POLITIQUE DE CERTIFICATION

AUTORITE DE CERTIFICATION CDC - ESSELIA

Version	Date	Description	Auteurs	Société
1.0	28/05/2010	Politique de Certification	Alain BOUILLE	Caisse des Dépôts

Etat du document – Classification	Référence
Diffusion publique	OID : 1.2.250.1.5.1.1.1.6.1

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 « AC CDC - RACINE ».

L'ensemble constitue une hiérarchie de certification.

La présente Politique de Certification définit les exigences relatives à l'AC « CDC - ESSELIA » pour des certificats serveurs, avec les profils suivants :

- Authentification Serveur
- Authentification Client
- Cachet Serveur
- Cachet Horodatage
- Répondeur OCSP
- Signature de code

Les spécificités de chaque profil sont clairement explicitées dans la présente Politique de Certification.

Ce document a été établi sur la base des Politiques de Certification types de l'Etat (v2.3), sans objectif de qualification selon le Référentiel Général de Sécurité (RGS).

1.2 Identification du document

Le numéro d'OID du présent document est **1.2.250.1.5.1.1.1.6.1**.

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 - ESSELIA v1.0 (**6**)
- Version (**1**)

Dans l'hypothèse de modifications ultérieures sur ce document, le numéro d'OID sera modifié pour sa dernière valeur « Version », et deviendra 1.2.250.1.5.1.1.1.6.**2** à l'occasion de sa prochaine révision.

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 demandes de certificats,
- Emission des certificats,
- Gestion des certificats,
- Publication de la Liste des Certificats Révoqués (LCR),
- 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 de la gestion du cycle de vie des certificats. Elle valide les demandes de certificats. Elle est garante du lien entre le serveur et le certificat qu'elle lui délivre.

Les acteurs de l'AE sont les Opérateurs d'Enregistrement. Ils sont nommés par le Responsable d'Application. Ils assurent le fonctionnement de l'AE : à ce titre ils sont en charge de la gestion du cycle de vie des certificats de l'Autorité de Certification, sur le périmètre de l'AE.

Les acteurs de l'AE sont authentifiés par certificat lors de l'accès aux interfaces de l'Autorité d'Enregistrement. A cet effet, ils doivent faire une demande de certificat de l'AC CDC – FIDELIA – Authentification.

L'AE assure les fonctions suivantes :

- Gestion des demandes de certificats ;
- Validation des demandes d'enregistrement ;
- Validation des demandes de révocation de certificats ;
- Participation au renouvellement des certificats ;
- Déclenchement des fonctions et procédures d'archivage des données ;
- Support niveau 2 pour les Responsables techniques.

L'AE est opérée par le Responsable d'Application de l'AC « CDC - ESSELIA».

1.3.3 Responsables techniques

Dans le cadre de la présente Politique de Certification, le rôle de « Responsable technique » correspond aux rôles définis dans les PC Types V2.3 du RGS sous le nom de « Responsables du Certificat d'Authentification Serveur » (RCAS) ou de « Responsables du Certificat de Cachet » (RCC).

Un certificat serveur est sous la responsabilité d'un « Responsable technique », personne physique qui se porte garante du lien entre la ressource serveur et la bi-clé.

Le Responsable technique est également responsable de l'utilisation de ce certificat vis-à-vis de l'organisation dont le serveur fait partie. Le Responsable technique a un lien contractuel avec l'organisation du serveur.

Le Responsable technique respecte les obligations le concernant : elles sont décrites dans la présente Politique de Certification.

En cas de départ ou de changement de fonction d'un Responsable technique, le certificat serveur devra être géré par un nouveau Responsable technique.

L'Autorité d'Enregistrement se porte garante du fait qu'un certificat serveur soit toujours placé sous la responsabilité d'un Responsable technique.

1.3.4 Utilisateurs de certificats

Les utilisateurs de certificats sont les personnes physiques ou les services techniques qui exploitent les certificats de l'AC CDC - ESSELIA.
Plus précisément :

- Pour les certificats du **profil « Authentification Serveur »**
  - Personnes physiques qui vérifient l'authenticité d'une ressource serveur lors de l'accès à cette ressource.
  - Service technique qui authentifie un composant dans le cadre d'une communication sécurisée (protocole SSL).
- Pour les certificats du **profil « Authentification Client »**
  - Service technique qui prouve son authenticité à un composant dans le cadre d'une communication sécurisée (protocole SSL).
- Pour les certificats du **profil « Cachet Serveur »**
  - Service technique qui vérifie la validité d'une signature serveur.
- Pour les certificats du **profil « Cachet Horodatage »**
  - Service technique qui vérifie la fiabilité d'une date.
- Pour les certificats du **profil « Répondeur OCSP »**
  - Service technique qui valide un certificat.
- Pour les certificats du **profil « Signature de code »**
  - Service technique qui vérifie l'authenticité d'un logiciel ou programme exécutable.

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 L'Opérateur de Service de Certification

L'OSC a la responsabilité d'opérer un service de certification gérant l'ensemble du cycle de vie des Certificats, conformément aux PC. Dans le cadre de la CDC, l'Opérateur technique est Keynectis, piloté par INFORMATIQUE CDC (iCDC) en délégation de l'AC. Un contrat est établi entre la Caisse des Dépôts, INFORMATIQUE CDC et Keynectis pour la fourniture technique du service de certification.

Le personnel de l'OSC peut être amené à utiliser des certificats à des fins d'authentification ou de signature sur les composantes qu'il maîtrise. Dans ce cas d'application, nous parlerons de certificats des composantes de l'OSC et les procédures de gestion de ces certificats sont décrites dans les politiques de certification afférentes.

1.3.5.3 Mandataire de certification

Dans le cadre de cette Politique de Certification, il n'est pas mis en place d'organisation utilisant des Mandataires de Certification.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats des serveurs

Les certificats émis par l'AC « CDC - ESSELIA » sont utilisables exclusivement pour des opérations réalisées par les Utilisateurs de certificats tels que définis au paragraphe 1.3.4. Ces opérations sont les suivantes :

- Pour les certificats du **profil « Authentification Serveur »**
  - Authentification du serveur dans le cadre du protocole SSL
- Pour les certificats du **profil « Authentification Client »**
  - Authentification du client dans le cadre du protocole SSL
- Pour les certificats du **profil « Cachet Serveur »**
  - Signature électronique au nom d'une personne morale.
- Pour les certificats du **profil « Cachet Horodatage »**
  - Horodatage.
- Pour les certificats du **profil « Répondeur OCSP »**
  - Signature des réponses OCSP.
- Pour les certificats du **profil « Signature de code »**
  - Signature d'un logiciel ou d'un programme exécutable.

Tout autre usage est effectué sous la seule responsabilité du Responsable technique en charge du certificat serveur.

L'AC « CDC - ESSELIA » n'émet pas de certificats pour d'autres populations et pour d'autres usages.

Les bi-clés associées aux certificats serveurs sont au format :

- Soit matériel (bi-clé protégée dans un HSM).
- Soit logiciel (bi-clé conservée dans un fichier au niveau du serveur).

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

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

- Signer des certificats serveurs.
- Signer des LCR.

1.4.2 Domaines d'utilisation interdits

Les certificats de la présente PC ne peuvent pas être utilisés en dehors des opérations listées au paragraphe 1.4.1 et 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 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 commentaires sur cette Politique de Certification doivent être adressés à :

Responsable de l'Autorité de Certification
Caisse des Dépôts
Direction du Risque et du Contrôle Interne
56 rue de Lille – 75 007 PARIS
igc@caissedesdepots.fr

Les questions à l'Autorité d'Enregistrement doivent être envoyées à l'adresse email suivante : AE-SSL@caissedesdepots.fr

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*
CSR	*Certificate Signing Request*
DGME	Direction Générale de la Modernisation de l'Etat
DN	*Distinguished Name*

DPC	Déclaration des Pratiques de Certification
ETSI	*European Telecommunications Standards Institute*
FQDN	*Fully Qualified Domain Name*
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
RCAS	Responsable du Certificat d'Authentification Serveur
RCC	Responsable du Certificat de Cachet
RSA	Rivest Shamir Adelman
RSSI	Responsable de la Sécurité du Système d'Information
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	*Transport Layer Security*
SSCD	*Signature Secure Creation Device*
URL	*Uniform Resource Locator*

1.6.2 Définitions

Applicatif de vérification d'authentification – Il s'agit de l'application mise en œuvre par l'utilisateur ou le serveur pour vérifier l'authentification d'un autre serveur et établir une session sécurisée avec ce serveur, notamment générer la clé symétrique de session et la chiffrer avec la clé publique du serveur contenue dans le certificat correspondant.

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.

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. 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 (AE) - Cette fonction vérifie les informations d'identification du futur Porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction 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 - 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 Type, le terme "certificat électronique" désigne uniquement un certificat délivré à un serveur informatique sous la responsabilité d'un RCAS et portant sur une bi-clé d'authentification et d'échange de clés symétriques de session, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

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.

Client : entité bénéficiaire de l'IGC. Cette entité s'appuie sur l'IGC de la CDC et une ou plusieurs AE Déléguées pour couvrir ses besoins de certificats, pour des usages et des populations de porteurs donnés, qui sont dans son périmètre de responsabilité.

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.

CSR (*Certificate Signing Request*) – message au format PKCS#10 qui permet d'adresser à l'Autorité de Certification une requête de création de certificat et signature de ce certificat, sur la base d'une clé publique préalablement générée.

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 de protection des clés privées – Il s'agit du dispositif matériel et/ou logiciel utilisé par le serveur pour stocker et mettre en œuvre sa clé privée.

Fenêtre de renouvellement – période de temps pendant laquelle un certificat peut être renouvelé. Elle démarre quelques mois avant la date d'expiration du certificat et peut se terminer après 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).

FQDN (*Fully Qualified Domain Name*) – nom de domaine complet d'un serveur l'identifiant de manière unique.

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).

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). Le rôle de mandataire de certification n'est pas utilisé par l'AC CDC – ESSELIA.

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.

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.

OCSP (*Online Certificate Status Protocol*) – protocole de vérification en ligne de certificat, défini dans la RFC 2560. Ce protocole permet de vérifier si un certificat est révoqué ou non, de manière alternative à la consultation d'une LCR. Les réponses retournées par le répondeur OCSP à l'émetteur d'une requête OCSP sont signées.

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, 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.

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.

Responsable du Certificat d'Authentification Serveur (RCAS) - Cf. chapitre 1.3.3.

Responsable du Certificat de Cachet (RCC) - Cf. chapitre 1.3.3.

Responsable d'Application de l'AC « CDC – ESSELIA » - 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.

Responsable technique - Cf. chapitre 1.3.3.

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.

Serveur informatique - Il s'agit d'un service applicatif (disposant d'un certificat fourni par l'AC), rattachés à l'entité (identifiée dans le certificat). Ce service est hébergé sur un ou plusieurs serveurs physiques rattachés à un même nom de domaine (FQDN).

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.

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 serveur.

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.

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 d'Application de l'AC « CDC – ESSELIA ».

2.2 Informations devant être publiées

L'AC « CDC - ESSELIA » publie la présente Politique de Certification.

L'OSC publie les éléments suivants :

- Les profils des certificats et LCR (cf. 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 - ESSELIA » et de l'AC Racine ;
- L'empreinte du certificat de l'AC « CDC - ESSELIA ».

L'empreinte du certificat de l'AC « CDC - ESSELIA » est 5d5347c3d35763e06051adb9ace0192896f18a6960bbcc5952322f4502cf5904

2.2.1 Publication de la Politique de Certification

La présente PC est publiée sur le site :
http://igc-pc.caissedesdepots.fr/pc-esselia.pdf

2.2.2 Publication du certificat d'AC

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

- Pour l'AC CDC – RACINE : http://www.caissedesdepots.fr/uploads/media/cdc-racine.crt
- Pour l'AC CDC – ESSELIA : http://www.caissedesdepots.fr/uploads/media/cdc-esselia.crt

2.2.3 Publication de la LCR

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

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

Ces adresses sont également indiquées dans les certificats serveurs.

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 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 24 heures.

Le statut des certificats est accessible via la LCR et via un service OCSP.

2.3.4 Disponibilité des informations publiées

Le service de certification électronique de l'OSC est accessible 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.

Ces dispositions, et cette garantie de service, sont assurées par l'OSC et elles constituent des obligations contractuelles de l'OSC vis-à-vis de l'AC.

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 serveur (*subject*) sont identifiés par un « *Distinguished Name* » (DN) de type X.520 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.520 ».

3.1.2 Nécessité d'utilisation de noms explicites

Les noms pour distinguer les serveurs contiennent les informations nécessaires et explicites permettant d'identifier les serveurs, présentes dans le champ « Subject - DN » du certificat.

Ces informations sont recueillies par l'Autorité d'Enregistrement lors de la phase d'enregistrement.

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 dont fait partie le serveur ;
- Champ O (*OrganizationName*) : la raison sociale de l'organisation dont fait partie le serveur, tel que figurant au K-Bis ;
- Champ OU (*Organization Unit*) : le numéro de SIREN ou SIRET de l'organisation du serveur (composé de neuf ou quatorze chiffres précédés de 0002);
- Champ CN (Common Name) :
  - Pour les certificats de **profils SSL serveur** ou **SSL client** : le FQDN du serveur.
  - Pour les **autres profils**, un nom explicite correspondant à un service applicatif.
    Le format du CN est une expression régulière (saisie libre). Les minuscules, le tiret - et les chiffres sont autorisés. Les caractères spéciaux saisissables au clavier sont interdits, par exemple =%^\|[]£@'^<,. «»{}µ+-~¡^°!"#$%&/()=?*{};:_>

Exemple, pour un serveur au sein de l'organisation d'INFORMATIQUE CDC dont le FQDN est myserver.domain.com, le DN du certificat SSL serveur est le suivant :
DN = {C=FR, O=INFORMATIQUE CDC, OU=0002 775665433, CN=myserver.domain.com}

3.1.3 Anonymisation ou pseudonymisation de serveurs

Les certificats objets de la présente PC ne peuvent en aucun cas être anonymes. Les pseudonymes ne sont pas acceptés. En particulier les certificats de type *Wild Card* ne sont pas acceptés.

3.1.4 Règles d'interprétation des différentes formes de noms

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

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 serveurs.

La clé d'unicité d'un certificat serveur au sein de l'AC CDC – ESSELIA est la combinaison du champ DN (*Distinguished Name*) et du *KeyUsage*.

La prise en compte du *KeyUsage* dans la clé d'unicité garantit la différenciation entre les certificats de profils différents éventuellement détenus par un même serveur.

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 serveur avant de certifier la clé publique.

En effet, lors du processus de demande de certificat, le Responsable technique génère une bi-clé pour le serveur et au niveau du serveur. Puis le Responsable technique crée une CSR. La CSR respecte le format standard PKCS#10 qui prouve la possession de la clé privée correspondant à la clé publique contenue dans la 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

Remarque : l'Autorité de Certification CDC – ESSELIA ne s'appuie pas sur le rôle de Mandataire de Certification.

3.2.3.1 Enregistrement d'un Responsable technique sans MC pour un certificat serveur à émettre

Le Responsable technique se déclare responsable du certificat serveur au moment de la demande. Il fournit son adresse email.
L'Autorité d'Enregistrement vérifie que les fonctions du demandeur sont compatibles avec le rôle de Responsable technique.

- Si c'est le cas, l'AE traite la demande comme décrit au paragraphe 4.2.
- Sinon, l'Autorité d'Enregistrement refuse la demande.

3.2.3.2 Enregistrement d'un nouveau Responsable technique sans MC pour un certificat serveur déjà émis

Lors du prochain événement relatif au cycle de vie du certificat, le Responsable technique ainsi que l'Autorité d'Enregistrement seront notifiés.

L'Autorité d'Enregistrement surveille que le Responsable technique enregistré lors de la première demande, ou un nouveau Responsable technique prend en charge l'action concernant le serveur.
Dans ce cas, le nouveau Responsable technique fournira son adresse email à l'AE.

3.2.3.3 Enregistrement d'un Mandataire de Certification

Sans objet.

3.2.3.4 Enregistrement d'un Responsable technique via un MC pour un certificat serveur à émettre

Sans objet.

3.2.3.5 Enregistrement d'un nouveau Responsable technique via un MC pour un certificat serveur déjà émis

Sans objet.

3.2.4 Informations non vérifiées du Responsable technique et/ou du serveur informatique

Sans objet.

3.2.5 Validation de l'autorité du demandeur

Pour l'AC CDC – ESSALIA, le demandeur est le Responsable technique.

Cette étape fait partie de l'étape de validation de l'identité d'un individu décrite au paragraphe 3.2.3.

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 reconnaitra toutes les autres AC externes qui disposeront du statut référencé « CFONB ».

Dans ce cas là, si une autre AC formule une demande d'accord, ou si les responsables de l'AC « CDC – ESSELIA » 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 - ESSELIA ».

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

- RFC 5280 ;
- RFC 3739 ;
- 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 délivré au serveur sans renouvellement de la bi-clé correspondante.

3.3.1 Identification et validation pour un renouvellement courant

Le Responsable technique ainsi que l'AE sont avertis de l'arrivée à expiration du certificat par serveur par courriel 90, 30 et 15 jours avant l'expiration.

Le Responsable technique enregistré lors de la première demande va prendre en charge la demande. L'Autorité d'Enregistrement traite la demande comme décrit au paragraphe 4.6.3.
Si c'est un nouveau Responsable technique qui prend en charge la demande, l'Autorité d'Enregistrement va effectuer les vérifications décrites au paragraphe 3.2.3.2 comme dans le cas d'une première demande.

3.3.2 Identification et validation pour un renouvellement après révocation

Ce processus est le même que dans le cas d'une première demande : voir le paragraphe 3.2.3.1.

3.4 Identification et validation d'une demande de révocation

La demande de révocation de certificat de l'AE CDC - ESSELIA peut être effectuée par les acteurs ci-dessous :

- Un Responsable technique.
- L'Autorité d'Enregistrement de l'AC « CDC – ESSELIA ».
- Le Responsable de l'AC « CDC – ESSELIA ».

L'origine d'une demande de révocation est vérifiée et tracée par l'Autorité d'Enregistrement.

- Le Responsable technique est authentifié à l'aide de son adresse email et d'un code de révocation (reçu dans une notification lors du retrait du certificat).
- L'Opérateur d'Enregistrement est authentifié à l'aide de son certificat de l'AC CDC – FIDELIA.
- Le Responsable de l'AC est authentifié par l'AE (face-à-face, signature manuscrite, mail signé).

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Les demandes de certificat de l'AC CDC – ESSELIA sont réalisées par les Responsables techniques ou par l'Autorité d'Enregistrement.

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

Le processus de demande de certificat serveur passe par les étapes suivantes :

- **Demande** : cette étape est l'objet du présent paragraphe.
- Validation des attributions du Responsable technique : cette étape est l'objet du paragraphe 3.2.
- Validation de la demande : cette étape est l'objet du paragraphe 4.2.1.

Le processus de demande s'appuie sur les étapes suivantes :

- Le Responsable technique crée une bi-clé au niveau du serveur.
- Le Responsable technique génère une CSR à partir de la clé publique générée.

Remarque : la CSR doit respecter les contraintes suivantes :

- Le format du DN est celui décrit au paragraphe 3.1.
- Les champs *KeyUsage* et *ExtendedKeyUsage* doivent être conformes au document « Profils de certificats / LCR / OCSP et Algorithmes cryptographiques » du RGS. Ils figurent au paragraphe 7.1.2.

Ensuite, le processus de demande se déroule de la manière suivante :

- Le Responsable technique envoie la CSR par mail à l'Autorité d'Enregistrement (AE-SSL@caissedesdepots.fr)

4.2 Traitement d'une demande de certificat

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

Le processus de demande de certificat serveur passe par les étapes suivantes :

- Demande : cette étape est l'objet du paragraphe 4.1.2.
- Validation des attributions du Responsable technique : cette étape est l'objet du paragraphe 3.2.
- **Validation de la demande** : cette étape est l'objet du présent paragraphe.

Le processus se déroule de la manière suivante :

- Un Opérateur d'Enregistrement prend en compte le mail de demande de certificat.
- L'Opérateur d'Enregistrement se connecte au niveau des interfaces de l'OSC.
- Il uploade la CSR au niveau de l'interface web.
- L'Opérateur d'Enregistrement valide la demande.
- Cela déclenche la génération et la signature d'un certificat au niveau de l'AC.

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

- De connaître les serveurs possédant actuellement un certificat ;
- De connaître le statut des demandes en cours ;
- De connaître le statut des certificats délivrés.

L'AE réalise ce suivi en sauvegardant les mails de demande de certificat.

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 Responsable technique, en justifiant le rejet.

4.2.3 Durée d'établissement du certificat

A l'issue de la validation de la demande et de la soumission de la CSR par l'AE, l'Autorité de Certification génère et signe le certificat.

Cette opération nécessite moins d'une minute.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à la génération du certificat par l'AC, le processus de délivrance se déroule de la manière suivante :

- L'Opérateur d'Enregistrement envoie par mail le certificat généré au Responsable technique, au format PKCS#7.
- Une notification de traitement de la demande est envoyée à l'AE ainsi qu'au Responsable technique.

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

Le Responsable technique reçoit un mail contenant le certificat au format PKCS#7 en provenance de l'AE.
L'AE reçoit également une notification confirmant le traitement de la demande.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

L'acceptation du certificat par le Responsable technique est tacite dès l'installation du certificat au niveau du serveur.
L'installation se déroule de la manière suivante :

- Le Responsable technique doit créer le conteneur de la clé privée et de la clé publique correspondant au certificat.
  Remarque : le format PKCS#12 doit être privilégié afin d'associer une donnée d'activation (code PIN) au certificat.

- Le Responsable technique installe le certificat au niveau du serveur. Le cas échéant, la donnée d'activation doit être saisie au moment de l'installation.

En cas de réclamation ou de problème, le Responsable technique doit prendre contact avec l'AE. Cela pourra donner lieu à la révocation du certificat.

4.4.2 Publication du certificat

Les certificats serveurs ne sont pas publiés après leur délivrance dans le référentiel de l'IGC.

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 serveur en envoyant une notification par mail.

De plus l'AE peut 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 Responsable technique

L'utilisation des clés privées associées aux certificats délivrées par l'AC CDC – ESSELIA doit être limitée aux usages définis au paragraphe 1.4.1.1.

A chacun de ces usages correspond un profil de certificat, qui les indique explicitement via les extensions de certificats (cf 7).

Toute autre utilisation est interdite, et engage la responsabilité personnelle du Responsable technique.

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 - ESSELIA », la notion de renouvellement de certificat, au sens de la RFC 3647, correspondant à la seule modification des dates de validité, n'est pas retenue. Seule la délivrance d'un nouveau certificat suite à un 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 Responsable technique 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 serveurs, par l'AC « CDC - ESSELIA », 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.

La fenêtre de renouvellement est de 3 mois avant la date d'expiration du certificat.

4.7.2 Origine d'une demande de nouveau certificat

Si la demande de nouveau certificat fait suite à une révocation, l'origine de la demande est un Responsable technique ou l'Autorité d'Enregistrement.

Si la demande de nouveau certificat se fait dans le cadre d'une demande de renouvellement du certificat, l'origine de la demande est un Responsable technique (celui ayant réalisé la première demande, ou un nouveau Responsable technique qui doit être nommé – voir le paragraphe 3.2.3.2).

Trois notifications d'arrivée à expiration du certificat sont envoyées au Responsable technique ainsi qu'à l'AE. Passé le délai d'expiration du certificat, une nouvelle demande devra être effectuée (voir le paragraphe 4.1).

4.7.3 Procédure de traitement d'une demande de nouveau certificat

Le processus de renouvellement avec changement de bi-clé est identique dans le cas d'un premier et d'un second renouvellement.

Si la demande de nouveau certificat fait suite à une révocation ou intervient après l'expiration du certificat, la procédure de traitement de la demande de nouveau certificat est identique à la procédure de traitement de la demande (voir les paragraphes 4.1 et 4.2).

La procédure est la suivante :

- Le Responsable technique et l'AE reçoivent une notification d'arrivée à expiration du certificat.
- Un Responsable technique (par défaut le même que celui ayant réalisé la première demande) prend en charge le renouvellement.
- Pour cela, le Responsable technique crée une bi-clé au niveau du serveur.
- Le Responsable technique génère une CSR à partir de la clé publique générée

Remarque : la CSR doit respecter les contraintes suivantes :

- Le format du DN doit être conforme aux exigences du paragraphe 3.1.2.
- Les champs *KeyUsage* et *ExtendedKeyUsage* doivent être conformes au document « Profils de certificats / LCR / OCSP et Algorithmes cryptographiques » du RGS. Ils figurent au paragraphe 7.1.2.

Ensuite, le processus de demande se déroule de la manière suivante :

- Le Responsable technique envoie la CSR par mail à l'Autorité d'Enregistrement (AE-SSL@caissedesdepots.fr)

L'étape suivante de validation des attributions du demandeur est décrite au paragraphe 3.3.

La dernière étape de traitement de la demande est identique au processus décrit au paragraphe 4.2.

4.7.4 Notification au Responsable technique 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 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 Responsable technique 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 serveurs

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

- Modification des informations du serveur transmises lors de la demande du certificat (par exemple, déménagement d'un serveur conduisant à un changement de FQDN).
- Non-respect par le Responsable technique des modalités d'usage du certificat.
- Non-respect de la Politique de Certification par le Responsable technique ou l'entité en charges de la ressource.
- Suspicion de compromission de la clé privée du serveur, perte ou vol de la clé privée et/ou des données d'activation associées.
- Demande de la part du Responsable technique, notamment :
  - Suite à un problème concernant la ressource serveur.
  - Du fait du départ ou de la mobilité d'un Responsable technique. Dans ce cas, un nouveau Responsable technique doit être nommé pour le certificat serveur.
- Arrêt définitif du serveur ou cessation d'activité de l'entité en charge de la ressource serveur.
- Révocation d'un certificat d'AC de la chaîne de confiance.
- Demande par l'Autorité d'Enregistrement.

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 serveurs 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 serveurs

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

- Un Responsable technique ;
- L'Autorité d'Enregistrement de l'AC « CDC – ESSELIA » ;
- Le Responsable de l'AC « CDC – ESSELIA ».

4.9.2.2 Certificats d'une des composantes de l'IGC

La révocation du certificat de l'AC « CDC - ESSELIA » ne peut être décidée que par le responsable de l'AC.

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 serveur

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 Responsables techniques peuvent être réalisées :

- En ligne via une interface mise à disposition par l'Opérateur de Service de Certification (pour les Responsables techniques uniquement).
- Par email à l'AE.

Les informations pratiques permettant de réaliser cette révocation quel que soit le canal sont disponibles sur le site de publication (voir le paragraphe 2.2).

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

- Le Responsable technique se connecte à l'URL de révocation. Celle-ci est rappelée au niveau du site de publication de l'AC (voir paragraphe 2.2).
- Le Responsable technique saisit son code de révocation. (Il a reçu ce code de révocation dans une notification par mail suite au retrait du certificat).

- Le Responsable technique 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.
- Une notification de la révocation est envoyée à l'AE ainsi qu'au Responsable technique.
- 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 certificat à l'aide du champ CN.
- 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.
- Une notification de la révocation est envoyée à l'AE ainsi qu'au Responsable technique.
- L'opération est enregistrée dans les journaux d'évènements.

Le processus de révocation par mail à l'origine d'un Responsable technique ou du Responsable d'AC (identifiés dans le paragraphe ci-dessous comme des demandeurs) est le suivant :

- Le demandeur envoie un mail à l'AE pour faire une demande de révocation
- **Remarque** : le mail doit préciser le certificat à révoquer à l'aide du champ CN.
- Un Opérateur d'Enregistrement prend en charge la demande, tel que décrit dans le paragraphe ci-dessus « processus de révocation par l'AE ».

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 Responsables techniques 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 - ESSELIA, 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 Responsable technique pour formuler la demande de révocation

Dès que le Responsable technique (ou une Personne Autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler une demande de révocation pour le serveur dont il a la charge sans délai.

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

4.9.5.1 Révocation d'un certificat serveur

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 Responsable technique 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 - ESSELIA » (tels que définis au paragraphe 1.3.3) doivent vérifier l'état du certificat de l'Autorité de Certification, et des certificats constituant la chaîne de certification.

La méthode utilisée dépend 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-esselia/.

4.9.7 Fréquence d'établissement des LCR

Les LCR sont établies et publiées sur Internet toutes les 24 heures.

L'information de l'état de révocation d'un certificat est immédiate dans le cadre 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 de 24 heures.

La durée entre la fin de génération de la LCR et sa publication est inférieure à 30 minutes.

L'information de l'état de révocation d'un certificat est immédiate dans le cadre du service OCSP. Dans ce cadre il n'y a donc pas de délai entre la révocation effective d'un certificat et la mise à disposition des Utilisateurs de cette information.

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

L'AC « CDC – ESSELIA » 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 d'authentification. 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 serveurs, 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.

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.

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

En cas de demande de révocation du certificat de l'AC, il informera dans les plus brefs délais l'AE. L'AE informera à son tour dans les plus brefs délais l'ensemble des

Responsables techniques concernés en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

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.

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-esselia/. Ce service permet de vérifier en temps réel et à chaque authentification l'état d'un certificat.

4.11 Fin de la relation entre le Responsable technique et l'AC

La fin de la relation entre le Responsable technique 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, dans la mesure où cette Politique de Certification ne décrit pas de profil de certificat de chiffrement (ou confidentialité).

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 serveur 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, 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

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 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.

Les cinq rôles fonctionnels de confiance sont les suivants :

- **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 » de l'AC « CDC – ESSELIA ».

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, 3 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 dans leur description de poste.

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'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, rejet…) ;
- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- 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, ...) ;
- 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 toutes les 2 semaines 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 jour ouvré ;
- 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 :

- PC et DPC ;
- Certificats, et LCR publiés ;
- Les journaux d'événements ;

- Les logiciels exécutables et fichiers de configuration des outils paramétrés chez l'Opérateur de Service de Certification Keynectis.

5.5.2 Période de conservation des archives

Toutes les données citées au paragraphe 5.5.1 sont archivées 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 – ESSELIA.

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 clés d'AC

La durée de vie des clés de l'AC « CDC - ESSELIA » 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 Responsables techniques 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.

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 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 et les Responsables techniques, en particulier en matière d'archivage des certificats des serveurs et des informations relatives aux certificats ;
- Elle assure la continuité du service d'archivage ;
- Elle assure la continuité du service de Révocation.

Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des Responsables techniques 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 définira 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 définira également, 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 Responsables techniques et les utilisateurs de certificats.

Le déroulement du processus devra être maîtrisé, sur la base d'un planning.

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 Responsables techniques 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 Responsables techniques 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.

L'AC définira 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 définira également, 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 Responsables techniques et les utilisateurs de certificats.

Le déroulement du processus devra être maîtrisé, sur la base d'un planning.

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 des bi clés

6.1.1 Génération des bi clés

6.1.1.1 Clés d'AC

Les clés de l'AC « CDC - ESSELIA » 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 serveurs générées par l'AC

Sans objet.

6.1.1.3 Clés serveurs générées au niveau du serveur

La clé privée est générée localement sur le serveur par le Responsable technique, qui est responsable de la protection de cette clé privée.

Le cas échéant elle sera générée dans un HSM.

6.1.2 Transmission de la clé privée au serveur

Sans objet (voir paragraphe 6.1.1.3).

6.1.3 Transmission de la clé publique à l'AC

Sans objet, pour la clé publique de l'AC.

Pour la clé publique du serveur, elle est transmise à l'AC à l'intérieur d'une CSR par mail puis via les interfaces de l'OSC.
Cela apporte des informations d'un niveau de fiabilité acceptable (relativement au niveau de sécurité de l'AC CDC – ESSELIA) sur l'authentification et l'intégrité de la transmission.

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 - ESSELIA ».
- 2048 bits pour la taille des clés des certificats serveurs.

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 - ESSELIA », et du certificat associé est limitée à la signature de certificats serveurs, 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 Responsable technique s'engage auprès de la CDC à contrôler l'usage réalisé de son certificat serveur dans les limites définies au paragraphe 1.4.1.

Toute autre utilisation est effectuée sous la responsabilité du Responsable technique.

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 de protection des clés privées des serveurs

Les clés privées des serveurs sont stockées au niveau des serveurs, ou dans des HSM le cas échéant.
Leur niveau de protection est sous la responsabilité des Responsables techniques.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle de la clé privée de l'AC « CDC - ESSELIA » 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 Responsables techniques est placée sous leur contrôle.

6.2.3 Séquestre de la clé privée

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

6.2.4 Copie de secours de la clé privée

La clé privée de l'AC « CDC - ESSELIA » 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 serveurs 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 – ESSELIA », et les clés privées des serveurs 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 - ESSELIA » 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 serveurs.

6.2.7 Stockage de la clé privée dans un module cryptographique

Le stockage de la clé privée de l'AC, et des clés privées des serveurs est réalisé par le matériel cryptographique (HSM) dans les conditions de sécurité définies par leur profil de protection respectif.

Remarque : ce paragraphe ne s'applique pas aux certificats serveurs stockés au format logiciel.

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 - ESSELIA » nécessite la présence de trois membres du comité de pilotage au moins.

6.2.8.2 Clés privées des serveurs

L'utilisation d'un code d'activation n'est pas imposée. Elle est toutefois recommandée quand c'est possible.

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 - ESSELIA » 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 serveurs

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 serveurs

La destruction de la clé privée d'un serveur ne peut être effectuée que localement au niveau du serveur, sous la responsabilité du Responsable technique.

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

Les modules cryptographiques de l'AC 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 - ESSELIA », et les clés publiques des serveurs 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 - ESSELIA » ont une durée de vie de 10 ans.

Les clés de signature et les certificats des serveurs ont une durée de vie de 3 ans.

6.4 Données d'activation

Remarque : ce paragraphe s'applique aux certificats serveurs pour lesquels une donnée d'activation peut être définie.

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 générées 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 serveur

Les éléments nécessaires à l'activation de la clé privée des serveurs (code d'activation) sont à définir par le serveur au moment de l'installation du support physique.

L'AC s'assure que le code d'activation retenu par le serveur est sécurisé. Notamment il ne doit pas être trivial, et il ne doit pas être diffusé par le Responsable technique.

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 – ESSELIA ».

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

Les données d'activation d'un serveur, quand elles sont définies, ne sont connues que par le seul Responsable technique, 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 de gestion du cycle de vie des certificats.

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 est évalué EAL4+.

Le service technique fourni par l'OSC est qualifié (voir l'information sur le site de l'ANSSI http://www.ssi.gouv.fr/site_rubrique52.html).

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 avertie 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.

L'AC est implantée sur un réseau protégé 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 - ESSELIA »

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

7.1.1.1 Champs de base

Certificat de base	Valeur
Version	2 (=version 3)
Serial number	11 21 b2 5d f3 86 8d 9c b3 90 0e 03 f8 dc a7 1d 09 4c
Issuer DN	C = FR O = CAISSE DES DEPOTS OU = 0002 180020026 CN = CDC - RACINE
Subject DN	C = FR O = CAISSE DES DEPOTS OU = 0002 180020026 CN = CDC - ESSELIA
NotBefore	YYMMDD000000Z
NotAfter	YYMMDD235959Z (10 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)	**X**	**FALSE**	**OCSP - URI:**http://igc-ocsp.caissedesdepots.fr/ocsp-racine/
Authority Key Identifier	{id-ce 35}	**X**	**FALSE**	
Basic Constraint	{id-ce 19}	**X**	**TRUE**	
CA				**Set**
Maximum Path Length				**0**
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://igc-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}	**X**	**FALSE**	
distributionPoint				**URI:**http://igc-crl.caissedesdepots.fr/cdc/racine.crl
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 serveurs

Les certificats serveurs contiendront les informations suivantes.

7.1.2.1 Champs de base communs à tous les profils

Certificat de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil
Taille de la clé	2048
Durée de validité	3 ans
Issuer DN	C = FR O = CAISSE DES DEPOTS OU = 0002 180020026 CN = CDC - ESSELIA
Subject DN	C = FR O = <Organisation à laquelle est rattachée le certificat esselia> OU = 0002 <code SIRET ou SIREN> CN = <FQDN ou nom explicite du service applicatif>
NotBefore	YYMMDDHHMMSS
NotAfter	YYMMDDHHMMSS + 3 ans
Public Key Algorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Parameters	NULL

7.1.2.2 Extensions de certificat communes à tous les profils

Extensions standards	OID	Inclure	Critique	Valeur
Authority Info Access	(1.3.6.1.5.5.7.1.1)	**X**	**FALSE**	**OCSP - URI:**http://igc-ocsp.caissedesdepots.fr/ocsp-esselia/
Authority Key Identifier	{id-ce 35}	**X**	**FALSE**	
Basic Constraint	{id-ce 19}	**X**	**TRUE**	
CA				**FALSE**
Maximum Path Length				n/a
Certificate Policies	{id-ce 32}	**X**	**FALSE**	
policyIdentifiers				**1.2.250.1.5.1.1.1.6.1**
policyQualifiers				n/a
CPSpointer				n/a
OID				n/a
Value				http://igc-pc.caissedesdepots.fr/pc-esselia.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}	**X**	**FALSE**	
distributionPoint				http://igc-crl.caissedesdepots.fr/cdc/esselia.crl
reasons				n/a
cRLIssuer				n/a
Issuer Alternative Name	{id-ce 18}			n/a
Subject Alternative Name				n/a
				n/a
Qualified Certificate Statement	1.3.6.1.5.5.7.1.3			n/a
Directice compliance				n/a
Monetary value				n/a
Currency/amount/exponent				n/a
Private Key Usage Period	{id-ce 16}			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				

7.1.2.3 Extensions de certificat pour le profil SSL serveur

Extensions standards	OID	Inclure	Critique	Valeur
Extended Key Usage	{id-ce 37}	**X**	**FALSE**	
Client Authentication	1.3.6.1.5.5.7.3.2			**Clear**
Server Authentication	1.3.6.1.5.5.7.3.1			**Set**
Email Protection				**Clear**
OCSP Signing				**Clear**
Time Stamping				**Clear**
Code Signing				**Clear**

Key Usage	{id-ce 15}	**X**	**TRUE**	
Digital Signature				**Set**
Non Repudiation				**Clear**
Key Encipherment				**Set**
Data Encipherment				**Clear**
Key Agreement				**Clear**
Key CertSign				**Clear**
Key CRL Sign				**Clear**

7.1.2.4 Extensions de certificat pour le profil SSL client

Extensions standards	OID	Inclure	Critique	Valeur
Extended Key Usage	{id-ce 37}	**X**	**FALSE**	
Client Authentication	1.3.6.1.5.5.7.3.2			**Set**
Server Authentication	1.3.6.1.5.5.7.3.1			**Clear**
Email Protection				**Clear**
OCSP Signing				**Clear**
Time Stamping				**Clear**
Code Signing				**Clear**
Key Usage	{id-ce 15}	**X**	**TRUE**	
Digital Signature				**Set**
Non Repudiation				**Clear**
Key Encipherment				**Clear**
Data Encipherment				**Clear**
Key Agreement				**Clear**
Key CertSign				**Clear**
Key CRL Sign				**Clear**

7.1.2.5 Extensions de certificat pour le profil cachet serveur

Extensions standards	OID	Inclure	Critique	Valeur
Extended Key Usage	{id-ce 37}			
Client Authentication	1.3.6.1.5.5.7.3.2			n/a
Server Authentication	1.3.6.1.5.5.7.3.1			n/a
Email Protection				n/a
OCSP Signing				n/a
Time Stamping				n/a
Code Signing				n/a
Key Usage	{id-ce 15}	**X**	**TRUE**	
Digital Signature				**Set**
Non Repudiation				**Set**
Key Encipherment				**Clear**
Data Encipherment				**Clear**
Key Agreement				**Clear**
Key CertSign				**Clear**
Key CRL Sign				**Clear**

7.1.2.6 Extensions de certificat pour le profil cachet horodatage

Extensions standards	OID	Inclure	Critique	Valeur
Extended Key Usage	{id-ce 37}	**X**	**TRUE**	

Client Authentication	1.3.6.1.5.5.7.3.2			**Clear**
Server Authentication	1.3.6.1.5.5.7.3.1			**Clear**
Email Protection				**Clear**
OCSP Signing				**Clear**
Time Stamping				**Set**
Code Signing				**Clear**
Key Usage	{id-ce 15}			
Digital Signature				n/a
Non Repudiation				n/a
Key Encipherment				n/a
Data Encipherment				n/a
Key Agreement				n/a
Key CertSign				n/a
Key CRL Sign				n/a

7.1.2.7 Extensions de certificat pour le profil OCSPResponder

Extensions standards	OID	Inclure	Critique	Valeur
Extended Key Usage	{id-ce 37}	**X**	**TRUE**	
Client Authentication	1.3.6.1.5.5.7.3.2			**Clear**
Server Authentication	1.3.6.1.5.5.7.3.1			**Clear**
Email Protection				**Clear**
OCSP Signing				**Set**
Time Stamping				**Clear**
Code Signing				**Clear**
Key Usage	{id-ce 15}			
Digital Signature				n/a
Non Repudiation				n/a
Key Encipherment				n/a
Data Encipherment				n/a
Key Agreement				n/a
Key CertSign				n/a
Key CRL Sign				n/a

7.1.2.8 Extensions de certificat pour le profil signature de code

Extensions standards	OID	Inclure	Critique	Valeur
Extended Key Usage	{id-ce 37}	**X**	**TRUE**	
Client Authentication	1.3.6.1.5.5.7.3.2			**Clear**
Server Authentication	1.3.6.1.5.5.7.3.1			**Clear**
Email Protection				**Clear**
OCSP Signing				**Clear**
Time Stamping				**Clear**
Code Signing				**Set**
Key Usage	{id-ce 15}			
Digital Signature				n/a
Non Repudiation				n/a
Key Encipherment				n/a
Data Encipherment				n/a

Key Agreement				n/a
Key CertSign				n/a
Key CRL Sign				n/a

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 contiendra la valeur « *unspecified* ».

Les LCR émises présentent les caractéristiques suivantes :

Version et algorithme :
- La version de la LCR est v2.
- L'algorithme de signature est sha256withRSA.

Extensions :
- Les extensions « Numéro de la LCR » et « *Autorithy Key Identifier* » seront présentes.

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

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

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

7.3 Profil OCSP

Le service OCSP est opéré par l'Opérateur de Service de Certification de l'AC. Pour les certificats serveurs, il est accessible à travers l'adresse :

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

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 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.

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 - ESSELIA sont définies dans la Déclaration des Pratiques de Certification.

8.3 Relations entre évaluateurs et entités évaluées

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, 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, etc.

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 hiérarchise. 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

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, comme la mise à disposition de la liste de révocation.

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, comme la mise à disposition de la liste de révocation.

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, comme la mise à disposition de la liste de révocation.

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, comme la mise à disposition de la liste de révocation.

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

Couverture et garantie concernant les entités utilisatrices

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 l'AC « CDC – ESSELIA », et des certificats des serveurs ;
- Les données d'activation (donnée d'activation des certificats serveurs et 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 le nom, le prénom et l'adresse email du responsable technique ainsi que les 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 responsable technique 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 utilisé 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 Responsable technique 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 Responsable technique 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 serveur.
- 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 DPC pour :

- la vérification de la compatibilité des informations recueillies avec celles exigées par la présente PC pour la délivrance de certificats serveurs ;
- la conformité des informations contenues dans le certificat avec les informations recueillies aux fins de délivrance de certificats ;
- 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 Responsables techniques

Le Responsable technique 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 - ESSELIA qu'aux fin définies au paragraphe 1.4 de la Politique de Certification de l'AC ;
- Protéger sa clé privée par des moyens appropriés à son environnement ;
- Protéger les données d'activation de la bi-clé correspondante ;
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans le certificat ;
- Faire, sans délai, une demande de révocation du certificat auprès de l'AE ou de l'AC en cas de compromission ou de suspicion de compromission de la 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.

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 - ESSELIA ;

- Vérifier que le certificat serveur n'est pas présent dans les listes de révocation de l'AC CDC - ESSELIA ;
- Vérifier la signature du certificat du serveur, et de la chaîne de certification, jusqu'à l'AC « AC CDC - RACINE » et contrôler la validité des certificats.

9.6.5 Autres participants

9.6.5.1 Mandataires de certification

Sans objet.

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 Responsable technique.

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 termes 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 - ESSELIA » 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 tous les 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.

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.