



**Déclaration d'IGC**

**AUTORITE DE CERTIFICATION**

**« CDC - LEGALIA » AUTHENTIFICATION OU**

**SIGNATURE**

Version	Date	Description	Auteurs	Société
1.8	21/0/2017	Création en conformité eIDAS	Vincent COUILLET	Caisse des Dépôts

Classification du document	Référence
Diffusion public	OID : 1.2.250.1.5.1.1.1.2.3
	OID : 1.2.250.1.5.1.1.1.3.3

Ce document est la propriété exclusive de la Caisse des Dépôts et Consignations.  
Son usage est réservé à l'ensemble des personnes habilitées selon leur niveau de confidentialité.  
Sa reproduction est régie par le Code de la propriété intellectuelle qui ne l'autorise qu'à l'usage privé du copiste.



## SOMMAIRE

1. INTRODUCTION	3
2. POINT DE CONTACT	3
3. TYPE DE CERTIFICAT, PROCEDURE DE VALIDATION ET USAGE DES CERTIFICATS	4
4. LIMITES D'UTILISATION	4
5. OBLIGATIONS DES PORTEURS DE CERTIFICATS	4
6. OBLIGATIONS DES UTILISATEURS ET VERIFICATION DES CERTIFICATS	6
7. LIMITATIONS DE GARANTIES ET LIMITATIONS DE RESPONSABILITES	6
8. DOCUMENTS APPLICABLES	7
9. POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES	7
10. POLITIQUE DE REMBOURSEMENT	7
11. DROIT APPLICABLE	7
12. AUDIT DE CONFORMITE	8

## 1. INTRODUCTION

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.

Le présent document est la Déclaration d'IGC de l'AC CDC – LEGALIA (PKI Disclosure Statement). Le présent document ne peut se substituer à la PC/DPC de l'AC Legalia, qui définit l'ensemble des engagements et des pratiques de l'IGC pour des certificats Porteurs de type Entreprise et/ou Administration ayant un profil **Authentification** (OID 1.2.250.1.5.1.1.1.2.3) ou un profil **Signature** (OID 1.2.250.1.5.1.1.1.3.3). Le présent document a pour but, en conformité avec les règles applicables, de résumer les points principaux des pratiques de l'AC CDC – LEGALIA à destination des porteurs de certificats et des tiers.

## 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](mailto:igc@caissedesdepots.fr)

Pour contacter l'Autorité d'Enregistrement :

- Par courrier : Caisse des Dépôts – AE « CDC – LEGALIA » - DCB – 15, quai Anatole France – 75356 PARIS 07 SP
- Par courriel : [ae-dbr@caissedesdepots.fr](mailto: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.

### 3. TYPE DE CERTIFICAT, PROCEDURE DE VALIDATION ET USAGE DES CERTIFICATS

Famille de Certificat	Certificat public	OID	Description
<b>Signature électronique qualifiée</b>	<b>oui</b>	1.2.250.1.5.1.1.1.3.3	<b>Certificat de signature électronique qualifié au sens du Règlement Européen eIDAS et conforme à ETSI TS 319 411-2 QCP-n-QSCD. Certificats délivrés sur token matériel qualifié QSCD par l'ANSSI, avec création des clés sur le token par le CSP. Clés RSA de taille 2048 bit et validité du certificat de 3 ans. Usage de la clé limité à la signature électronique qualifiée.</b>
<b>Authentification NCP+</b>	<b>oui</b>	1.2.250.1.5.1.1.1.2.3	<b>Certificat d'authentification conforme à ETSI TS 319 411-1 NCP+ délivrés sur token matériel qualifié QSCD par l'ANSSI, avec création des clés sur le token par le CSP. Clés RSA de taille 2048 bit et validité du certificat de 3 ans. Usage de la clé limité à l'authentification.</b>

### 4. LIMITES D'UTILISATION

Tout autre usage que les usages décrits dans la PC/DPC et la section ci-dessus sont interdits.

Les certificats ne doivent pas être utilisés au-delà de leur période de validité

À des fins de conformité légales et réglementaires, les traces des opérations réalisées par CDC – LEGALIA sont conservées. En particulier :

- Les dossiers d'enregistrement sont conservés 10 ans.
- Les certificats et les informations sur le statut des certificats (CRL, OCSP) sont conservés au moins 8 ans après leur date d'expiration.
- Les traces techniques assurant l'imputabilité des actions sont conservées 7 ans après leur génération.

### 5. OBLIGATIONS DES PORTEURS DE CERTIFICATS

Les obligations des porteurs sont décrites dans le contrat de souscription ainsi que dans la PC/DPC. Nous les rappelons ci-dessous à titre indicatif (les obligations présentes dans le contrat de souscription et dans la PC/DPC faisant foi).

- L'ABONNE s'engage à se conformer aux procédures décrites dans le message électronique envoyé par L'AUTORITE DE CERTIFICATION pour le retrait du CERTIFICAT. Il s'engage à respecter les règles suivantes :
  - Protéger sa CLÉ USB ou sa CARTE A PUCÉ par le CODE PIN qu'il a lui-même défini lors du retrait de son CERTIFICAT.

- Ne pas confier à un tiers le CODE PIN, le prêter à un tiers ou laisser un tiers en prendre connaissance.
  - Modifier régulièrement le CODE PIN de son CERTIFICAT.
  - Garder secret le CODE PIN après son changement et protéger son CODE PIN de toute COMPROMISSION par perte, vol ou capture informatique. L'ABONNE s'engage à s'assurer de la sécurité du poste informatique sur lequel il utilise le CERTIFICAT.
  - Utiliser son CERTIFICAT dans le cadre des applications définies dans la Politique de Certification.
  - Informer sans délai L'AUTORITE DE CERTIFICATION en cas de COMPROMISSION avérée ou soupçonnée de sa clé privée ainsi que de toute altération, perte ou vol de sa CLÉ USB ou de sa CARTE A PUCE et demander immédiatement la REVOCATION DU CERTIFICAT en précisant le nom, prénom et adresse électronique de l'ABONNE concerné par l'incident.
  - Ne pas inscrire son CODE PIN sur quelque support physique que ce soit, notamment papier.
  - Effectuer les démarches conformément au Manuel d'utilisation qui lui a été transmis par email avec son code PIN.
  - Ranger sa CLÉ USB ou sa CARTE A PUCE après utilisation du CERTIFICAT de manière sécurisée afin d'éviter tout risque d'usurpation d'identité.
- L'ABONNE s'engage à respecter les prérequis techniques décrits en Annexe V du contrat.
  - L'ABONNE reconnaît être informé que, d'une façon générale, L'AUTORITE DE CERTIFICATION n'assure pas l'archivage des documents et messages signés à l'aide d'un CERTIFICAT émis par L'AUTORITE DE CERTIFICATION.
  - L'ABONNE s'engage à fournir toutes informations utiles lors de la création du CERTIFICAT et pendant toute la durée de validité du CERTIFICAT. Les informations fournies doivent être exactes et accompagnées des pièces justificatives prévues dans ce document.
  - L'ABONNE se charge d'informer le TIERS UTILISATEUR de l'obligation qui lui est faite de vérifier le CERTIFICAT et la SIGNATURE associée à l'échange, au message et au document électronique.
  - L'ABONNE est pleinement responsable de l'utilisation de sa CLÉ USB ou de sa CARTE A PUCE, de son CODE PIN. L'ABONNE reconnaît et accepte les opérations ainsi initiées et leurs caractéristiques dont la preuve est constituée par l'enregistrement électronique.
  - L'ABONNE s'engage à vérifier que la CLÉ USB ou la CARTE A PUCE sur laquelle il va utiliser son CERTIFICAT est agréée par L'AUTORITE DE CERTIFICATION.
  - L'ABONNE s'engage à n'utiliser son certificat que pour l'usage auquel il est destiné (Authentification ou Signature).
  - L'ABONNE s'engage à prendre toutes les mesures propres pour assurer la sécurité de la CLÉ USB ou de la CARTE A PUCE dont il a la garde.
  - En cas de dysfonctionnement du support de certificat électronique au moment de son initialisation, conformément aux dispositions du manuel d'utilisation AC - CDC LEGALIA ad hoc, l'ABONNE s'engage à prendre contact avec l'ASSISTANCE TECHNIQUE de L'AUTORITE DE CERTIFICATION dans les plus brefs délais.
  - Toute modification d'information signalée comme obligatoire lors de l'enregistrement doit être notifiée par écrit à L'AUTORITE DE CERTIFICATION et accompagnée des justificatifs requis.
  - L'ABONNE s'engage à ne plus utiliser un CERTIFICAT suite à l'expiration de celui-ci, suite à une demande de REVOCATION ou suite à la notification de la REVOCATION du CERTIFICAT, quelle qu'en soit la raison.
  - L'ABONNE s'engage à révoquer le CERTIFICAT, notamment si l'un des motifs suivants se réalise :

- Informations le concernant, figurant dans le CERTIFICAT, devenues inexactes (adresse mail, nom, etc).
- Changement de sa fonction rendant inutile l'usage du CERTIFICAT.
- Soupçon d'une utilisation frauduleuse.
- Non-respect des règles d'utilisation du CERTIFICAT, énoncées ci-dessus.

La demande de REVOCATION du CERTIFICAT sera effectuée par :

- En ligne à l'URL indiquée dans le contrat.
- Par écrit conformément au modèle fourni dans le formulaire « FORMULAIRE TYPE DE REVOCATION DE CERTIFICAT » téléchargeable sur le site <http://www.caissedesdepots.fr/confiance.html>.
- Par mail ou par téléphone auprès de l'AUTORITE D'ENREGISTREMENT

## **6. OBLIGATIONS DES UTILISATEURS ET VERIFICATION DES CERTIFICATS**

Les obligations des porteurs sont décrites dans le contrat de souscription ainsi que dans la PC/DPC. Nous les rappelons ci-dessous à titre indicatif (les obligations présentes dans le contrat de souscription et dans la PC/DPC faisant foi).

Les personnes ou entités auxquelles sont destinés les documents signés à l'aide d'un certificat produit dans le cadre du service

1. peuvent et doivent vérifier la validité de la signature électronique et du certificat ayant servi à créer cette signature, ainsi que l'ensemble des éléments de la chaîne de certification jusqu'au certificat racine. En particulier, ils doivent vérifier le statut de chacun des certificats de la chaîne et s'assurer qu'ils n'ont pas été révoqués.
2. Prendre en compte toutes les limitations, en particulier les limitations d'usage, tel que décrit dans les CGU annexées au contrat ainsi que dans la Politique de Certification /Déclaration des pratique de Certification associée, ainsi que, le cas échéant, toutes limitations contractuelles supplémentaires ayant fait l'objet d'un accord contractuel entre CDC –LEGALIA et l'utilisateur de certificat.

À cette fin, CDC – LEGALIA met publiquement à disposition de l'ensemble des utilisateurs de certificats l'ensemble des éléments (chaîne de certificat, CRL, liens vers les serveurs OCSP) permettant de vérifier la validité des certificats émis à l'adresse suivante :

<http://www.caissedesdepots.fr/confiance>

## **7. LIMITATIONS DE GARANTIES ET LIMITATIONS DE RESPONSABILITES**

Ces limitations sont exposées dans les CGUs annexées au contrat de souscription. Les principales limitations sont rappelées ici à titre indicatif :

- La CDC n'est pas responsable de la conservation ou de la protection de la clé privée de l'ABONNE, qui en est le seul responsable. En conséquence, tous les dommages liés à la COMPROMISSION de la clé privée d'un ABONNE sont à la charge du CLIENT.
- La CDC s'engage à tout mettre en œuvre pour que son site soit consultable à tout moment et que l'intégrité des informations utiles à la vérification soit protégée. La CDC se réserve cependant la faculté, sans que sa responsabilité ne puisse être engagée, de suspendre l'accès au dit site lorsqu'elle estime qu'un événement susceptible d'en affecter le

fonctionnement ou l'intégrité le nécessite et ce pour la durée nécessaire à l'intervention envisagée.

- En aucun cas la CDC n'intervient, de quelque façon que ce soit, dans les relations entre le CLIENT et les ABONNES détenteurs de CERTIFICATS, ou entre le CLIENT et les TIERS UTILISATEURS desdits CERTIFICATS.
- 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

## 8. DOCUMENTS APPLICABLES

Les documents applicables sont les suivants :

- PC/DPC de l'AC CDC - LEGALIA
- Contrat d'adhésion incluant les CGUs

Ces documents sont disponibles à l'adresse suivante.

<http://www.caissedesdepots.fr/confiance>

## 9. POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES

Les données à caractère personnel relatives au MANDATAIRE DE CERTIFICATION ou à l'ABONNE, transmises et détenues par la CDC, ne peuvent être divulguées sans avoir obtenu le consentement préalable de la personne concernée. Elles peuvent cependant être communiquées au sous-traitant ou à toute filiale de la CDC, dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978.

## 10. POLITIQUE DE REMBOURSEMENT

Pas d'exigences particulières.

## 11. DROIT APPLICABLE

Le présent service est soumis 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.

## 12. **AUDIT DE CONFORMITE**

L'autorité de Certification est auditée conformément aux normes ETSI EN 319 411-1 et ETSI EN 319 411-2 de façon régulière par un organisme d'évaluation indépendant accrédité (Voir Section 8 de la PC/DPC).