectuée à la demande d'un Porteur de Certificat ou en fin de période de validité d'un Certificat et qui consiste à générer un nouveau Certificat, identique en tous points au précédent, à l'exception des dates de validité, et de la clé publique.

Responsable d'Application de l'AC CDC - LEGALIA - Le Responsable d'Application est chargé 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.

Responsable de l'Autorité de Certification – Il représente physiquement l'Autorité de Certification.

Révocation d'un Certificat - Opération dont le résultat est la suppression de la caution de l'AC sur un Certificat donné, avant la fin de sa période de validité.
La demande peut être la conséquence de différents types d'événements tels que la compromission d'une bi-clé, le changement d'informations contenues dans un certificat, etc.
L'opération de révocation est considérée terminée quand le certificat mis en cause est publié dans la Liste des Certificats Révoqués. Le certificat est alors inutilisable.

Support physique (ou support cryptographique) - carte à puce ou clé cryptographique avec port USB pouvant contenir des bi-clés et des certificats.

Système d'information – Tout ensemble de moyen destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Titre d'identité - carte d'identité nationale, passeport, ou carte de séjour (pour les étrangers) servant à prouver l'identité d'un futur Porteur auprès de l'AE.

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives.

Nota - Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager.

Utilisateur de certificat - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du Porteur du certificat.

Validation de certificat - Opération de contrôle du statut d'un Certificat ou d'une chaîne de certification.

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

2.1 Entités chargées de la mise à disposition des informations

L'AC est chargée de la mise à disposition des informations devant être publiées. Opérationnellement, cette fonction est assurée sous la responsabilité du Responsable du Service de Certification.

2.2 Informations devant être publiées

Les informations publiées par l'AC CDC - LEGALIA (http://www.caissedesdepots.fr/confiance) sont les suivantes :

- La présente Politique de Certification ;
- Les Conditions Générales d'Utilisation ;
- Les formulaires nécessaires à la gestion des certificats : demande d'enregistrement, demande de révocation ;
- Le Mandat nécessaire à la nomination d'un nouveau Mandataire de Certification ;
- Les points de contacts avec l'Autorité de Certification ou l'AE.
- Les profils des certificats et LCR (voir paragraphe §7) ;
- La liste des certificats révoqués (LCR) ;
- L'URL pour la révocation des certificats en *self-service* ;
- Le certificat de l'Autorité de Certification CDC - LEGALIA ;
- L'empreinte du certificat de l'AC CDC - LEGALIA.

L'empreinte du certificat de l'AC CDC - LEGALIA est (algorithme SHA-256) :
E7 FC 14 CF ED F7 F5 3F 9D 6B AB 80 79 F5 29 E9 C7 07 4C 06 58 21 5A CA 87 17 1B E1 AA 8F 54 F4

La DPC n'est pas publiée mais consultable sur demande auprès de l'AC.

2.2.1 Publication de la Politique de Certification

La présente PC est publiée sur le site :
http://www.caissedesdepots.fr/uploads/media/pc-legalia.pdf

2.2.2 Publication du certificat d'AC

Le certificat de l'Autorité de Certification est publiée sur :

- Pour l'AC CDC - RACINE : http://www.caissedesdepots.fr/uploads/media/cdc-racine.crt
- Pour l'AC CDC - LEGALIA : http://www.caissedesdepots.fr/uploads/media/cdc-legalia.crt

2.2.3 Publication de la LCR

La liste de certificats révoqués (LCR) est publiée sur :
http://igc-crl.caissedesdepots.fr/cdc/legalia.crl

Elle est également accessible à travers un service OCSP :
http://igc-ocsp.caissedesdepots.fr/ocsp-legalia/

Ces URL sont également indiquées dans les certificats des Porteurs.

Enfin, elle est également publiée au travers d'un service LDAP :
ldap://igc-ldap.caissedesdepots.fr/cn=CDC%20-%20LEGALIA,ou=0002%20180020026,o=CAISSE%20DES%20DEPOTS,c=FR

2.3 Délais et fréquences de publication

2.3.1 Fréquence de publication de la Politique de Certification

La Politique de Certification est revue a minima tous les deux ans, et mise à jour si nécessaire conformément aux dispositions décrites en section §9.12.1. La Politique de Certification est publiée dès sa validation, dans un délai maximal de 24 heures.

2.3.2 Fréquence de publication du certificat d'AC

Le certificat d'AC est diffusé dans un délai maximum de 24 heures à l'issue de sa génération.

2.3.3 Fréquence de publication de la LCR

La publication des LCR est effectuée toutes les heures. Le statut des certificats est accessible via la LCR et via un service OCSP.

2.3.4 Disponibilité des informations publiées

Les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.) sont publiées dès que nécessaires afin que soit assurée à tout moment la cohérence avec les engagements, moyens et procédures effectifs de l'AC.

Le service de certification électronique et toutes les composantes de l'AC sont accessibles 24h/24 et 7j/7.

Le taux de disponibilité du service (dont émission, révocation du certificat) est de 99% base mensuelle, et une indisponibilité continue du service (incident de gravité 1) ne pourra pas être supérieure à 6 heures en heures ouvrées d'exploitation et 8 heures en heures non ouvrées.

2.4 Contrôle d'accès aux informations publiées

Les informations publiées sont mises à disposition en lecture à l'ensemble de la communauté des Utilisateurs. Les PC, certificats d'AC et LCR sont mis à disposition en lecture de manière internationale.

Les ajouts, suppressions et modifications sont limités aux personnes autorisées de l'AC. L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Les noms utilisés sont 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 la section 7 décrivant le profil des certificats. Le nom distinctif est sous la forme d'une chaîne de type « *UTF8 string* » de type « nom X.501 ».

3.1.2 Nécessité d'utilisation de noms explicites

Les noms pour distinguer les Porteurs sont explicites et contiennent les informations nécessaires permettant d'identifier les Porteurs, présents dans le champ « *Subject - DN* » du certificat, comme les informations nom, prénom et organisation du Porteur. Ces informations sont recueillies par le Mandataire de Certification lors de la phase de vérification de l'identité du Porteur.

Le nom (champ CN) est celui du Porteur tel qu'il figure dans les documents d'identité. Les informations portées dans le champ « *Subject DN* » du certificat sont décrites ci-dessous de manière explicite :

- Champ C (*CountryName*) : le pays dans lequel est enregistrée l'organisation du Porteur ;
- Champ O (*OrganizationName*) : la raison sociale de l'organisation représentée par le Porteur, tel que figurant au K-Bis ;
- Champ OU (*Organization Unit*) : le numéro de SIREN ou de SIRET de l'organisation représentée par le Porteur ;
- Champ CN (Common Name) : le nom du Porteur sous la forme Prénom NOM (éventuellement le second prénom peut être ajouté s'il apparaît sur les documents d'identité, en cas d'homonymie un numéro d'ordre sera ajouté à la suite d'un espace après le NOM du Porteur).

3.1.3 Pseudonymisation des Porteurs

L'identité utilisée pour les certificats de porteurs n'est ni un pseudonyme ni un nom anonyme.

3.1.4 Règles d'interprétation des différentes formes de noms

Les noms utilisés pour les Porteurs sont suffisamment explicites, et ne nécessitent pas d'interprétation particulière.

Tous les caractères sont au format *UTF-8*, i.e. sans accents ni caractères spécifiques à la langue française et de manière conforme au standard X.501. Pour les prénoms et noms composés, le tiret est utilisé comme élément séparateur.

Exemple :

DN = {C=FR, O=CAISSE DES DEPOTS, OU=0002 180020026, CN=Jean-Michel DUPONT}

3.1.5 Unicité des noms

L'AE résoudra les problèmes d'homonymie éventuelle, et garantit l'unicité des noms utilisés pour les certificats des Porteurs. La clé d'unicité d'un certificat au sein de l'AC CDC - LEGALIA est le *CommonName* (CN) du Porteur : Prénom NOM (voir paragraphe § 3.1.2)

Le champ DN, contenant le numéro de SIREN/SIRET de l'organisation de rattachement, garantit la clé d'unicité dans le cas où des Porteurs de structures différentes auraient le même CN.

En cas d'homonymie sur le couple « Prénom NOM », au sein d'une même organisation, l'AE inscrira également le deuxième prénom du Porteur au sein de l'attribut *CommonName* (CN) du certificat, éventuellement le troisième prénom s'il existe, enfin, si l'homonymie persiste, un numéro d'ordre composé de trois caractères numériques sera ajouté à la suite d'un caractère « espace » après le NOM

Les prénoms présentés doivent l'être dans le même ordre que sur la pièce d'identité et séparés par une virgule sans espace ni avant ni après la virgule, suivi d'un espace, suivi du nom de l'état civil du porteur.

Exemple :
DN = {C=FR, O=CAISSE DES DEPOTS, OU=0002 180020026, CN=Michel,Paul DUPONT 001}

3.1.6 Identification, authentification et rôle des marques déposées

L'AE s'assurera avec un soin raisonnable du droit d'usage des noms et marques déposés par le demandeur.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

L'AC s'assure de la détention de la clé privée par le Porteur de certificat avant de certifier la clé publique. En effet, lors du processus de demande de certificat, le Porteur génère sa bi-clé au sein de son support physique, et fournit à l'AC une preuve de possession de sa clé privée (demande PKCS#10) correspondant à la clé publique contenue dans sa demande de certificat.

3.2.2 Validation de l'identité d'un organisme

Cf. chapitre §3.2.3.

3.2.3 Validation de l'identité d'un individu

3.2.3.1 Enregistrement d'un Porteur [PARTICULIER]

Sans objet.

3.2.3.2 Enregistrement d'un Porteur [ENTREPRISE] / [ADMINISTRATION] sans MC

L'enregistrement d'un Porteur passe par les étapes suivantes :

- Fourniture des **documents d'enregistrement** dûment complétés dont :
  - Formulaire de demande co-signé par le Porteur et le Représentant Légal

  - Photocopie certifiée conforme d'un titre d'identité (Carte Nationale d'Identité, Passeport…)
- Signature des **Conditions Générales d'Utilisation**.
- **Validation de l'identité** du Porteur par l'AE en face-à-face sur la base de la pièce d'identité fournie lors de la demande.
- **Archivage** de l'ensemble des pièces du dossier d'enregistrement.

Les documents relatifs à l'identification de l'organisme sont identiques à ceux demandés au paragraphe § 3.2.3.3.

3.2.3.3 Enregistrement d'un Mandataire de Certification

L'enregistrement d'un Mandataire de Certification passe par les étapes suivantes :

- **Signature d'un Mandat** et fourniture de documents complémentaires **par le Représentant Légal.**
- **Signature des Conditions Générales d'Utilisation** ainsi que du Mandat par le futur Mandataire de Certification.
- **Validation de l'identité** du Mandataire de Certification par l'AE en face-à-face sur la base de la pièce d'identité fournie lors de la demande.
- **Archivage** de l'ensemble des pièces du dossier d'enregistrement.

Le futur MC télécharge au niveau du site institutionnel de la Caisse des Dépôts les documents suivants :

- Mandat du MC
- Conditions Générales d'Utilisation (CGU).

Le futur MC remplit ces documents et les signe. Le futur MC se déplace auprès du Représentant Légal afin de lui faire signer le Mandat. Le Représentant Légal doit retourner le Mandat signé au futur MC ainsi que deux documents complémentaires :

- Attestation d'identification unique de l'entreprise (extrait K-bis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers).
- Attestation de Représentant Légal.

L'ensemble des documents cités constitue le dossier d'enregistrement.

Le futur MC se déplace auprès de l'AE, muni du dossier d'enregistrement, et rencontre en face-à-face un Opérateur d'Enregistrement.

L'Opérateur d'Enregistrement valide le dossier d'enregistrement. Pour cela, il vérifie :

- La complétude du Dossier d'Enregistrement :
  - Mandat du Mandataire de Certification. Le mandat désigne le Mandataire de Certification. Il doit être co-signé par le Représentant Légal et le Mandataire de Certification. Il doit être daté de moins de 3 mois.
  - Conditions Générales d'Utilisation signées par le MC.
  - Attestation d'identification unique de l'entreprise.
  - Attestation de Représentant Légal.
- La signature du Représentant Légal et du futur Mandataire de Certification sur le mandat.

L'Opérateur d'Enregistrement photocopie un titre d'identité du Mandataire de Certification. L'Opérateur d'Enregistrement et le Mandataire de Certification signent cette photocopie en ajoutant la mention « Certifiée conforme à l'original ». Cette photocopie vient s'ajouter au dossier d'enregistrement.

L'Opérateur d'Enregistrement archive le dossier d'enregistrement.

3.2.3.4 Enregistrement d'un Porteur [ENTREPRISE] / [ADMINISTRATION] via un MC

L'enregistrement d'un Porteur passe par les étapes suivantes :

- **Demande.**
- **Validation de l'identité du Porteur**.

Ces deux étapes sont l'objet du présent paragraphe.

- Validation de la demande.

Les modalités de validation de l'identité des Porteurs sont définies pour chacun des Clients, dans la « Convention AC – AE ». Le Client, via le Mandataire de Certification, s'engage sur la fiabilité de l'identité communiquée par le Porteur à l'AE lors de l'enregistrement.

Dans tous les cas, la demande et la validation de l'identité du Porteur se déroulent de la manière décrite ci-après. Le futur Porteur se déplace auprès du Mandataire de Certification pour faire sa demande de certificat. Le Mandataire de Certification procède à la vérification de l'identité du Porteur en face-à-face. Pour cela le Porteur présente un titre d'identité. Le Mandataire de Certification photocopie le titre d'identité du Porteur, et y ajoute la mention « Certifié conforme à l'original ». Le Mandataire de Certification et le Porteur signent cette photocopie. Le Mandataire de Certification fait remplir le formulaire de demande par le Porteur. Le Porteur signe le formulaire. Le Porteur signe les Conditions Générales d'Utilisation.

L'ensemble de ces documents constitue le dossier d'enregistrement du Porteur :

- Formulaire de demande signé par le Porteur et le Mandataire de Certification
- Conditions Générales d'Utilisation signées par le Porteur.
- Photocopie d'un titre d'identité signée par le Mandataire de Certification et le Porteur.

Le Mandataire de Certification envoie le dossier d'enregistrement à l'AE.

3.2.4 Informations non vérifiées du Porteur

Sans objet.

3.2.5 Validation de l'autorité du demandeur

Pour l'AC CDC - LEGALIA, le demandeur est toujours le futur Porteur.

L'AE, et par délégation le Mandataire de Certification, s'assurent que le demandeur dispose des pouvoirs nécessaires pour effectuer cette demande. Cette vérification est effectuée sur la base des informations fournies dans la demande de certificat, et selon des règles spécifiques au Métier, que l'AE fera valider par les responsables de l'Autorité de Certification, avant mise en application.

3.2.6 Certification croisée d'AC

L'AC n'a aucun accord de reconnaissance avec une AC extérieure au domaine de sécurité auquel elle appartient. Néanmoins l'AC pourra reconnaître, moyennant la signature d'un accord de reconnaissance, toutes les autres AC externes qui disposeront du statut référencé « RGS »à un niveau équivalent ou supérieur à celui de CDC – LEGALIA, pour des usages d'authentification et de signature.

Dans ce cas là, si une autre AC formule une demande d'accord, ou si les responsables de l'AC CDC - LEGALIA émettent le besoin de mettre en place un accord de reconnaissance avec une autre AC, le comité de pilotage de l'AC diligentera une série d'investigations (audits / analyse de risques) pour déterminer si l'AC à reconnaître émet bien des

certificats de même qualité, avec le même niveau de sécurité, que ceux de la présente AC CDC - LEGALIA.

Notamment, la CDC pourra attendre des AC demandant un accord de reconnaissance de respecter les formats des certificats suivant les normes :

- IETF RFC 5280 ;
- IETF RFC 3739 et ETSI - TS 101 862 dans le cadre de certificats qualifiés.

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

Un nouveau certificat ne peut pas être fourni au Porteur sans renouvellement de la bi-clé correspondante.

3.3.1 Identification et validation pour un renouvellement courant

Le Porteur est averti de l'arrivée à expiration de son certificat par courriel 90, 30 et 15 jours avant l'expiration. Ces notifications sont envoyées en copie à l'AE.

3.3.1.1 Cas du premier renouvellement

L'AE se base sur le dossier d'enregistrement fourni lors de la première demande et archivé pour l'identification et la validation de la demande de renouvellement. Le Porteur doit répondre à une notification de l'AE pour valider le renouvellement. Il recevra ensuite une URL de retrait et un code de retrait dans deux mails séparés, pour procéder au renouvellement.

3.3.1.2 Cas du second renouvellement

Lors du second renouvellement, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial (voir paragraphe §3.2).

3.3.2 Identification et validation pour un renouvellement après révocation

Suite à la révocation d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initial (voir paragraphe §3.2).

3.4 Identification et validation d'une demande de révocation

La demande de révocation de certificat CDC - LEGALIA peut être effectuée par les acteurs ci-dessous :

- Le Porteur ou un Mandataire de Certification de l'entité de rattachement du Porteur;
- L'Autorité d'Enregistrement de l'AC CDC - LEGALIA ;
- Un Représentant Légal de l'entité du Porteur;
- Le Responsable de l'AC CDC - LEGALIA.

Toute personne à l'origine d'une demande de révocation est authentifiée.

- Le Porteur est authentifié à l'aide de son code de révocation choisi au moment de la demande de certificat.
- Le Mandataire de Certification est authentifié sur la base d'une signature manuscrite par comparaison avec la signature présente dans son dossier d'enregistrement.

- L'Opérateur d'Enregistrement est authentifié à l'aide de son certificat de l'AC CDC - FIDELIA.
- Le Représentant Légal est authentifié sur la base d'une signature manuscrite à l'aide d'un carton de signature.
- Le Responsable de l'AC est authentifié par l'AE (face-à-face, signature manuscrite, mail signé).
- Toute demande traitée par téléphone est authentifiée sur la base des informations contenues dans la photocopie de la pièce d'identité du demandeur.

Remarque 1 : le Porteur est identifié par la personne à l'origine de la demande à l'aide des informations suivantes :

- Si le Porteur est à l'origine de la demande : l'identifiant utilisé peut être l'adresse email ou le contenu du champ CN du Porteur.
- Sinon : le Porteur doit être identifié à l'aide de ses nom, prénom et adresse e-mail.

Remarque 2 : le demandeur, quand il s'agit du Mandataire de Certification ou du Représentant Légal doit être identifié à l'aide des informations suivantes :

- Nom, prénom, nom de la société d'appartenance et numéro de téléphone professionnel.

3.5 Identification et validation d'une demande de déblocage du support cryptographique

Après 3 saisies consécutives erronées du code PIN, le support cryptographique se bloque par mesure de sécurité.

Le déblocage n'est alors possible que par un responsable de sécurité, qui n'effectuera ce déblocage qu'en présence du Porteur. Celui-ci saisira un nouveau code PIN afin que la non-utilisation du certificat par un tiers soit garantie.

Si cette condition ne peut être remplie, le certificat du Porteur stocké sur le support bloqué est révoqué et une nouvelle demande de certificat est effectuée sur demande du Mandataire ou du Porteur.
Le Mandataire est tenu informé de l'ensemble des opérations et remet au Porteur un support cryptographique vierge à personnaliser.

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 Mandataire de Certification, dûment mandaté pour cette entité, dans le cas d'un consentement préalable du futur Porteur.
- par un Porteur directement, avec le consentement de son entité (Représentant Légal)

Cette demande doit avoir fait l'objet d'une vérification et d'une validation par l'AE, préalablement à la délivrance du certificat électronique.

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

Les deux étapes de demande et de validation de l'identité du Porteur, objet du paragraphe §3.2.3.4, sont précisées dans ce paragraphe.
La validation de la demande est décrite au paragraphe §4.2.1.

Comme vu au paragraphe §3.2.3.4, la demande de certificat doit s'appuyer sur un dossier d'enregistrement, intégrant notamment un formulaire de demande comportant les informations suivantes :

- La référence du contrat entre l'AC et le Client dont le Porteur fait partie.
- Les coordonnées du futur Porteur :
  - Nom, prénom ;
  - Adresse électronique professionnelle ;
  - Adresse postale.
- Le code de révocation, choisi par le Porteur, et qu'il aura à utiliser en cas de perte ou de compromission de son support physique. Le Porteur devra respecter la politique des mots de passe qui est explicitée dans le formulaire de demande ;
- La date et la signature (papier) du Porteur.

Le dossier d'enregistrement doit être transmis à l'AE pour validation.
Il peut être au format papier ou au format électronique. Le format électronique pourra résulter d'un scan des documents papier préalablement signés.

4.2 Traitement d'une demande de certificat

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

L'enregistrement d'un Porteur passe par les étapes suivantes :

- Demande.
- Validation de l'identité du Porteur.
  Ces deux étapes sont l'objet des paragraphes §3.2.3.4 et §4.1.2.
- **Validation de la demande** : cette étape est l'objet du présent paragraphe.

Pré-requis : l'Autorité d'Enregistrement a reçu le dossier d'enregistrement.

Au sein de cette AE, un Opérateur de saisie prend en charge la demande et saisit les informations du Porteur au niveau des interfaces de l'OSC en se basant sur les

informations écrites dans le formulaire de demande. Cela déclenche l'envoi d'une notification à l'ensemble des Opérateurs de l'AE informant qu'une nouvelle demande doit être validée.

Un Opérateur de validation procède à la validation de la demande, en vérifiant :

- La cohérence de la demande avec le mandat du Mandataire de Certification (vérification de la signature manuscrite du MC).
- La complétude du Dossier d'Enregistrement
- La cohérence entre les informations saisies dans le formulaire de demande et le Dossier d'Enregistrement.
- **Remarque** : les documents du dossier d'enregistrement doivent dater de moins de 3 mois.

Si ces points sont vérifiés, l'Opérateur de validation valide la demande au niveau des interfaces de l'OSC.

- Sinon, l'Opérateur d'Enregistrement signale que le Dossier d'Enregistrement n'est pas valide. Cela déclenche l'envoi d'un mail à la boîte mail générique de l'AE, qui signale cette non-conformité au MC. Un nouveau déplacement du Porteur est nécessaire.

La validation de la demande déclenche au niveau de l'IGC :

- L'envoi d'une notification à l'AE informant de la validation de la demande.
- L'envoi d'une notification au Porteur contenant l'URL de retrait personnalisée.
- L'envoi d'une notification au Porteur contenant le code de retrait.
- L'envoi d'une notification au Porteur contenant le code de révocation.

L'Opérateur d'Enregistrement fait parvenir au futur Porteur par courrier le support physique.

- N.B 1 : le support physique est associé à un code PIN par défaut. Ce code PIN initial devra être changé par le Porteur avant le retrait.
- N.B 2 : concernant les courriers :
    - Ils peuvent être envoyés dans un lot de courriers similaires au Mandataire de Certification. C'est le Mandataire de Certification qui les remet aux Porteurs.
    - OU ils sont envoyés directement au Porteur à l'adresse qu'il a renseignée dans le formulaire de demande.

Dans ces conditions, le Porteur va pouvoir procéder au retrait de son certificat, en *self-service* (à la condition supplémentaire que les pré-requis techniques soient vérifiés sur son poste de travail).

L'AE est en charge d'établir le suivi des demandes et des affectations de certificats. Ce suivi doit permettre :

- De connaître les Porteurs rattachés à un mandataire ;
- Le statut des demandes en cours ;
- Le statut des certificats délivrés.

L'AE réalise ce suivi en conservant les supports papiers qui lui ont été transmis par les mandataires et en maintenant un document de suivi des demandes partagé par l'ensemble des Opérateurs d'Enregistrement.

4.2.2 Acceptation ou rejet de la demande

La demande est validée par un Opérateur d'Enregistrement au niveau des interfaces techniques de l'OSC : la demande peut être acceptée ou rejetée. En cas de rejet, l'AE en informe le Porteur et le Mandataire de Certification, en justifiant le rejet.

4.2.3 Durée d'établissement du certificat

A l'issue de la validation de la demande par l'AE, la durée d'établissement du certificat dépend essentiellement du Porteur qui est à l'origine de la récupération de ce certificat.
La durée des opérations successives du processus de génération du certificat par le Porteur (voir § 4.3.1) est de l'ordre de la minute.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

La délivrance du certificat par l'AC au Porteur est réalisée en *self-service* par le Porteur.

Remarque : s'il a reçu un nouveau support physique, le Porteur doit changer son code PIN. Le retrait de certificat ne peut pas être réalisé avec un code PIN initial.

Une fois que le Porteur a reçu les notifications de retrait (3 mails mail contenant l'URL de retrait, le code de retrait et le code de révocation) et son support physique (le cas échéant), il procède lui-même au retrait du certificat, qui comprend les étapes suivantes :

- Le Porteur accède à l'URL de retrait.
- Le Porteur change le code PIN de son support physique (en respectant la politique de mot de passe) liée à ce support physique.
- Le Porteur saisit son code de retrait.
- Le Porteur saisit son nouveau code PIN pour déclencher la personnalisation électrique du certificat.
- La personnalisation électrique se déroule de la manière suivante :
  - Génération des clés du Porteur sur son support physique ;
  - Création d'un fichier au format PKCS#10 de la demande de certificat ;
  - Transmission sécurisé de la demande de certificat à l'AC ;
- L'AC signe le certificat et le remet au Porteur : le certificat est généré et automatiquement installé sur le support physique.
  N.B : le certificat est également installé dans le navigateur du Porteur de façon synchrone.
- Suite à la génération du certificat, l'Autorité de Certification envoie une notification de confirmation à l'AE et au Porteur.

Une durée limitée, définie à 2 mois, permet de contrôler le temps octroyé au Porteur pour le retrait. Si le demandeur dépasse ce délai de 2 mois, il doit refaire une demande, en suivant la même procédure que pour la demande initiale.

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

Après délivrance du certificat, une notification est envoyée au Porteur (et à l'AE en copie).

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

L'acceptation du certificat par le Porteur est tacite 7 jours après l'installation de son certificat sur son support cryptographique (clé USB ou carte à puce). Dans le cas d'une réclamation faite par le Porteur, le certificat est révoqué par l'AE et le Porteur est invité à faire une nouvelle demande de délivrance d'un certificat.

4.4.2 Publication du certificat

Les certificats ne sont pas publiés après leur délivrance.

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

L'AC prévient l'AE de la délivrance d'un certificat à un Porteur en envoyant une notification par mail. L'AE peut également être informée de la délivrance du certificat en consultant la liste des certificats créés via les interfaces techniques de l'OSC.

4.5 Usage de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le Porteur

Le Porteur s'engage, en signant le formulaire de demande et les Conditions Générales d'Utilisation à n'utiliser son certificat qu'a des fins d'authentification ou de signature sur les applications cibles définies en §1.4.1. Toute autre utilisation est interdite, et engage la responsabilité personnelle du Porteur de certificat. Cet usage est indiqué explicitement dans les extensions des certificats (cf. chapitre §7).

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

Cf. chapitre précédent et chapitre §I.4 : les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats.

4.6 Renouvellement d'un certificat

Pour l'AC CDC - LEGALIA, la notion de renouvellement de certificat, au sens RFC 3647, correspondant à la seule modification des dates de validité, n'est pas retenue. Seule la délivrance d'un nouveau certificat suite à changement de la bi-clé est autorisée.

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 de bi-clé

Les bi-clés émises pour les certificats des Porteurs, par l'AC CDC - LEGALIA, ont une durée de vie de 3 ans. La délivrance d'un nouveau certificat avant la fin de vie ne peut être que la conséquence d'une révocation, ou d'une demande de renouvellement. La fenêtre de renouvellement est de 3 mois avant la date d'expiration du certificat.

4.7.2 Origine d'une demande d'un nouveau certificat

Si la demande de nouveau certificat fait suite à une révocation, l'origine de la demande est le Porteur, l'Autorité d'Enregistrement ou le Mandataire de Certification.

Si la demande de nouveau certificat se fait dans le cadre d'une demande de renouvellement du certificat, l'origine de la demande est le Porteur.

Le Porteur reçoit des notifications d'arrivée à expiration de son certificat en provenance de l'AE à partir du début de la fenêtre de renouvellement. Le Porteur reçoit trois notifications. Le Porteur doit confirmer à l'AE sa demande de renouvellement par retour de mail. S'il passe le délai d'expiration du certificat, il devra faire une nouvelle demande (voir le paragraphe §4.1).

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

La procédure de traitement d'une demande de nouveau certificat est identique à la procédure de demande initiale (voir le paragraphe §4.2) dans les cas suivants :

- La demande de nouveau certificat fait suite à une révocation.
- Il s'agit d'un second renouvellement.

Dans le cas d'un premier renouvellement, la procédure de traitement d'une demande de nouveau certificat est la suivante :

- Suite à la réception d'une notification d'expiration et d'un mail de confirmation du Porteur, un Opérateur d'Enregistrement prend en compte la demande.
- **Remarque** : le Porteur précise s'il souhaite changer ou non de support physique. Il est recommandé de changer de support physique lors du 2ème renouvellement.

- L'Opérateur d'enregistrement (rôle d'opérateur de saisie) va réaliser une demande de renouvellement au niveau des interfaces techniques de l'OSC.
- Un Opérateur de validation valide la demande.
- La validation de la demande déclenche :
  - L'envoi d'une notification à l'AE informant de la validation de la demande.
  - L'envoi d'une notification au Porteur contenant l'URL de retrait.
  - L'envoi d'une notification au Porteur contenant le code de retrait.
  - L'envoi d'une notification au Porteur contenant le code de révocation.
- Le Porteur retire son certificat tel que décrit au paragraphe 4.3.

Remarque : le processus de premier renouvellement ne requiert pas l'étape de validation de l'identité du Porteur.

En cas de modifications apportées au corpus documentaire entre la délivrance du premier certificat et celui lié au renouvellement, le Porteur en est informé et pourra les consulter sur le site dédié cité au §2.2.

4.7.4 Notification au Porteur de l'établissement du nouveau certificat

Identique à la demande (paragraphe §4.3.2).

4.7.5 Démarche d'acceptation du nouveau certificat

Identique à la demande (paragraphe §4.4.1).

4.7.6 Publication du nouveau certificat

Identique à la demande (paragraphe §4.4.2).

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

Identique à la demande (paragraphe §4.4.3).

4.8 Modification du certificat

Les modifications de certificats Porteur et de certificats d'AC ne sont pas autorisées.

4.8.1 Causes possibles de modification d'un certificat

Sans objet.

4.8.2 Origine d'une demande de modification de certificat

Sans objet.

4.8.3 Procédure de traitement d'une demande de modification de 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 suite à une mobilité) ;
- le Porteur ou son organisation d'appartenance n'a pas respecté ses obligations découlant de la présente PC et rappelée dans les Conditions Générales d'Utilisation ;
- 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 code PIN du support physique du Porteur est suspecté de compromission, est compromis ou est définitivement oublié ;
- le Porteur, le Représentant légal de l'entité, l'Autorité de Certification ou l'Autorité d'Enregistrement demandent la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du Porteur et/ou de son support physique) ;
- le décès du Porteur ou la cessation d'activité de l'entité du Porteur ;
- la résiliation ou le terme normal du Contrat Relatif aux Services de certification électronique ;
- une rupture technologique nécessitant de procéder à la génération de nouvelles bi-clés (longueurs des clés trop faibles, algorithmes de hashage compromis).
- La révocation d'un certificat d'AC de la chaîne de confiance.

Lorsque l'une des circonstances ci-dessus se réalise et que l'AC en a eu connaissance, le certificat concerné est révoqué et le numéro de série placé dans la nouvelle Liste de Certificats Révoqués (LCR).

4.9.1.2 Certificats d'une composante de l'IGC

Les circonstances suivantes déclenchent la révocation du certificat d'une composante de l'IGC (notamment le certificat de l'AC servant à la signature des certificats Porteurs et des LCRs) :

- 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 elle 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 ;
- L'Autorité d'Enregistrement de l'AC CDC - LEGALIA;
- Un Représentant Légal de l'entité du Porteur;
- Le Mandataire de Certification du Porteur concerné.
- Le Responsable de l'AC CDC - LEGALIA.

Le Porteur est informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat, lors de son enregistrement.

4.9.2.2 Certificats d'une composante de l'IGC

La révocation du certificat de l'AC CDC - LEGALIA ne peut être décidée que par le responsable de l'AC ou par des autorités judiciaires via une décision de justice.

La révocation des certificats des autres composantes est décidée par l'entité opérant la composante (l'AE ou l'OSC) 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 demandes de révocation émanant des Porteurs peuvent être réalisées :

- En ligne via une interface mise à disposition par l'Opérateur de Service de Certification. L'URL de connexion pour les Porteurs est :
  - [Authentification]: https://igc-rev.caissedesdepots.fr/GroupeCDC/CDC/LEGALIA-AUTH:I
  - [Signature] : https://igc-rev.caissedesdepots.fr/GroupeCDC/CDC/LEGALIA-SIGN:I
- Par courrier à l'aide d'un formulaire à l'intention de l'AE concernée.
- Par téléphone ou par courrier électronique avec échange d'un secret partagé (code de révocation du Porteur).

Les demandes de révocation émanant du Mandataire de Certification, du Représentant Légal du Porteur ou du Responsable de l'AC sont traitées par l'AE. Elles doivent être réalisées par courrier à l'aide d'un formulaire à l'intention de l'AE concernée.

Les informations pratiques permettant de réaliser cette révocation quel que soit le canal (en ligne, par téléphone, ou par email) sont disponibles sur le site institutionnel de la Caisse des dépôts à l'URL suivante : http://www.caissedesdepots.fr/confiance.html

Le processus de révocation en *self-service* par le Porteur est le suivant :

- Le Porteur se connecte à l'URL de révocation. Celle-ci figure dans une notification reçue par le Porteur après validation de la demande de certificat. Cette notification contient également le code de révocation qui a été choisi par le Porteur dans le formulaire de demande.
- Le Porteur saisit son code de révocation.

- Le Porteur sélectionne le certificat à révoquer, ainsi qu'un motif de révocation.
- Cela déclenche la révocation par l'AC. Le numéro de série du certificat révoqué apparaîtra dans la prochaine CRL publiée.
- Le Porteur et l'AE reçoivent une notification de la révocation.
- L'opération est enregistrée dans les journaux d'évènements.

Le processus de révocation par l'AE est le suivant :

- Un Opérateur d'Enregistrement se connecte aux interfaces de l'OSC. Il s'authentifie à l'aide de son certificat.
- Il recherche le Porteur à l'aide de son adresse email.
- L'Opérateur d'Enregistrement sélectionne le certificat à révoquer ainsi qu'un motif de révocation et envoie la demande de révocation.
- Cela déclenche la révocation par l'AC. Le numéro de série du certificat révoqué apparaîtra dans la prochaine CRL publiée.
- Le Porteur et l'AE reçoivent une notification de la révocation.
- L'opération est enregistrée dans les journaux d'évènements.
- L'opération est prise en compte aux heures et jours ouvrés uniquement.

Le processus de révocation à l'origine du Mandataire de Certification, du Représentant légal, du Responsable d'AC ou du Porteur (identifiés dans le paragraphe ci-dessous comme des demandeurs) est le suivant :

- Le demandeur se connecte au site de publication de l'Autorité de Certification : http://www.caissedesdepots.fr/confiance.html
- Le demandeur télécharge un formulaire de révocation.
- Le demandeur imprime le formulaire, le complète et le signe.
  - N.B : le Porteur est identifié par son adresse email.
- Le Représentant légal, le Mandataire de Certification, le Responsable d'AC ou le Porteur transmet le formulaire à l'AE.
- L'AE prend en charge la demande. L'Opérateur d'Enregistrement valide la signature du demandeur : Représentant Légal, Mandataire de Certification, Responsable d'AC, Porteur.
- Si la demande provient d'un demandeur autorisé (cf. liste ci-dessus), l'Opérateur d'Enregistrement suit le « processus de révocation par l'AE » présenté ci-dessus.
- L'opération est prise en compte aux heures et jours ouvrés uniquement.

Remarque : le Porteur suit ce processus dans le cas où la fonction de révocation en self-service est indisponible.

Remarque : les causes de révocation définitive des certificats ne sont pas publiées dans la LCR.

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

Les demandes de révocation d'une des composantes de l'AC sont à effectuer auprès du Responsable de l'Autorité de Certification, qui effectuera les vérifications d'usage, pour qualifier cette demande.

4.9.3.2.1 Cas de l'AC

En cas de demande de révocation du certificat de l'AC, elle informera dans les plus brefs délais les AE. Ces AE informeront à leur tour dans les plus brefs délais l'ensemble des Mandataires de Certification et Porteurs concernés, que les certificats d'AC émis pour leur compte ne sont plus valides. 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. Parallèlement aux AE, l'AC devra informer l'OSC de la révocation du certificat de l'AC.

4.9.3.2.2 Cas de l'AE

En cas de révocation d'un certificat d'un des Opérateurs d'Enregistrement de l'AC CDC - LEGALIA, le Responsable d'AE s'assurera qu'il reste toujours suffisamment d'Opérateurs d'Enregistrement pour assurer la continuité de service de l'AC.

4.9.3.2.3 Cas de l'OSC

En cas de révocation d'un certificat d'un des services de l'OSC, ce dernier devra en informer l'AC au plus tôt et détailler les impacts liés à cette révocation pour l'AC.

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

L'AC met tout en œuvre pour que le délai maximum de traitement soit le plus court possible, entre la demande de révocation et sa réalisation effective.

Opérationnellement, la fonction de gestion des révocations en ligne est disponible 24h/24 et 7j/7. Le Porteur peut accéder lui-même à ce service pour procéder à la révocation de son certificat. Dans ce cas, la révocation est immédiate. Le numéro de série du certificat révoqué apparaîtra dans la LCR suivante.

Pour les autres modes de révocation, le traitement des demandes de révocation est réalisé pendant les jours et heures ouvrés par les personnels de l'AE. Ce schéma est convenu dans le cas où les utilisateurs de certificats ne sont opérationnels que pendant les heures et jours ouvrés.

De manière générale, le service de certification électronique de Keynectis est accessible 24h/24 et 7j/7. Le taux de disponibilité du service (dont le système de révocation d'un certificat) affiche une indisponibilité inférieure à 4h par mois), et une indisponibilité continue du service (incident de gravité 1) ne pourra pas être supérieure à 1 heure en heures ouvrées et non ouvrées d'exploitation.

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

En cas de révocation d'un certificat d'AC, cette dernière en informe l'OSC qui révoque immédiatement le certificat. Cette révocation est alors effective dès lors que le numéro de série du certificat apparaît dans la LCR.

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

Les Utilisateurs des certificats délivrés par l'AC CDC - LEGALIA (tels que définis au paragraphe 1.3.4) doivent vérifier l'état du certificat de l'Autorité de Certification, et des certificats constituant la chaîne de certification. La méthode utilisée dépend du Porteur et des contraintes liées aux applications utilisatrices.

Par défaut, la liste des certificats révoqués est mise à disposition sous la forme d'un fichier « CRL ». L'URL de publication des CRL figure dans le champ CRLDP du certificat.

Un service de vérification en ligne de l'état des certificats est également disponible à l'adresse : http://igc-ocsp.caissedesdepots.fr/ocsp-legalia/.

4.9.7 Fréquence d'établissement des LCR

Les LCR sont établies et publiées sur Internet toutes les heures. L'information de l'état de révocation d'un certificat est également disponible au travers du service OCSP.

4.9.8 Délai maximum de publication d'une LCR

Les LCR sont rendues publiques et visibles de manière internationale dans un délai maximal d'une heure. La durée entre la fin de génération de la LCR et sa publication n'est pas supérieure à 30 minutes.

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

L'AC CDC - LEGALIA utilise un service de vérification en ligne de l'état des certificats (OCSP). Ce service permet de vérifier un certificat en temps réel à chaque utilisation du certificat, le service se base cependant sur une LCR horaire. Ce service est accessible 24h/24 et 7j/7. Le taux de disponibilité du service est de 99% base mensuelle (indisponibilité inférieure à 8h par mois), et une indisponibilité continue du service (incident de gravité 1) ne pourra pas être supérieure à 2 heures en heures ouvrées et non ouvrées d'exploitation.

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

Cf. §4.9.6.

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.

En cas de révocation d'un certificat d'un des Opérateurs d'Enregistrement de l'AC CDC - LEGALIA, le Responsable d'AE s'assurera qu'il reste toujours suffisamment de personnes représentant les AE, pour assurer la continuité de service de l'AC.

Les demandes de révocation d'une des composantes de l'AC sont à effectuer auprès du Responsable de l'Autorité de Certification, qui effectuera les vérifications d'usages, pour qualifier cette demande.

4.9.13 Causes possibles d'une suspension

Sans objet : la suspension de certificats n'est pas un service assuré.

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

Les LCR sont publiées au format v2, accessibles sur Internet sous forme d'une liste visible de manière internationale pour tous.
Elles sont également publiées au travers d'un service LDAP :
ldap://igc-ldap.caissedesdepots.fr/cn=CDC%20-%20LEGALIA,ou=0002%20180020026,o=CAISSE%20DES%20DEPOTS,c=FR

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24, 7 jours sur 7. De manière générale, le service de certification électronique de Keynectis est accessible 24h/24 et 7j/7. Le taux de disponibilité du service (dont le service de publication sur l'état des certificats) est de 99% base mensuelle (indisponibilité inférieure à 8h par mois), et une indisponibilité continue du service (incident de gravité 1) ne pourra pas être supérieure à 2 heures en heures ouvrées et non ouvrées d'exploitation.

4.10.3 Dispositifs optionnels

Un service OCSP est établi à l'adresse http://igc-ocsp.caissedesdepots.fr/ocsp-legalia/. Ce service permet de vérifier en temps réel et à chaque authentification ou à chaque vérification de signature l'état d'un certificat.

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

La fin de la relation entre le Porteur et l'AC est une cause de révocation.

4.12 Séquestre de clé et recouvrement

Il n'est pas procédé à un séquestre de clé.

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 présentées dans ce chapitre résultent de la stratégie de gestion de risques définie par le comité de pilotage de l'Autorité de Certification. Des précisions quant aux conditions de réalisation de ces exigences sont fournies dans la DPC.

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

La localisation géographique des sites ne nécessite pas de mesures particulières face à des risques de type tremblement de terre, explosion, risque volcanique ou crue.

5.1.2 Accès physique

L'accès physique aux fonctions de génération des certificats et de gestion des révocations, est strictement limité aux seules personnes nominativement autorisées.

L'accès physique aux composantes de l'AC supportant ces fonctions est limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique, permettant la séparation des rôles entre les différents intervenants. La traçabilité des accès est assurée.

En dehors des heures ouvrables, des mesures de détection d'intrusion physique sont mises en œuvre. Des mesures de sécurité physique sont également mises en place pour limiter les accès aux supports sensibles (supports de clés, dossier d'enregistrement, DPC, documents d'applications).

5.1.3 Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre de manière à ce qu'une interruption de service d'alimentation électrique, ou une défaillance de climatisation ne portent pas atteinte aux engagements pris par l'AC en matière de disponibilité (gestion des révocations et informations relatives à l'état des certificats en particulier).

5.1.4 Vulnérabilité aux dégâts des eaux

La définition du périmètre de sécurité prend en considération les risques inhérents aux dégâts des eaux. Des moyens de protection sont mis en œuvre pour parer les risques résiduels (rupture de canalisation par exemple).

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre l'incendie permettent de respecter les engagements pris par l'AC en matière de disponibilité (gestion des révocations et informations relatives à l'état des certificats en particulier), et de pérennité de l'archivage.

5.1.6 Conservation des supports

Les moyens de conservation des supports permettent de respecter les engagements pris par l'AC en matière de restitution et de pérennité de l'archivage.

5.1.7 Mise hors service des supports

En fin de vie, les supports sont, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

5.1.8 Sauvegarde hors site

Afin de permettre une reprise après incident conforme aux engagements pris par l'AC, des sauvegardes hors site des informations et fonctions critiques sont réalisées. La confidentialité des informations, et l'intégrité des applications sauvegardées sont garanties de manière homogène sur le site opérationnel et sur le site de sauvegarde. Cela concerne en particulier les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Pour assurer la sécurité de l'AC, un Comité de Pilotage est mis en place, chargé de l'application opérationnelle de la PC au travers de la mise en œuvre des mesures définies dans la DPC.

Le Comité de Pilotage réalise, ou fait réaliser, les analyses de risques sur le périmètre dont il a la charge, décide de la stratégie de gestion des risques, valide et suit les plans d'actions correspondants. Il fait réaliser les audits internes sur sa composante, et suit la mise en place des mesures correctives nécessaires.

Le Comité de Pilotage de l'AC réunit 5 personnes, ayant chacune un rôle dans la gestion de la sécurité de l'Autorité de Certification dont voici le détail :

- **Responsable de sécurité** : chargé de la mise en œuvre de la politique de sécurité de l'Autorité de Certification. Il gère les contrôles d'accès physiques aux équipements des systèmes de l'AC. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats.
- **Responsable d'application** : Le responsable d'application est chargé 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** - Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de l'AC. Il assure l'administration technique des systèmes et des réseaux de l'AC.
- **Opérateur** - Un opérateur au sein de l'AC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par l'AC.
- **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 l'AC, par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité.

La description des rôles et responsabilités de chacune de ces personnes est établie dans les documents de « Déclaration des Pratiques de Certification » [DPC] de l'AC CDC - LEGALIA et « Rôles et Responsabilités » [ROLES].

5.2.2 Nombre de personnes requises par tâches

Selon la tâche à effectuer une ou plusieurs personnes devront être présentes lors de l'exécution de la tâche. Pour les tâches critiques de l'AC, trois personnes devront être mobilisées pour s'assurer de la qualité et de la sécurité de ces interventions.

5.2.3 Identification et authentification pour chaque rôle

Des mesures d'identification et d'authentification sont mises en place afin de supporter la mise en œuvre de la politique de contrôle d'accès et la traçabilité des opérations ; la politique de contrôle d'accès limite l'accès aux seules personnes autorisées conformément à leur besoin d'en connaître.
Les rôles attribués sont notifiés par écrit aux personnes concernées au travers du document [ROLES].

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.

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

- responsable de sécurité et ingénieur système / opérateur
- auditeur/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

Tout intervenant amené à occuper un rôle identifié comme sensible est soumis à une clause de confidentialité. Les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles. Le personnel d'encadrement possède l'expertise appropriée, et est familier des procédures de sécurité. Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités (description de poste), et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 Procédures de vérification des antécédents

Des procédures de vérification des antécédents sont mises en place pour les personnes appelées à occuper un rôle sensible. L'AC demande en particulier la production d'une copie du bulletin n°3 de leur casier judiciaire. Ces vérifications sont effectuées préalablement à l'affectation à un rôle de confiance et revues au minimum tous les 3 ans.

5.3.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures de fonctionnement de l'Autorité de Certification

5.3.4 Exigences et fréquence en matière de formation continue

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants. Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.

5.3.5 Fréquence et séquence de rotations entre différentes attributions

La rotation entre les attributions est effectuée à l'occasion d'un changement de poste ou de fonction de l'une des personnes disposant d'un rôle opérationnel ou d'un rôle de

confiance pour l'AC. La validité des attributions, en fonction des postes réellement occupés par les personnes cibles est revue à l'occasion de chaque audit interne.

5.3.6 Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans la définition de poste ou la charte de sécurité du personnel (charte d'utilisation des ressources informatiques, numériques et technologiques) pour les rôles sensibles tenus par le personnel de l'AC.

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

Les exigences vis-à-vis des prestataires externes sont contractualisées.

5.3.8 Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de leur prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans l'infrastructure de gestion de clés disposent des procédures correspondantes.

5.4 Procédures de constitution des données d'audit

5.4.1 Type d'événements à enregistrer

Les événements suivants sont enregistrés:

- événements systèmes des différentes composantes de l'IGC (démarrage des serveurs, accès réseau, …) ;
- événements techniques des applications composant l'IGC ;
- événements fonctionnels des applications composant l'IGC (demande de certificats, validation, révocation, rejet…) ;
- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats…) ;
- accès physiques aux locaux ;
- publication et mise à jour des informations liées à l'AC ;
- génération puis publication des LCR
- actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les Porteurs,...) ;
- Changements apportés au personnel.

Ces journaux permettent d'assurer la traçabilité et l'imputabilité des actions effectuées.

5.4.2 Fréquence de traitement des journaux d'événements

Les journaux d'événements sont exploités de manière quotidienne, et systématiquement en cas de remontée d'événement anormal.

5.4.3 Période de conservation des journaux d'événements

Les journaux d'enregistrement sont conservés sur site pendant au maximum un mois avant d'être envoyés vers la solution d'archivage.

Selon la loi française, les enregistrements d'accès physique et les enregistrements de vidéo surveillance ne sont pas conservés plus d'un mois.

5.4.4 Protection des journaux d'événements

Les journaux d'événements sont accessibles uniquement au personnel autorisé de l'AC. Ils ne sont pas modifiables. Des alarmes sont remontées en cas de modification des journaux, ou des paramètres définissant le contenu des journaux.

5.4.5 Procédure de sauvegarde des journaux d'événements

La sauvegarde des journaux électroniques est réalisée tous les 30 jours.

5.4.6 Système de collecte des journaux d'événements

Un système de collecte des journaux d'événements est mis en place.

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

Sans objet.

5.4.8 Evaluation des vulnérabilités

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

Opérationnellement, la fréquence de contrôle des journaux d'événements est de :

- Fréquence d'analyse complète des journaux d'évènements : 1 fois par semaine et dès la détection d'une anomalie.
- Fréquence de contrôle des journaux d'évènements pour identification des tentatives en échec d'accès ou d'opération : 1 fois par 24h.
- Fréquence de rapprochement des journaux d'évènements : 1 fois par mois.

Le contrôle des journaux des événements fonctionnels est réalisé à la demande en cas de litige, ou pour analyse de comportement de l'Autorité de Certification.

5.5 Archivage des données

L'AC procède en propre à l'archivage des données ci-dessous, et se réserve le droit de déléguer tout ou partie de ces obligations à un tiers avec lequel elle contractera sur la base de ces obligations.

5.5.1 Types de données à archiver

Les données de l'AC à archiver sont les suivantes, selon les processus décrits dans la DPC :

- PC et DPC, ainsi que leur publication ;
- Certificats, et LCR publiés ;
- Dossiers d'enregistrement des Porteurs et Conditions Générales d'Utilisation signées, présentés par les Mandataires de Certification ;
- Les mandats des Mandataires de Certification ;
- Les attestations d'identification uniques de l'entreprise des Clients ;
- Les attestations des Représentants légaux des Clients ;
- Les demandes de révocation de certificats ;
- Les conventions AC – AE établies pour les différents métiers couverts par l'AC ;
- Les journaux d'événements ;
- Les logiciels exécutables et fichiers de configuration :
    - Du middleware installé sur le poste du client ;
    - Des outils paramétrés chez l'Opérateur de Service de Certification Keynectis.

5.5.2 Période de conservation des archives

Les certificats de l'AC sont archivés pendant 10 ans. Les dossiers d'enregistrement sont archivés dans un bureau d'archive local à l'AE avant d'être transférés sur le site d'archivage de l'AC pour une période de 10 ans. Les certificats et LCR sont archivés pendant 10 ans. Les journaux d'événements sont archivés pendant 10 ans.

5.5.3 Protection des archives

Quel que soit leur support, les archives sont protégées en intégrité, et ne sont accessibles qu'aux personnes autorisées. Ces archives sont lisibles et exploitables sur l'ensemble de leur cycle de vie.

5.5.4 Procédure de sauvegarde des archives

Les archives sont sauvegardées de manière sécurisée, et accessibles uniquement aux seules personnes autorisées (c'est-à-dire au comité de pilotage de l'AC ou à toute personne en ayant reçu l'autorisation par ce comité de pilotage).

5.5.5 Exigences d'horodatage des données

L'horodatage des données des événements journalisés est automatique. Pour cela, les composants de l'IGC sont synchronisés sur un même serveur synchronisé avec l'heure universelle. Une synchronisation est également mise en place entre les infrastructures internes de l'AC et les infrastructures externes de l'OSC.

5.5.6 Système de collecte des archives

Sans objet.

5.5.7 Procédure de récupération et de vérification des archives

Toute demande de récupération d'archive doit être adressée au Responsable d'Application de l'AC CDC - LEGALIA. La récupération et la vérification des archives peuvent être effectuées dans un délai de 10 ans. La restitution et la vérification des archives sont effectuées dans un délai maximal de 2 jours ouvrés.

5.6 Changement de clé d'AC

La durée de vie des clés de l'AC CDC - LEGALIA est de 10 ans. Son renouvellement sera demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.
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 du certificat d'AC doit être supérieure à celle des certificats qu'elle signe.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats. A l'occasion du processus de renouvellement, les demandes des Porteurs seront automatiquement orientées pour signature vers la nouvelle bi-clé d'AC.

Le certificat d'AC 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

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

Un incident majeur – perte, suspicion de compromission, compromission ou vol de clé privée de gestion des certificats par exemple – doit être immédiatement signalé à l'AC. La publication de la révocation du certificat, si elle s'avère nécessaire, est effectuée dans la plus grande urgence par tout moyen nécessaire. L'AC préviendra alors directement et sans délai le contact identifié sur le site : http://www.references.modernisation.gouv.fr.

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

Un plan de continuité est mis en place permettant de répondre aux exigences de disponibilité des différentes composantes de l'IGC. Ce plan de continuité est propre à chaque branche métier du Groupe CDC. Ce plan de continuité est testé au moins une fois par an.

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

La compromission d'une clé d'AC entraîne immédiatement la révocation du certificat correspondant. Les cas de compromission des éléments secrets des autres composantes sont traités dans le plan de continuité d'activité.

5.7.4 Capacités de continuité d'activité suite à un sinistre

La capacité de continuité de l'activité suite à un sinistre est également traitée dans le plan de continuité d'activité.

5.8 Fin de vie de l'IGC

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

Une ou plusieurs Composantes de l'IGC peuvent être amenées à cesser leur activité ou à les transférer à une autre entité. Le transfert d'activité ne comporte pas d'incidence sur la validité des Certificats émis antérieurement au transfert considéré, et la reprise de cette activité est organisée par l'AC en collaboration avec la nouvelle entité.

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC a pris les mesures suivantes :

- Elle a mis en place des procédures permettant d'assurer un service constant pour les AE, les Porteurs et leurs représentants (Mandataires, représentants légaux), en particulier en matière d'archivage (notamment, archivage des certificats des Porteurs et des informations relatives aux certificats)
- Elle assure la continuité du service d'archivage ;
- Elle assure la continuité du service de Révocation ;
- Elle prévient les Mandataires de Certification dans le cas où les changements envisagés peuvent avoir des répercussions sur les engagements pris.

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 s'engage à les informer de ce transfert aussitôt que possible et, au moins, 1 mois avant.

L'AC communiquera au plus tôt, aux représentants concernés de l'administration, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC communiquera également à l'administration concernée, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus.

L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les Porteurs et les utilisateurs de certificats. L'AC tiendra informée l'administration concernée de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus.

La cessation d'activité affecte l'activité de l'AC, telle que définie ci-dessous.

5.8.2 Cessation d'activité affectant l'AC

La cessation d'activité comporte une incidence sur la validité des Certificats émis antérieurement à la cessation concernée, et une procédure spécifique est mise en œuvre dans ce cas.

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 s'engage à les informer de cette cessation aussitôt que possible et, au moins, 1 mois avant.

En cas de cessation d'activité, l'AC s'engage à respecter les principes suivants :

- Prévenir les Porteurs, Mandataires de Certification, et représentants de l'AE au moins un mois en avance ;
- La clé privée d'émission des certificats ne sera transmise en aucun cas ;
- Toutes les mesures nécessaires seront prises pour la détruire ou la rendre inopérante ;
- Le certificat d'AC sera révoqué ;
- Tous les certificats émis encore en cours de validité seront révoqués ;
- Tous les mandataires de certification, responsables des certificats révoqués ou à révoquer seront tenus informés.

L'AC communiquera au plus tôt, aux représentants concernés de l'administration, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC communiquera également à l'administration concernée, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus.

L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les Porteurs et les utilisateurs de certificats. L'AC tiendra informée l'administration concernée de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus. Les représentants du comité de pilotage de l'AC devront se

réunir pour réaliser les opérations sensibles de désactivation des clés d'AC, et de révocation des certificats préalablement émis.

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

Les clés de l'AC CDC - LEGALIA sont générées lors de la cérémonie des clés, en présence du comité de pilotage de l'AC, et suivant la procédure du maître de cérémonie. Cette séance de cérémonie des clés a lieu sous le contrôle d'un officier public ministériel, veillant à la bonne application des procédures et au respect des exigences de sécurité définies dans ce document et dans la Déclaration des Pratiques de Certification.

6.1.1.2 Clés Porteurs générées par l'AC

Sans objet.

6.1.1.3 Clés Porteurs générées par le Porteur

La clé privée est générée sur le support physique SSCD du Porteur lors du retrait de son certificat. Un code PIN personnel choisi par le Porteur protège l'accès au contenu du support physique : la clé privée du Porteur reste sous son contrôle exclusif.

6.1.2 Transmission de la clé privée à son propriétaire

La clé privée est générée localement au moment du retrait déclenché par le (futur) Porteur du certificat au niveau du support physique SSCD protégé par un code PIN personnel.

Le support physique utilisé par l'Autorité de Certification CDC - LEGALIA est évalué EAL 4+ et qualifié renforcé. Il garantit la sécurité des échanges entre le support physique et les différents composants de l'Autorité de Certification.

6.1.3 Transmission de clé publique à l'AC

Sans objet pour la clé publique de l'AC. Pour la clé publique du Porteur, elle est transmise à l'AC par un canal assurant l'intégrité et l'authentification de la transmission, lors de la phase de retrait du certificat.

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 sont mises à disposition des utilisateurs de certificats, et consultables publiquement tel que défini en section 2.2.2.

6.1.5 Tailles des clés

Les tailles de clés sont les suivantes :

- 2048 bits pour la taille des clés de l'AC CDC - LEGALIA.
- 2048 bits pour la taille des clés des Porteurs pour un certificat d'authentification ou de signature.

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

Cf chapitre §7.

6.1.7 Objectifs d'usages de la clé

L'utilisation de la clé privée pour l'AC CDC - LEGALIA, et du certificat associé est limitée à la signature de certificats Porteurs, et de LCR. La clé privée d'AC n'est utilisée que dans un environnement sécurisé, au sein d'un boîtier cryptographique matériel (HSM).

Le Porteur s'engage, en signant le formulaire de demande de certificat et les Conditions Générales d'Utilisation correspondantes, auprès de la CDC à n'utiliser son certificat qu'à des fins d'authentification ou de signature sur les applications cibles définies en §1.4.1. Toute autre utilisation est effectuée sous la responsabilité du Porteur de certificat.

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Module cryptographique de l'AC

Le module cryptographique de l'AC pour la génération et la mise en œuvre des clés de signature répond aux exigences énoncées par la réglementation. Il s'agit d'un boîtier cryptographique matériel, répondant aux critères communs au niveau EAL4+, dédié à la gestion des certificats de la Caisse des Dépôts. Le module cryptographique de signature de certificat et des informations de révocation ne fait pas l'objet de manipulation non autorisée lors de son transport ou lors de son stockage.

6.2.1.2 Dispositifs d'authentification des Porteurs

L'AC fournit au Porteur un dispositif matériel de stockage de clé privée. Les Porteurs sont responsables de la confidentialité de leurs données d'activation (code PIN). La clé privée des Porteurs n'est utilisée que dans un environnement sécurisé, au sein du support physique, évalué EAL4+, et qualifié renforcé par l'ANSSI (carte MultiApp ID IAS ECC sur composant NXP conçue par Gemalto).

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle de la clé privée de l'AC CDC - LEGALIA est effectué par au moins trois membres du comité de pilotage, qui sont présents simultanément pour rendre l'usage de ces clés possibles. La clé privée des Porteurs est sous leur contrôle exclusif.

6.2.3 Séquestre de la clé privée

La clé privée de l'AC CDC - LEGALIA, et les clés privées des Porteurs, ne font pas l'objet de séquestre.

6.2.4 Copie de secours de la clé privée

La clé privée de l'AC CDC - LEGALIA fait l'objet de copie de secours. Ces copies de secours bénéficient du même niveau de sécurité que la clé privée originale. La clé privée des Porteurs ne fait pas l'objet d'une copie de secours.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC CDC - LEGALIA, et les clés privées des Porteurs ne font pas l'objet d'un archivage.

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

Il n'y a pas de transfert possible de la clé privée de l'AC CDC - LEGALIA puisqu'elle est générée et stockée par le même HSM. Le seul transfert possible est le transfert de clés privées vers le HSM de secours, à partir de la copie de secours (cf. ci-dessus). Il n'y a aucun transfert possible de la clé privée des Porteurs.

6.2.7 Stockage de la clé privée dans un module cryptographique

Le stockage de la clé privée de l'AC, et des clés privés des Porteurs est réalisé par le matériel cryptographique (respectivement HSM, clé USB ou carte à puce) dans les conditions de sécurité définies par leur profil de protection respectif, support à l'évaluation EAL 4+.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'AC

L'activation de la clé privée de l'AC CDC - LEGALIA nécessite la présence de trois membres du comité de pilotage au moins.

6.2.8.2 Clés privées des Porteurs

L'activation de la clé privée d'un Porteur nécessite la saisie du code PIN du support physique, et est sous le contrôle exclusif du Porteur.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

La clé privée de l'AC CDC - LEGALIA est désactivable à partir du module cryptographique. Cette désactivation nécessite la présence de trois membres du comité de pilotage au moins.

6.2.9.2 Clés privées des Porteurs

Sans objet.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'AC

La destruction de la clé privée de l'AC ne peut être effectuée qu'à partir du module cryptographique (HSM).

6.2.10.2 Clés privées des Porteurs

La destruction de la clé privée d'un Porteur ne peut être effectuée qu'à partir du support physique.

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

Les modules cryptographiques de l'AC, et des clés privés des Porteurs ont fait l'objet d'une évaluation EAL 4+.

6.3 Autres aspects de la gestion des bi clés

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC CDC - LEGALIA, et les clés publiques des Porteurs sont archivées dans le cadre de la politique d'archivage des certificats (cf. 5.5).

6.3.2 Durée de vie des bi-clés et des certificats

Les clés de signature et les certificats de l'AC CDC - LEGALIA ont une durée de vie de 10 ans.
La durée de vie opérationnelle d'un certificat Porteur est limitée par son expiration (3 ans) ou sa révocation. La durée de vie opérationnelle d'une bi-clé est équivalente à celle du certificat auquel elle correspond.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

Les éléments nécessaires à l'activation de la clé privée de l'AC, sont générés de manière sécurisée, et uniquement accessibles aux membres du comité de pilotage, seuls autorisés à procéder à cette activation.

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

Les éléments nécessaires à l'activation de la clé privée des Porteurs (code PIN du support physique) sont à définir par le Porteur au moment de l'installation du support physique. Ce mécanisme nécessite l'installation préalable des outils permettant au système d'exploitation utilisé par le Porteur de communiquer avec le support physique.

L'AC s'assure que le code d'activation retenu par le Porteur est sécurisé, en appliquant une politique de mots de passe visant à refuser les mots de passe trop simple. Cette politique de gestion des mots de passe est directement intégrée dans la configuration des outils nécessaires à l'utilisation du support physique. La politique de gestion des mots de passe est alors explicitement présentée au Porteur lors des opérations de changement de code PIN. Dans ce cas l'ancien code PIN est demandé au Porteur.

Politique pour le code PIN
La politique est la suivante :

- Le mot de passe doit comporter 6 caractères, et il doit comporter des chiffres de « 0 » à « 9 ».
- L'utilisation du PIN précédent est interdite.
- Les séquences de 6 caractères identiques sont interdites.
- De plus, les codes PIN suivants sont interdits : « 123456 », « 012345 », « 654321 », « 543210 ».

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 des clés d'AC ne sont délivrées qu'aux membres du comité de pilotage. Leur identité est tenue dans un référentiel documentaire maintenu par l'AC CDC - LEGALIA.

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

Les données d'activation d'un Porteur ne sont connues que par le seul Porteur, et sous son contrôle exclusif.

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

6.5.1.1 Identification et authentification

Les systèmes, applications et bases de données identifient et authentifient de façon unique les utilisateurs. Toute interaction entre le système et un utilisateur n'est possible qu'après une identification et une authentification réussies. Pour chaque interaction, le système établit l'identité de l'entité. Les informations d'authentification sont stockées de façon telle qu'elles sont seulement accessibles par des utilisateurs autorisés.

6.5.1.2 Contrôle d'accès

Les profils et droits d'accès aux équipements de l'AC sont définis et documentés, ainsi que les procédures d'enregistrement des Porteurs. Les systèmes, applications et bases de données, peuvent distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. Il est possible de :

- Refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet,
- Limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas cet objet,
- Accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel.

Quelqu'un qui n'est pas un utilisateur autorisé ne peut pas accorder ou retirer des droits d'accès à un objet. De même, seuls des utilisateurs autorisés peuvent introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.

6.5.1.3 Administration et exploitation

L'utilisation de programmes utilitaires est restreinte et contrôlée.
Les procédures opérationnelles d'administration et exploitation de l'Autorité de Certification sont documentées, suivies et régulièrement mises à jour.
Les conditions de mise en service (paramétrage initial de sécurité des serveurs) sont documentées.

Les conditions de fin de vie (destruction et mise au rebus) des équipements sont documentées afin de garantir la non divulgation des informations sensibles qu'ils peuvent détenir.

L'ensemble des matériels sensibles de l'IGC fait l'objet de procédure de maintenance afin de garantir la disponibilité des fonctions et des informations.
Des mesures de contrôles des actions de maintenance sont mises en application.

6.5.1.4 Intégrité des composantes

Des mesures de maîtrise de détection et de prévention sont mises en œuvre sur l'ensemble des composants de l'IGC afin de fournir une protection contre les logiciels

malveillants. Les composantes du réseau local sont maintenues dans un environnement physiquement sécurisé ; des vérifications périodiques de conformité de leur configuration sont effectuées.

6.5.1.5 Sécurité des flux

Des mesures de sécurité sont mises en œuvre de manière à garantir l'authentification d'origine, l'intégrité et la confidentialité le cas échéant des données échangées entre entités intervenant dans le processus.

6.5.1.6 Journalisation et audit

Un suivi d'activité est possible au travers des journaux d'événements.

6.5.1.7 Supervision et contrôle

Une surveillance permanente est mise en place et des systèmes d'alarme installés pour détecter enregistrer et réagir rapidement face à toute tentative non autorisée et ou irrégulière d'accès aux ressources (physique et / ou logique).

6.5.1.8 Sensibilisation

Des procédures appropriées de sensibilisation des usagers de l'IGC sont mises en œuvre.

6.5.2 Niveau de qualification des systèmes informatiques

- Le boîtier cryptographique HSM et le support physique des Porteurs sont évalués EAL4+.
- Les supports physiques sont qualifiés au niveau renforcé.
- Le service technique fourni par l'OSC est qualifié.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

Les infrastructures de développement et d'essai sont séparées des infrastructures opérationnelles de l'IGC. Les critères de recette et validation de nouveaux systèmes d'information, de mises à niveau et nouvelles versions sont documentés et des essais adéquats du système sont effectués avant sa recette et mise en production.

6.6.2 Mesures liées à la gestion de la sécurité

L'IGC est suivie dans le cadre de la mise en place du système de management de la sécurité de l'AC. Le comité de pilotage gère la remontée d'information vers l'AC qui est averti de toute modification significative. Les évolutions des composantes font l'objet d'une remise à jour des procédures opérationnelles.

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

En ce qui concerne les logiciels et matériels évalués, l'AC poursuit sa surveillance des exigences du processus de maintenance pour maintenir le niveau de confiance.

6.7 Mesures de sécurité réseau

Les mesures mises en place répondent à la stratégie de gestion des risques de la CDC pour les systèmes d'information. L'AC est implantée sur un réseau protégée par au moins deux niveaux de passerelles de type « coupe-feu ». Ces passerelles sont

configurées de façon à n'accepter que les flux strictement nécessaires. Les communications réseau véhiculant des informations confidentielles font l'objet de mesures de protection contre l'écoute des informations. Des scans périodiques de détection de vulnérabilités sur les équipements de l'IGC sont conduits. Des passerelles de sécurité sont mises en place afin de protéger la composante locale du système d'information des accès non autorisés.

6.8 Horodatage / système de datation

Cf. §5.5.5.

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 Profils des certificats

Les certificats de l'IGC CDC sont au format X509v3.

7.1.1 Certificat de l'AC CDC - LEGALIA

```
    Data:
        Version: 3 (0x2)
        Serial Number: 11:21:0a:35:c8:2b:57:cf:e7:69:fd:c8:55:5f:f1:a6:a9:5f
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=FR, O=CAISSE DES DEPOTS, OU=0002 180020026, CN=CDC - RACINE
        Validity
            Not Before: Nov 17 00:00:00 2009 GMT
            Not After : Nov 15 00:00:00 2019 GMT
        Subject: C=FR, O=CAISSE DES DEPOTS, OU=0002 180020026, CN=CDC - LEGALIA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:d5:60:28:38:18:22:79:57:55:92:95:88:fa:de:
                    a5:9d:1f:a4:b9:61:c8:a5:00:f8:4f:d8:02:4d:95:
                    01:18:52:b3:7f:31:88:03:9e:ee:af:d8:f4:65:60:
                    67:af:63:5a:83:2f:9f:c1:ce:fb:8b:3c:02:f5:c4:
                    e2:ca:25:95:0c:a1:ef:e3:eb:d8:53:16:be:cf:51:
                    f0:14:97:f3:00:e8:79:4a:b9:da:54:c3:21:b3:90:
                    db:34:4d:9e:11:ee:0c:37:3d:ad:53:e2:4a:a1:7c:
                    93:a6:55:17:01:7a:e1:55:ac:ef:c6:d9:ae:14:fc:
                    0d:12:0d:42:90:b3:09:2a:e9:40:bc:08:70:68:52:
                    8e:a8:63:51:c7:e0:b1:12:84:d9:c0:70:91:f5:fb:
                    a5:3b:ec:08:13:2d:ec:b1:7f:3d:d4:8d:f2:ea:5d:
                    e2:b5:17:a3:31:af:26:2f:da:f7:ac:7e:1e:f9:97:
                    36:82:f2:e5:a8:a4:ee:fc:21:5b:f2:d9:b1:a0:9d:
                    81:58:67:b2:d5:cd:a2:28:6d:d7:4d:87:ba:7d:14:
                    7f:52:8f:37:a1:bf:52:01:08:61:44:09:35:79:3b:
                    96:e5:38:4e:fc:af:8d:8e:cb:2b:36:ba:c0:39:f0:
                    fd:4f:8e:85:f2:7d:24:28:12:6b:97:51:25:16:bc:
                    93:8d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            Authority Information Access:
                OCSP - URI:http://igc-ocsp.caissedesdepots.fr/ocsp-racine/
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: http://igc-pc.caissedesdepots.fr/pc-racine.pdf
            X509v3 CRL Distribution Points:
                URI:http://igc-crl.caissedesdepots.fr/cdc/racine.crl
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                04:16:3A:3F:01:62:EC:FA:D6:DB:5D:64:2B:7E:03:E0:94:85:A2:E5
            X509v3 Authority Key Identifier:
                keyid:78:D3:33:04:E2:2A:ED:94:09:2A:15:E1:0C:4E:33:F9:F2:F7:07:7D
    Signature Algorithm: sha256WithRSAEncryption
        10:1a:ea:d4:9b:b2:d5:7c:bf:6a:2d:a8:4e:dc:d1:b3:e0:4b:
        67:0e:c1:e1:d5:25:11:e8:0f:a1:4d:14:10:f7:3d:c2:ac:d7:
        fa:d8:f8:79:bc:09:1e:ab:5c:ba:67:bc:23:85:c1:46:0a:78:
        2e:b6:c2:8d:ed:a5:4b:a5:cc:3e:63:91:43:ab:32:a3:a5:00:
        87:04:7b:2b:d6:5d:f4:37:6e:02:3d:b3:4b:c2:cb:24:9e:5f:
        0d:7d:fd:96:c4:e8:e6:52:75:6a:12:18:d3:40:07:bb:39:e0:
        fe:00:95:62:6b:14:cb:46:d6:04:cd:e1:e0:db:e6:cc:9a:41:
        3d:39:7c:06:d0:92:8b:2b:15:f0:dd:60:fc:a7:c0:b4:29:2c:
        3f:3b:4b:97:6e:b0:8c:00:9a:4e:be:0f:ef:a5:35:6e:2d:50:
        16:33:b3:32:55:ce:87:95:7f:ec:be:38:81:68:ee:19:54:96:
        10:ab:22:2c:e1:89:3c:d7:ac:b5:66:5b:e6:df:3b:71:7f:0d:
        59:6d:66:7c:cd:1b:e3:41:4b:c9:fe:1b:9a:fb:3a:ff:01:1f:
        e8:35:8f:b5:88:fb:a7:13:89:5e:4d:57:46:83:28:c3:62:b3:
        5e:73:eb:26:df:61:45:86:60:4a:57:27:e9:f8:51:64:26:56:
        57:ab:94:dd
```

7.1.2 Certificat des Porteurs

7.1.2.1 Champs de base

```
    Data:
        Version: 3 (0x2)
        Serial Number: […]
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=FR, O=CAISSE DES DEPOTS, OU=0002 180020026, CN=CDC - LEGALIA
        Validity
            Not Before: Jan 22 13:12:21 2013 GMT
            Not After : Jan 22 13:12:21 2016 GMT
        Subject: C=FR, O=Entite, OU=0002 SIREN ou SIRET, CN=Prenom NOM
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit): [...]
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Key Usage: critical
                [Authentification] Digital Signature
                [Signature] Non Repudiation
            Authority Information Access:
                OCSP - URI:http://igc-ocsp.caissedesdepots.fr/ocsp-legalia/
            X509v3 Certificate Policies:
                [Authentification] Policy: 1.2.250.1.5.1.1.1.2.2
                [Signature] Policy: 1.2.250.1.5.1.1.1.3.2
                  CPS: http://igc-pc.caissedesdepots.fr/pc-legalia.pdf
            X509v3 CRL Distribution Points:
                URI:http://igc-crl.caissedesdepots.fr/cdc/legalia.crl
                URI:ldap://igc-ldap.caissedesdepots.fr/cn=CDC%20-
%20LEGALIA,ou=0002%20180020026,o=CAISSE%20DES%20DEPOTS,c=FR?certificaterevocationli
st?sub?objectclass=pkiCA
            X509v3 Subject Alternative Name:
                email:[…]
            X509v3 Subject Key Identifier:
                […]
            X509v3 Authority Key Identifier:
                keyid:[…]
    Signature Algorithm: sha256WithRSAEncryption [...]
```

7.2 Profil des listes de certificats révoqués

L'émetteur de la liste de révocation a comme DN le nom de l'Autorité de Certification signataire de cette LCR. Les certificats révoqués sont listés et nommés par leur numéro de série. La date de révocation est précisée. Pour chaque certificat révoqué, la raison de révocation ne sera pas publiée.

Les LCR émises présentent les caractéristiques suivantes :

- La version de la LCR est v2.
- L'algorithme de signature est sha256WithRSAEncryption.
- Les extensions Numéro de la LCR & Authority Key Identifier sont présentes.
- Durée de validité : 24 heures
- Périodicité de mise à jour : 1 heure
- URL http de publication (CRLdp) : http://igc-crl.caissedesdepots.fr/cdc/legalia.crl

7.3 Profil OCSP

Le service OCSP est opéré par l'Opérateur de Service de Certification de l'AC. Pour les certificats Porteurs, il est accessible via l'URL : http://igc-ocsp.caissedesdepots.fr/ocsp-legalia/
Le profil OCSP est détaillé dans la DPC.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquences et / ou circonstances des évaluations

Un contrôle de conformité à la PC pourra être effectué, sur demande du comité de pilotage de l'Autorité de Certification et sous la responsabilité du Contrôleur. L'AC s'engage à effectuer ce contrôle au minimum une fois tous les ans.

Par ailleurs, avant la première mise en service d'une composante de son IGC ou suite à toute modification significative au sein d'une composante, l'AC fera également procéder à un contrôle de conformité de cette composante.

Dans le cadre de sa qualification RGS, l'Autorité de Certification CDC – LEGALIA est soumise aux audits correspondants de la part de l'organisme de qualification.

8.2 Identités / qualification des évaluateurs

Le contrôleur se doit d'être rigoureux pour s'assurer que les politiques, déclarations et services sont correctement mis en œuvre et détecter les cas de non conformités qui pourraient compromettre la sécurité du service offert. L'AC s'engage à mandater des contrôleurs internes qui soient compétents en sécurité des systèmes d'information, en particulier dans le domaine d'activité de la composante contrôlée. Les personnes susceptibles d'effectuer ces contrôles pour l'AC CDC - LEGALIA sont définies dans la Déclaration des Pratiques de Certification.

8.3 Relations entre évaluateurs et entités évaluées

Les auditeurs en charge de l'audit de conformité sont :

- Une entreprise privée indépendante de la CDC
- Une équipe interne à la CDC indépendante de la composante contrôlée.

L'AC détermine si les auditeurs répondent aux exigences ci-dessus avant de les désigner. Le contrôleur est désigné par l'AC, qui l'autorise à contrôler les pratiques de la composante cible de l'audit. Il sera indépendant de l'AC et de l'AE.

8.4 Sujets couverts par les évaluations

Le contrôleur procède à des contrôles de conformité de la composante auditée, soit tout ou partie de la mise en œuvre :

- des politiques de certification ;
- des déclarations de pratique de certification ;
- des services de certification mis en œuvre.

A chaque audit ponctuel, le contrôleur établira un programme d'audit, permettant de définir précisément quelle composante de l'IGC est visée par l'audit. Ce contrôle sera effectué à chaque mise en service d'une nouvelle composante, ou d'une modification majeure sur une composante existante. Tous les ans, les auditeurs proposeront au responsable de l'application une liste de composantes, et procédures qu'ils souhaiteront vérifier, et établiront ainsi le programme détaillé de l'audit.

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 qui peut être « réussite, échec, ou à confirmer ».

En cas d'échec, l'équipe d'audit remet des recommandations à l'AC, décrit le niveau de criticité et les failles identifiées à corriger. 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… Le choix des mesures à appliquer appartient ensuite à l'AC.

En cas de résultat « à confirmer », l'équipe d'audit identifie les non conformités, et les hiérarchisent. Il appartient à l'AC de proposer un calendrier de résolution des non conformités ; un contrôle de vérification permettra de lever les non conformités identifiées. En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC.

8.6 Communication des résultats

Les résultats de l'audit seront tenus à la disposition du comité de pilotage de l'Autorité de Certification, et 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

Les certificats sont émis par la Caisse des Dépôts (CDC), qui se réserve le droit d'en facturer la délivrance, ou de facturer les services connexes associés.

9.1.2 Tarifs pour accéder aux certificats

Les certificats sont émis par la Caisse des Dépôts (CDC), qui se réserve le droit d'en facturer la délivrance, ou de facturer les services connexes associés.

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

Les certificats sont émis par la Caisse des Dépôts (CDC), qui se réserve le droit d'en facturer la délivrance, ou de facturer les services connexes associés.

9.1.4 Tarifs pour d'autres services

Les certificats sont émis par la Caisse des Dépôts (CDC), qui se réserve le droit d'en facturer la délivrance, ou de facturer les services connexes associés.

9.1.5 Politique de remboursement

Pas d'exigences particulières.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

Les risques susceptibles d'engager la responsabilité de la CDC sont couverts en propre par la CDC, qui est son propre assureur.

9.2.2 Autres ressources

La CDC reconnaît disposer d'une garantie financière suffisante spécialement affectée à la couverture des risques financiers afférents à son activité de PSCE.

9.2.3 Couverture et garantie concernant les entités utilisatrices

En cas de dommage subi par une entité utilisatrice du fait d'un manquement par l'AC à ses obligations, l'AC pourra être amenée à dédommager l'entité utilisatrice dans la limite de la responsabilité de l'AC définie dans les conditions générales d'utilisation et aux présentes.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

L'AC met en place un inventaire de tous les biens informationnels et procède à une classification de manière à définir des exigences de protection en accord avec les besoins.

En particulier, les informations suivantes sont traitées comme confidentielles :

- Les clés privées de l'AC CDC - LEGALIA, et des certificats des Porteurs ;
- Les informations personnelles (nom prénom, email) recueillies sur les Porteurs et les Mandataires de Certification lors du processus de demande de certificats ;
- Les données d'activation (code PIN d'accès au support physique ou secrets d'activation du HSM) ;
- Les journaux d'événements ;
- Les rapports d'audit ;
- Les causes de révocation des certificats.

9.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3 Responsabilités en terme de protection des informations confidentielles

Les informations confidentielles ne sont accessibles qu'aux personnes concernées par de telles informations ou qui ont l'obligation de conserver et/ou traiter de telles informations. La CDC s'engage à traiter les informations confidentielles recueillies dans le respect des lois et règlements en vigueur.

Les informations confidentielles listées ci-dessus ne feront l'objet de communication externe que pour les strictes nécessités de la gestion des opérations effectuées en exécution de la DPC, pour répondre aux exigences légales ou pour l'exécution de prestations de services confiées à des tiers, étant précisé que ces tiers sont contractuellement tenus d'une obligation de confidentialité.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

Des mesures techniques, procédurales et organisationnelles sont mises en place pour garantir la protection des données personnelles recueillies lors de l'enregistrement. La CDC se conforme aux dispositions légales et réglementaires en vigueur concernant la collecte et le traitement de données à caractère personnel. En application des dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les personnes physiques disposent d'un droit d'accès, de rectification ou d'opposition des données à caractère personnel les concernant. Ce droit peut être exercé en adressant un mail à l'Autorité d'Enregistrement.

9.4.2 Informations à caractère personnel

Les informations à caractère personnel sont les informations nominatives du Porteur et du Mandataire de Certification, enregistrées au sein du dossier d'enregistrement. Il s'agit des informations nom / prénom / email, ainsi que des motifs de révocation.

9.4.3 Informations à caractère non personnel

Pas d'exigence spécifique.

9.4.4 Responsabilité en terme de protection des données personnelles

Il est entendu que toute collecte de données à caractère personnel par l'AC est réalisée dans le strict respect des lois et règlements en vigueur, en particulier de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. L'AC reconnaît

avoir procédé aux formalités déclaratives qui lui incombent au titre de la présente PC et des traitements de données à caractère personnel qui seraient réalisés.

9.4.5 Notification et consentement d'utilisation des données personnelles

Le Porteur est averti de l'utilisation faite par l'AC de ces données personnelles, à l'occasion de la phase de signature des Conditions Générales d'Utilisation des Certificats lors de l'enregistrement. Il signe personnellement ces conditions d'usage, valant acceptation et consentement.

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

Les enregistrements peuvent être mis à disposition en cas de besoin pour servir de preuve lors d'une procédure judiciaire ou administrative.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Pas d'exigence spécifique.

9.5 Droits sur la propriété intellectuelle et industrielle

Lors de l'exécution des prestations de services définies aux présentes, il peut être échangé ou utiliser des éléments protégés par la législation sur les droits d'auteur ou les bases de données. Ces éléments, ainsi que les droits de propriété intellectuelle qui y sont attachés, resteront la propriété du détenteur des droits correspondants. Le bénéficiaire des services aura le droit de reproduire ces éléments pour son usage interne. Il ne pourra, sans l'autorisation préalable du détenteur des droits, mettre à disposition de tiers, extraire ou réutiliser, en tout ou partie, ces éléments ou des œuvres dérivées ou copies notamment les logiciels et bases de données.

Du fait de son enregistrement, le Porteur n'acquiert sur les données de création de chiffrement qui lui sont remis par l'AE qu'un droit d'usage limité aux opérations effectuées conformément à la présente politique de certification et aux conditions contractuelles d'utilisation du service. Le Porteur n'acquiert aucun droit de propriété, de quelque nature que ce soit, sur les certificats et les bi-clés, qu'il s'engage à restituer à l'AE et à cesser d'utiliser dans les cas prévues aux présentes ou dans les conditions d'utilisation du service.

9.6 Interprétations contractuelles et garanties

9.6.1 Autorités de certification

La CDC est responsable, en tant que PSCE :

- de la validation et de la publication de la PC,
- de la validation de la DPC, et de sa conformité à la PC,
- de la conformité des certificats émis vis-à-vis de la présente PC,
- du respect de tous les principes de sécurité par les différentes composantes de l'IGC, et des contrôles afférents.

La CDC fait son affaire de toute conséquence dommageable résultant directement du non-respect du présent document par elle-même ou l'une des entités de l'IGC, conformément aux principes de la responsabilité civile. La CDC s'engage à mettre en œuvre les moyens décrits dans la présente PC pour assurer la sécurité des prestations, prendre les actions nécessaires pour remédier aux non conformités suite à un audit de conformité, permettre l'émission et la délivrance du certificat, la mise en œuvre des

procédures de renouvellement et de révocation des certificats, et la publication de la présente PC et de la liste des certificats révoqués.

Sauf à démontrer qu'elle n'a commis aucune faute intentionnelle ou de négligence, la CDC est responsable de tout préjudice causé à toute personne physique ou morale qui s'est fiée raisonnablement aux certificats délivrés dans chacun des cas suivants :

- Les informations contenues dans le certificat ne correspondent pas aux informations fournies lors de l'enregistrement
- La délivrance du certificat n'a pas donné lieu à vérification de possession de la clé privée correspondante par le Porteur
- L'AC n'a pas fait procéder à l'enregistrement de la révocation d'un certificat, et publié cette information conformément à ses engagements.

La CDC n'est pas responsable du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation.

9.6.2 Service d'enregistrement

L'AE s'engage à mettre en œuvre les moyens décrits dans la présente PC complétée par la « Convention AC – AE » pour le métier considéré, et complétée par la DPC pour :

- la vérification de la compatibilité des informations recueillies avec celles exigées par la présente PC pour la délivrance de certificats Porteurs ;
- la conformité des informations contenues dans le certificat avec les informations recueillies aux fins de délivrance de certificats ;
- la vérification des pièces justificatives qui lui ont été communiquées en support à l'identification de l'éventuel mandataire de certification et des Porteurs ;
- la vérification de l'authenticité d'une demande de révocation qui lui est soumis,
- la protection de ses clés privées et de ses données d'activation, utilisées dans le cadre de ses relations avec l'AC.

9.6.3 Porteurs de certificats

Le Porteur a le devoir de :

- communiquer des informations exactes et à jour lors de la demande de certificat, et lors des demandes de renouvellement ;
- n'utiliser les certificats de l'AC CDC - LEGALIA qu'à des fins d'authentification (OID 1.2.250.1.5.1.1.1.2.2) ou de signature (OID 1.2.250.1.5.1.1.1.3.2) conformément à la Politique de Certification de l'AC ;
- utiliser le support physique (remis par la CDC) pour effectuer le retrait du certificat ;
- protéger sa clé privée par des moyens appropriés à son environnement ;
- protéger les données d'activation de la bi-clé correspondante (code PIN) ;
- 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 mandataire de certification ou de l'AC en cas de :
    - perte ou de vol de la clé USB ou de la carte à puce
    - compromission ou de suspicion de compromission de sa clé privée
- Arrêter toute utilisation du certificat et de la clé privée associée, en cas d'arrêt d'activité de l'AC, ou de révocation du certificat de l'Autorité de Certification par la CDC.

La relation entre le Porteur et l'AC est formalisée par un engagement du Porteur défini dans les Conditions Générales d'Utilisation du certificat.

9.6.4 Utilisateurs de certificats

Les utilisateurs des certificats doivent :

- Vérifier l'usage pour lequel le certificat a été émis ;
- Vérifier que le certificat utilisé a bien été émis par l'AC CDC - LEGALIA ;
- Vérifier que le certificat du Porteur n'est pas présent dans les listes de révocation de l'AC CDC - LEGALIA ;
- Vérifier la signature du certificat du Porteur, et de la chaîne de certification, jusqu'à l'AC « CDC - RACINE » et contrôler la validité des certificats.

9.6.5 Autres participants

9.6.5.1 Mandataires de certification

Le Mandataire de Certification a le devoir de :

- Identifier le Porteur conformément aux exigences fixées dans la « convention AC – AE » [CONV AC AE] pour le métier concerné ;
- Garantir l'authenticité, le caractère complet et à jour des informations communiquées lors de la demande de certificat ainsi que des documents qui accompagnent ces informations ;
- Informer sans délai l'AE et l'AC de toute modification relative à ces informations et/ou documents ;
- Assurer l'information des Porteurs de certificat sur les Conditions Générales d'Utilisation des certificats, de la gestion des clés ou encore de l'équipement et des logiciels permettant de les utiliser ;
- Faire protéger la clé privée de chaque Porteur de certificat par des moyens appropriés à son environnement ;
- Faire protéger les données d'activation (code PIN) de chaque Porteur par des moyens appropriés à son environnement ;
- Faire respecter les Conditions Générales d'Utilisation de la clé privée et du certificat correspondant par chaque Porteur ;
- Faire demander la révocation d'un certificat dès lors qu'elle est nécessaire,
- Faire informer sans délai l'AE ou l'AC en cas de suspicion de compromission ou de compromission de la clé privée d'un de ses Porteurs de certificats.

9.7 Limite de garantie

Pas d'exigence particulière.

9.8 Limite de responsabilité

Sous réserve des dispositions d'ordre public applicables, la CDC ne pourra pas être tenue responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation, des LCR ainsi que de tout autre équipement ou logiciel mis à disposition.

La CDC décline en particulier sa responsabilité pour tout dommage résultant :

- d'un emploi des bi clés pour un usage autre que ceux prévus ;
- de l'usage de certificats révoqués ou expirés ;
- de l'absence de révocation d'un certificat entraînant l'utilisation du certificat et de la bi-clé par un tiers non autorisé ;
- d'un cas de force majeure tel que défini par les tribunaux français.

La CDC décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le Porteur ou le Mandataire de Certification.

9.9 Indemnités

Pas d'exigence particulière.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

Le présent document est applicable jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

Sauf événement exceptionnel lié à la sécurité, les évolutions du présent document n'imposent pas la révocation des certificats déjà émis.

9.10.3 Effets de la fin de validité et clauses restant applicables

Pas d'exigence particulière.

9.11 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, la CDC fera valider ce changement au travers d'une expertise technique, et analysera l'impact en terme de sécurité et de qualité de service offert.

Si nécessaire, une procédure exceptionnelle d'information sera réalisée pour notifier les composantes de l'AC des modifications à prendre en compte, avec un préavis raisonnable avant l'entrée en vigueur des modifications.

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

L'AC procède à toute modification des spécifications stipulées dans la PC et la DPC et/ou des Composantes de l'AC qui lui apparaissent nécessaires pour l'amélioration de la qualité des services de Certification et de la sécurité des processus. L'AC procède également à toute modification des spécifications stipulées dans la PC et la DPC et/ou des Composantes de l'AC qui est rendue nécessaire par une législation, réglementation en vigueur ou par les résultats des Contrôles. Le Responsable d'Application de l'AC CDC – LEGALIA est responsable de la procédure d'amendement de la Politique de Certification. La CDC s'engage à contrôler que tout changement apporté au présent document reste conforme aux objectifs de conformité aux exigences réglementaires associé au service fourni.

9.12.2 Mécanisme et période d'information sur les amendements

Toutes les composantes et acteurs de l'IGC sont tenus informés des amendements effectués sur la PC, et des impacts pour eux.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

Toute évolution majeure de la PC ayant un impact majeur sur les certificats déjà émis sera signifiée par une évolution de l'OID (cf. §1.2).

Dans l'hypothèse de modifications ultérieures sur ce document, le numéro d'OID sera modifié pour sa dernière valeur « Version », et deviendra 1.2.250.1.5.1.1.1.2.**3** pour l'usage « Authentification » , 1.2.250.1.5.1.1.1.3.**3** pour l'usage « Signature », à l'occasion de sa prochaine révision.

9.13 Dispositions concernant la résolution de conflits

En cas de litige découlant de l'interprétation ou de l'exécution de la présente Politique de Certification, les parties se réservent la faculté de rechercher une solution amiable. A défaut ou en cas d'échec de la tentative de conciliation, le différend pourra être soumis aux tribunaux compétents du ressort de la cour d'appel de Paris, nonobstant pluralité de défendeurs ou appel en garantie, même pour les procédures d'urgence ou les procédures conservatoires en référé ou par requête.

9.14 Juridictions compétentes

La présente Politique de Certification est soumise au droit français.
En matière contractuelle, tout litige relatif à la validité, l'interprétation, l'exécution de la présente Politique de Certification sera soumise aux tribunaux compétents du ressort de la cour d'appel de Paris.

9.15 Conformité aux législations et réglementations

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

9.16 Dispositions diverses

9.16.1 Accord global

Pas d'exigence particulière.

9.16.2 Transfert d'activités

Cf. chapitre §5.7.

9.16.3 Conséquences d'une clause non valide

Pas d'exigence particulière.

9.16.4 Application et renonciation

Pas d'exigence particulière.

9.16.5 Force Majeure

Sont considérés comme cas de force majeure de nature à suspendre les obligations de CDC aux termes de la présente politique de certification, outre ceux habituellement retenus par les tribunaux français, les conflits sociaux, intervention des autorités civiles ou militaires, catastrophes naturelles, incendies, dégâts des eaux, mauvais fonctionnement ou interruption du réseau de télécommunications externe.

9.17 Autres dispositions

Pas d'exigence particulière.

10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 Réglementation

Renvoi	Document
[RGS]	Référentiel Général de Sécurité Version 1.0
[DécretRGS]	décret n° 2010-112 du 2 février 2010
[RGS A_12]	Politique d'Horodatage Type version 2.3
[PCTYPE]	RGS_A_11 Politique de Certification Type "Authentification et Signature" version 2.3

10.2 Documents techniques

Renvoi	Document
[DPC]	CDC - LEGALIA - DPC authentification ou signature
[ROLES]	CDC - LEGALIA - Rôles et responsabilités
[CONV AC AE]	CDC - LEGALIA - Convention AC - AE - DRCI - DSB