POLITIQUE DE CERTIFICATION

AUTORITE DE CERTIFICATION

« CDC RACINE »

Version	Date	Description	Auteurs	Société
1.0	08/03/2017	Politique de Certification	Alain BOUILLE	Caisse des Dépôts

Etat du document – Classification	Référence
Diffusion publique	OID : 1.2.250.1.5.1.1.1.1.2

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, clients et partenaires, 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, des partenaires et 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 - RACINE ».

Ce document a été établi sur la base de la Politique de Certification type de l'Etat (PRISv2.1).

1.2 Identification du document

Le numéro d'OID du présent document est **1.2.250.1.5.1.1.1.1.2.**

Le numéro d'OID de ce document répond aux principes de nommage suivant :

- 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 - RACINE v1.0 (**1**)
- Version (**1**)

Dans l'hypothèse de modifications ultérieures sur ce document, le numéro d'OID sera modifié pour sa dernière valeur « Version », et deviendra **1.2.250.1.5.1.1.1.1.3** à l'occasion de sa prochaine révision.

1.3 Entités intervenant dans l'IGC

L'AC « CDC - RACINE » gère exclusivement des certificats d'Autorités de Certification « Filles ».

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.

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 clé publique (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,
- Publication de la Liste des Certificats Révoqués (CRL),
- 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.

1.3.2 Autorité d'enregistrement

L'Autorité d'Enregistrement (AE) est responsable des fonctions qui lui sont déléguées par l'AC, en vertu de la Politique de Certification.

Pour l'AC « CDC - RACINE », l'AE assure les fonctions suivantes :

- Gestion des demandes de Certificats,
- Vérification de l'identité et de l'habilitation de la personne physique, le mandataire de certification, à demander la création du certificat de l'AC Fille, au titre de l'une de ses fonctions ou mandats,
- Vérification des demandes de révocation de Certificats.

1.3.3 Mandataire de certification

Le Mandataire de Certification est une personne physique, dûment identifiée, et désignée par et sous la responsabilité du Directeur Général de la Caisse des Depots, afin de le représenter pour effectuer une demande de création de certificats d'Autorité de Certification « fille ».

1.3.4 Porteurs de certificats

Les seuls porteurs de certificats émis par l'AC « CDC - RACINE » sont les entités à qui se rattachent les certificats des ACs Filles.

Les certificats d'ACs « Filles » sont sous la responsabilité d'entité appartenant au périmètre de la CDC.

Il n'y a pas véritablement de porteurs "personnes physiques" pour les AC « Filles ». Elles sont représentées par leur mandataire de certification.

1.3.5 Utilisateurs de certificats

Les utilisateurs de certificats sont l'ensemble des utilisateurs des AC "Filles", tel que défini dans les PCs respectives de ces ACs Filles.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

La présente politique de certification traite des bi clés et certificats des AC «Filles » de l'AC « CDC - RACINE ».

Ces certificats sont exclusivement utilisés pour la signature des certificats et des CRL gérés par les AC « Filles » de l'AC « CDC - RACINE ».

La liste des Key Usage de chaque AC Fille est limitée pour ne permettre à une AC Fille de ne générer qu'un seul type de certificat (soit certificat serveur, soit certificat individu, soit certificat AC « petite fille »).

1.4.2 Domaines d'utilisation interdits

Les certificats d'AC « Fille » ne peuvent pas être utilisés en dehors de la signature des certificats et des CRL des AC « Filles » de l'AC « CDC - RACINE ».

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.

1.5.2 Point de contact

Les demandes d'information ou commentaires sur cette Politique de Certification doivent être adressés à :

Responsable de l'Autorité de Certification
Direction des Risques Groupe
26 rue de Lille
75007 Paris
igc@caissedesdepots.fr

1.5.3 Entité déterminant la conformité d'une DPC avec ce document

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 la CDC.

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

2.1 Informations devant être publiées

Les informations publiées sont les suivantes :

- La présente politique de certification ;
- Les profils des certificats et CRL (cf. 7) ;
- La liste des certificats révoqués (CRL) ;
- Le certificat de l'Autorité de Certification « CDC - RACINE » ;
- L'empreinte du certificat de l'AC « CDC - RACINE ».

L'empreinte du certificat de l'AC « CDC - RACINE » est :
d65e4579ab82798afbf0038af7d4eb8bd1557bc99dade286bc08fb64b1cdbd7a

2.2 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.

2.2.1 Publication de la Politique de Certification

La présente PC est publiée sur le site : www.caissedesdepots.fr/confiance
La DPC n'est pas publiée.
Sous réserve d'acceptation, elle n'est consultable qu'aux fins de vérification de bonne application des procédures, sur demande adressée à :

Responsable du Service de Certification
Caisse des Dépôts
Direction des Risques et du Contrôle Interne
56 rue de Lille – 75 007 Paris
igc@caissedesdepots.fr

2.2.2 Publication du certificat d'AC

Le certificat de l'Autorité de Certification est publiée sur :
https://confiance.caissedesdepots.fr/igc/legalia/cdc-racine-eidas.cer

2.2.3 Publication de la CRL

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

et accessible à travers un service OCSP : http://igc-ocsp.caissedesdepots.fr/ocsp-racine/

Ces adresses sont également indiquées dans le Certificat du Porteur (dans les certificats des ACs Filles dans ce cas).

2.3 Délais et fréquences de publication

2.3.1 Fréquence de publication de la Politique de Certification

La politique de certification est revue à 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 48 heures.

2.3.2 Fréquence de publication du certificat d'AC

Le certificat d'AC est diffusé dans un délai maximum de 48 heures à l'issue de sa génération.

2.3.3 Fréquence de publication de la CRL

L'ARL est publiée tous les 9 mois et après chaque révocation.

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 CRL sont mis à disposition en lecture de manière internationale.

Les ajouts, suppressions et modifications sont limités aux personnes autorisées de l'AC.

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 « CDC - RACINE » (issuer) et « l'AC Fille » (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.

3.1.2 Nécessité d'utilisation de noms explicites

Les noms pour distinguer les porteurs sont explicites. Le nom distinctif est sous la forme d'une chaîne de type UTF8string de type nom X 501

3.1.3 Anonymisation ou pseudonymisation des porteurs

Sans objet.

3.1.4 Règles d'interprétation des différentes formes de noms

Sans objet.

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 ACs « Filles ».

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

La génération des bi clés des « ACs Filles » étant effectuée sous le contrôle de l'AC « CDC - RACINE », la preuve de possession de la clé privée est automatiquement acquise.

3.2.2 Validation de l'identité d'un porteur AC « Fille »

La validation de l'identité de la personne à l'origine de la demande de certificat d'AC est effectuée par l'AE, lors d'un face à face avec le mandataire de certification, et en préalable de la cérémonie des clés.

3.2.3 Informations non vérifiées du porteur

Sans objet

3.2.4 Validation de l'autorité du demandeur

L'AE s'assure que le mandataire de certification dispose des pouvoirs nécessaires pour effectuer cette demande. Cette vérification est effectuée lors du face à face entre l'AE et le mandataire de certification.

3.2.5 Contrôle de l'autorité du demandeur et approbation de la demande

Cf. ci-dessus.

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

Lorsqu'il s'agit de certificats d'AC, 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

Sans objet

3.3.2 Identification et validation pour un renouvellement après révocation

Sans objet

3.4 Identification et validation d'une demande de révocation

La révocation est effectuée par l'Autorité d'Enregistrement, qui valide ainsi la demande.

La demande de révocation de clé pour une AC « Fille », ne peut émaner que d'un mandataire de certification, et est validée lors d'un face à face avec l'Autorité d'Enregistrement.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Une demande de certificat pour une Autorité de Certification « Fille » émane du mandataire de certification

Cette demande doit être formulée par écrit, et avoir fait l'objet d'une vérification par l'AE, préalablement à la séance de cérémonie des clés.

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

La demande de certificat pour une « AC Fille » comporte dans tous les cas :

- Le type de population cible pour les certificats que devra émettre cette nouvelle Autorité de Certification ;
- Le type de certificats que devra émettre cette nouvelle Autorité de Certification (certificat individu, ou certificat serveur ou certificat d'AC);
- Les usages attendus de ces certificats (signature, authentification, chiffrement, signature de certificat, mixte…)
- Les nom, prénom et fonction du mandataire de certification ;
- Le nom demandé pour cette nouvelle Autorité de Certification ;
- La signature du mandataire de certification;
- La signature du DG de la CDC (ou la signature de la personne ayant délégation du DG pour signer ce type de demande).

4.2 Traitement d'une demande de certificat

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

L'Autorité d'Enregistrement exécute le processus d'identification du mandataire de certification, et valide sa demande.

L'AE vérifie l'Identité du Mandataire de Certification et la cohérence des justificatifs présentés. Elle s'assure de l'existence et de la validité des pouvoirs du Mandataire de Certification.

4.2.2 Acceptation ou rejet de la demande

La demande est acceptée ou rejetée préalablement à la réalisation de la cérémonie des clés.
En cas de rejet, l'AE en informe le Mandataire de Certification, en justifiant le rejet.

4.2.3 Durée d'établissement du certificat

Les certificats des AC « Filles » sont générés lors de la cérémonie des clés. Le délai entre la signature et l'installation du certificat de l'AC « CDC – RACINE » et des AC Filles est de quelques minutes.

Cette procédure est réalisée sous couvert des instances présentes à la cérémonie des clés et font l'objet d'une notification et d'une acceptation dans le script de cérémonie des clés.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

La génération des bi clés des AC « Filles » est consignée lors de la cérémonie des clés.

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

Cf. ci-dessus
Le mandataire de certification (ou son représentant) est présent lors de la cérémonie des clés.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

L'acceptation du certificat est réputée acquise à l'issue de la cérémonie des clés.

4.4.2 Publication du certificat

Les certificats d'AC « Fille » sont publiés sur le site internet http://www.caissedesdepots.fr/confiance, à une adresse indiquée dans leurs Politiques de Certification respectives.

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

Sans objet

4.5 Usage du bi-clé et du certificat

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

Pour les AC « Filles » de l'AC « CDC - RACINE », l'utilisation des clés privées est limitée :

- A la signature des certificats d'AC « Fille »;
- A la signature des CRL.

Cet usage est indiqué explicitement dans les extensions des certificats (cf 7).

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

Pour les certificats d'AC « Fille », les utilisateurs de ces certificats pourront vérifier leur révocation ou expiration en analysant le contenu de ces certificats, et la liste de révocation mise à disposition par l'Autorité de Certification « CDC - RACINE ».

4.6 Renouvellement d'un certificat

Pour l'AC « CDC - RACINE », 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.

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 Cause possible de changement de bi-clé

Les bi-clés émises pour les certificats d'AC filles, par l'AC « CDC - RACINE », ont une durée de vie de 10 ans.

La délivrance d'un nouveau certificat avant la fin de vie ne peut être que la conséquence d'une révocation, ou de la demande de renouvellement anticipée, pour garantir la continuité de service.

4.7.2 Origine d'une demande de nouveau certificat

Dans tous les cas, la procédure de demande de nouveau certificat est identique à la procédure de demande initiale.

4.7.3 Procédure de traitement d'une demande de nouveau certificat

Identique à la demande initiale.

4.7.4 Notification au porteur de l'établissement du nouveau certificat

Identique à la demande initiale.

4.7.5 Démarche d'acceptation du nouveau certificat

Identique à la demande initiale.

4.7.6 Publication du nouveau certificat

Identique à la demande initiale.

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

Identique à la demande initiale.

4.8 Modification du certificat

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

4.8.1 Cause possible 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

Les causes de révocation sont les suivantes :

- Compromission, suspicion de compromission, perte ou vol de clé privée ;
- Cessation de l'activité de l'AC « Fille » concernée ;
- Décision suite à un échec de contrôle de conformité ;
- Révocation de l'AC « CDC - RACINE ».

4.9.2 Origine d'une demande de révocation

Les personnes pouvant demander une révocation de certificat d'AC « Fille » sont les mandataires de certification, ayant eu l'autorisation de faire la demande d'origine pour cette AC « Fille » (ou son successeur dans ses fonctions).

4.9.3 Procédure de traitement d'une demande de révocation

Le traitement d'une demande de révocation est effectué par l'Autorité d'Enregistrement.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

La demande de révocation doit être formulée au plus tôt dès lors que le porteur ou son responsable a connaissance d'une cause effective de révocation.

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

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.

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

Les utilisateurs des certificats délivrés par l'AC « CDC - RACINE » doivent vérifier la chaîne de certification, et donc l'état du certificat de l'Autorité de Certification.

La méthode utilisée est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

4.9.7 Fréquence d'établissement des CRL

Les CRL sont établies et publiées sur Internet tous les 9 mois, et rendues publiques après toute révocation de certificat.

4.9.8 Délai maximum de publication d'une CRL

Les CRL sont rendues publiques et visibles de manière internationale dans un délai maximal de 24 heures.

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

Les systèmes de révocation et de vérification ont un taux de disponibilité de 99,5 pour cent, et respectent une durée maximum d'indisponibilité de 4 heures.

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

Sans objet

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 CRL sont publiées au format v2, accessibles sur Internet sous forme d'une liste visible de manière internationale pour tous.

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.

4.10.3 Dispositifs optionnels

Sans objet

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 de 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, génération des éléments secrets du porteur 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 oeuvre.

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 oeuvre 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 Exposition 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 oeuvre 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

Les supports recensés comme sensibles en termes de confidentialité font l'objet de mesures de destruction, ou peuvent être réutilisés dans un contexte opérationnel identique, pour un même niveau de sensibilité.

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 oeuvre 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.

5.2.2 Nombre de personnes requises par tâche

Toute tâche sensible est réalisée par trois membres du comité de pilotage au moins, chacun possédant une partie du secret.

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 oeuvre 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 dans leur description de poste.

5.2.4 Rôles exigeant une séparation des attributions

Tout rôle de confiance est dissocié et séparé de tout autre rôle de confiance.

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.

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 en matière de formation continue et fréquences des formations

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

Sans objet

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 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'événement 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, …).

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

La période de conservation des journaux d'événement est de :

- de un mois pour les événements systèmes ;
- de un an pour les événements techniques ;
- de 10 ans pour les événements fonctionnels.

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

Les procédures de sauvegarde des journaux sont quotidiennes par delta avec la sauvegarde précédente, et globale de manière hebdomadaire.

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.

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

5.5.1 Types de données à archiver

Les données de l'AC à archiver sont les suivantes :

- PC et DPC ;
- Certificats, et CRL publiés ;
- Dossiers d'enregistrement des porteurs, présentés par les mandataires de certification ;
- Journaux d'événements ;
- Logiciels exécutables et fichiers de configuration.

5.5.2 Période de conservation des archives

Les certificats et CRL sont archivés pendant 10 ans.

Les journaux d'événements sont archivés pendant 10 ans

5.5.3 Protection des archives

Quelque 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.

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 du Service de Certification.
La récupération et la vérification des archives peuvent être effectuées dans un délai de 10 ans.
Un délai d'une semaine est considéré comme acceptable, pour la restitution et la vérification des archives.

5.6 Changement de clés d'AC

La durée de vie des clés de l'AC « CDC - RACINE » est de 20 ans.
La durée de vie des clés d'une l'AC « Fille » est de 10 ans.

5.7 Reprise suite à compromission et sinistre

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

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

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 révocation du certificat, si elle s'avère nécessaire, est effectuée dans la plus grande urgence par tout moyen nécessaire.

5.7.2 Procédure 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

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

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 prend les mesures suivantes :

- 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.

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

5.8.2 Cessation d'activité affectant l'activité de 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.

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

- 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.

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 de bi clé

Les clés de l'AC « CDC - RACINE » et des AC « Fille » sont générées lors de la cérémonie des clés, en présence du comité de pilotage de l'AC « CDC - RACINE », 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.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet

6.1.3 Transmission de clé publique à l'AC

Sans objet, les clés sont générées par l'AC.

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

2048 bits pour la taille des clés de l'AC « CDC - RACINE »
2048 bits pour la taille des clés des AC « Fille »

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

Cf section 7

6.1.7 Objectifs d'usages de la clé

L'utilisation de la clé privée pour l'AC « CDC - RACINE », et du certificat associé est limitée à la signature de certificats d'AC Fille, et de CRL.

La clé privée d'AC n'est utilisée que dans un environnement sécurisé, au sein d'un boîtier cryptographique matériel (HSM).

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

Le module cryptographique de l'AC pour la génération et la mise en oeuvre des clés de signature répond aux exigences énoncées par la réglementation, au sein de la documentation PRISv2.1.

Il s'agit d'un boîtier cryptographique matériel, 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

6.2.2 Contrôle des clés privées par plusieurs personnes

Le contrôle de la clé privée de l'AC « CDC - RACINE », et des clés privés des « AC Filles » est effectué par au moins trois membres du comité de pilotage, qui sont présents simultanément pour rendre l'usage de ces clés possibles.

6.2.3 Séquestre de la clé privée

La clé privée de l'AC « CDC - RACINE », et les clés privées des « AC Filles » ne font pas l'objet de séquestre.

6.2.4 Copie de secours de la clé privée

La clé privée de l'AC « CDC - RACINE », et des clés privées des « AC Filles » font l'objet de copie de secours. Ces copies de secours bénéficient du même sécurité que la clé privée originale.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC «CDC - RACINE», et les clés privées des « AC Filles » 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 des clés privées de l'AC « CDC - RACINE », et des clés privés des « AC Filles » puisqu'elles sont générées et stockées 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).

6.2.7 Stockage de la clé privée dans le module cryptographique

Le stockage de la clé privée de l'AC « CDC - RACINE », et des clés privés des « AC Filles » est réalisé par le boîtier cryptographique dans les conditions de sécurité définies par le profil de protection support à l'évaluation EAL 4+.

6.2.8 Méthode d'activation de la clé privée

L'activation de la clé privée de l'AC « CDC - RACINE », et des clés privés des « AC Filles » nécessite la présence de trois membres du comité de pilotage au moins.

6.2.9 Méthode de désactivation de la clé privée

La clé privée de l'AC « CDC - RACINE », et des clés privés des « AC Filles » est désactivable à partir du module cryptographique. Cette désactivation nécessite la présence de trois membres du comité de pilotage au moins.

6.2.10 Méthode de destruction des clés privées

La destruction de la clé privée de l'AC « CDC - RACINE », et des clés privés des « AC Filles » ne peut être effectuée qu'à partir du module cryptographique.

6.2.11 Niveau d'évaluation sécurité du module cryptographique

Les modules cryptographiques de l'AC « CDC - RACINE », et des clés privés des « AC Filles » 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 - RACINE », et des « AC Filles » 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 - RACINE » ont une durée de vie de 12 ans.
Les clés de signature et les certificats de l'AC « Filles » ont une durée de vie de 10 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Les éléments nécessaires à l'activation de la clé privée de l'AC «CDC - RACINE», et des clés privés des « AC Filles », sont générées de manière sécurisée, et uniquement accessibles aux membres du comité de pilotage, seuls autorisés à procéder à cette activation.

6.4.2 Protection des données d'activation

Les données d'activation des clés d'AC ne sont délivrées qu'aux membres du comité de pilotage.

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 et de désenregistrement des utilisateurs.

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 font 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 oeuvre 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 oeuvre 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 Jounalisation 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 oeuvre.

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Sans objet, sauf pour le boîtier cryptographique HSM, qui est évalué EAL4+.

6.6 Mesures de sécurité liées au développement des systèmes

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

Sans objet

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.

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 composant 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 CRL

7.1 Profils des certificats

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

7.1.1 Certificat de l'AC « CDC - RACINE »

Le certificat de l'AC « CDC - RACINE » contient les informations suivantes.

7.1.1.1 Champs de base

Certificat de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer DN	C = FR O = CAISSE DES DEPOTS ET CONSIGNATIONS 2.5.4.97 = SI:FR-180020026 OU = 0002 180020026 CN = CDC - RACINE
Subject DN	C = FR O = CAISSE DES DEPOTS ET CONSIGNATIONS 2.5.4.97 = SI:FR-180020026 OU = 0002 180020026 CN = CDC - RACINE
NotBefore	YYMMDD000000Z
NotAfter	YYMMDD235959Z (20 ans)
Public Key Algorithm	rsaEncryption
Signature Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Parameters	NULL

7.1.1.2 Extensions de certificat

Extensions standards	OID	Inclure	Critique	Valeur
Authority Info Access	(1.3.6.1.5.5.7.1.1)			n/a
Authority Key Identifier	{id-ce 35}	**X**	**FALSE**	
Basic Constraint	{id-ce 19}	**X**	**TRUE**	
CA				**Set**
Maximum Path Length				**none**
Certificate Policies	{id-ce 32}	**X**	**FALSE**	
policyIdentifiers				**2.5.29.32.0** (anyPolicy)
policyQualifiers				n/a
CPSpointer				n/a
OID				n/a
value				http://iqc-pc.caissedesdepots.fr/pc-racine.pdf
User Notice				n/a
OID				n/a
value				n/a
noticeRef				n/a
organization				n/a

noticeNumbers				n/a
explicitText				n/a
CRL Distribution Points	{id-ce 31}			n/a
distributionPoint				n/a
reasons				n/a
cRLIssuer				n/a
Extended Key Usage	{id-ce 37}			n/a
Issuer Alternative Name	{id-ce 18}			n/a
Key Usage	{id-ce 15}	**X**	**TRUE**	
Digital Signature				**Clear**
Non Repudiation				**Clear**
Key Encipherment				**Clear**
Data Encipherment				**Clear**
Key Agreement				**Clear**
Key CertSign				**Set**
Key CRL Sign				**Set**
Private Key Usage Period	{id-ce 16}			n/a
Subject Alternative Name	{id-ce 17}			n/a
Subject Key Identifier	{id-ce 14}	**X**	**FALSE**	
Methods of generating key ID				**Methode 1 SHA-1 de la valeur binaire du champ SubjectPublicKey du certificat**
Other Extensions				

7.1.2 Certificat des AC « Filles »

Les certificats des AC « Filles » contiendront les informations suivantes.

7.1.2.1 Champs de base

Certificat de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil
Issuer DN	C = FR O = CAISSE DES DEPOTS ET CONSIGNATIONS 2.5.4.97 = SI:FR-180020026 OU = 0002 180020026 CN = CDC - RACINE
Subject DN	C = FR O = CAISSE DES DEPOTS ET CONSIGNATIONS 2.5.4.97 = SI:FR-180020026 OU = 0002 180020026 CN = < AC Fille >
NotBefore	YYMMDD000000Z
NotAfter	YYMMDD235959Z (10 ans)
Public Key Algorithm	rsaEncryption
Signature Algorithm	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Parameters	NULL

7.1.2.2 Extensions de certificat

Les extensions de certificats des AC Filles sont définies pour chaque AC Fille et spécifiées dans leur Politique de Certification respective.

7.2 Profil des listes de certificats révoqués

Les CRL émises présentent les caractéristiques suivantes :

Durée et fréquence de mise à jour :
CRL :
Durée de validité : 7 jours
Périodicité de mise à jour : 24 heures

ARL :
Durée de validité : 12 mois
Périodicité de mise à jour : 9 mois ou après chaque révocation

Informations et principes de base :
La version de la CRL est v2.
L'émetteur de la liste de révocation a comme DN le nom de l'Autorité de Certification signataire de cette CRL.
Les certificats révoqués sont listés.
Les certificats sont nommés par leur numéro de série.
La date de révocation est précisée.
Les certificats révoqués contiendront la valeur « unspecified » pour la raison de révocation.

Extensions :
Les extensions Numéro de la CRL & Autorithy Key Identifier seront présentes.

Lieux de publication :
URL http de publication : http://igc-crl.caissedesdepots.fr/cdc/racine-eidas.crl

7.3 Profil OCSP

Le service OCSP est opéré par l'Opérateur de Service de Certification de l'AC. Il est accessible à travers l'adresse :

http://igc-ocsp.caissedesdepots.fr/ocsp-racine/

7.3.1 Numéro de version

Sans objet

7.3.2 Extensions OCSP

Sans objet.

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.

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 oeuvre et détecter les cas de non conformités qui pourraient compromettre la sécurité du service offert.

8.3 Relations entre évaluateurs et entités évaluées

Le contrôleur est désigné par l'AC. Il devra être indépendant de l'AC, de l'AE.

8.4 Périmètre des évaluations

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

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

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. 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.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

Les certificats sont émis par la Caisse des Dépôts (CDC), qui se réservent le droit d'en facturer la délivrance.

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.

9.2.2 Autres ressources

La CDC reconnaît disposer d'une garantie financière suffisante spécialement affectée à la couverture des risques financiers.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Pas d'exigence spécifique.

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 procéde 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 l'AC «CDC - RACINE», et des « AC Filles » ;
- Les données d'activation ;
- 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

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

La CDC s'engage à traiter les informations confidentielles recueillies dans le respect des lois et règlements en vigueur.

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.

9.4.2 Informations à caractère personnel

Sans objet

9.4.3 Informations à caractère non personnel

Pas d'exigence spécifique.

9.4.4 Responsabilité en terme de protection des données personnelles

Sans objet

9.4.5 Notification et consentement d'utilisation des données personnelles

Sans objet

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 à la certification en justice.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Pas d'exigence spécifique.

9.5 Droits sur la propriété intellectuelle et industrielle

La fourniture de service par la CDC ne saurait être interprétée comme entraînant la cession d'un quelconque droit de propriété intellectuelle.

9.6 Interprétations contractuelles et garanties

9.6.1 Autorités de certification

La CDC est responsable :

- 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 du non-respect du présent document par elle-même ou l'une des entités de l'IGC.

Sauf à démontrer qu'il n'a commis aucune faute intentionnelle ou de négligence, la CDC est responsable de tout préjudice causé à toute personne physique ou morale qu'y 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.
Enfin, la CDC engage sa responsabilité en cas de faute ou de négligence dans les précautions à prendre en terme de confidentialité des données personnelles qui lui sont confiées par les mandataires de certification.

9.6.2 Autorité d'enregistrement

Cf. ci-dessus

9.6.3 Mandataires de certification

Le mandataire de certification a le devoir de :

- Communiquer des informations exactes et à jour lors de sa demande ou du renouvellement du certificat
- Informer l'AC de toute modification des informations contenues dans son certificat
- Faire sans délai une demande de révocation auprès de l'AC en cas de perte, de compromission ou de suspicion de compromission d'une clé privée
- Interrompre immédiatement et définitivement l'usage des clés privées en cas de compromission

9.6.4 Utilisateurs de certificats

Les utilisateurs des certificats doivent :

- Vérifier l'usage pour lequel le certificat a été émis
- Contrôler que le certificat émis par l'AC est adapté au niveau de sécurité et pour le service de confiance requis par l'application
- Vérifier la signature du certificat du porteur jusqu'à l'AC « CDC - RACINE » et contrôler la validité des certificats

9.6.5 Autres participants

Pas d'exigence particulière

9.7 Limite de garantie

Sans objet

9.8 Limite de responsabilité

La CDC ne pourra pas être tenu pour responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation, des CRL 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 ;
- d'un cas de force majeur 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 mandataire de certification.

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

9.9 Indemnités

Sans objet

9.10 Durée et fin anticipée de 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

Sans objet

9.11 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, 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 du service de Certification, 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).

9.13 Dispositions concernant la résolution de conflits

Conformément aux textes législatifs et à la réglementation en vigueur, les certificats émis en vertu de la présente Politique Certification sont des certificats dont les conditions d'utilisation sont définies par la présente Politique Certification et par les conditions générales d'utilisation qui définissent les relations entre l'IGC de la CDC, et ses utilisateurs.

Les relations entre la CDC et le porteur du certificat sont régies par les conditions générales d'utilisation du certificat.

9.14 Juridictions compétentes

La présente Politique de Certification est soumise au droit français.
Tout litige relatif à la validité, l'interprétation, l'exécution de la présente Politique de Certification sera soumis aux tribunaux compétents 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 spécifique

9.16.2 Transfert d'activités

Cf. chapitre 5.7

9.16.3 Conséquences d'une clause non valide

Pas d'exigence spécifique

9.16.4 Application et renonciation

Pas d'exigence spécifique

9.16.5 Force majeure

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

9.17 Autres dispositions

Sans objet

10 GLOSSAIRE

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

Autorité de certification
Entité responsable de l'émission, de la délivrance et de la gestion des certificats électroniques. L'Autorité de Certification est responsable des certificats émis en son nom.

Autorité d'Enregistrement
Entité responsable de l'identification et de l'authentification des demandeurs de certificats électroniques au profit d'une AC.

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 oeuvre de techniques cryptologiques basées sur des algorithmes asymétriques.

Certificat
Clé publique d'un utilisateur, concaténée à d'autres informations rendues infalsifiables par signature avec la clé privée de l'autorité de certification qui l'a délivré.

Certificat d'AC
Certificat d'une autorité de certification.

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.

Code d'activation
Données privées associées à un porteur permettant d'initialiser ses éléments secrets.

Code de retrait
Données permettant d'identifier une demande d'un porteur sur l'AC.

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

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

Infrastructure de Gestion de Clés (IGC)
Ensemble de composantes fournissant des services de gestion de clés et de certificats au profit d'une communauté d'utilisateurs.

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

Mandataire de certification
Le Mandataire de Certification est une personne physique, dûment identifiée, désignée par et sous la responsabilité du responsable de l'Autorité de Certification, afin de la représenter lors de la réalisation des demandes de certificats.

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

Politique de certification (PC)
Ensemble de règles relative à l'applicabilité d'un certificat à une communauté et / ou à une classe d'applications ayant des besoins de sécurité communs.

Porteurs de certificat
Individu ou composant technique pour lequel est émis un certificat, et ayant connaissance des données d'activation de la clé privée associée.

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.

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.

Utilisateur de certificat
Toute entité qui utilise le Certificat d'un Porteur de Certificat, en particulier pour s'assurer de l'authenticité d'une signature numérique ou chiffrer des données.

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

Vérification de signature
Opération de contrôle d'une signature numérique.