Référence du document : ROOT PC 0020
Révision du document : 1.3
Date du document : 21/07/2017
Classification : Publique

# Autorité de Certification Racine MediaCert

## Politique de Certification





Scellé par Cyril Lootvoet (Responsable de l'Autorité de Certification)

# Table des Matières

## Liste des modifications

| Version | Date | Description | Auteur | Validation |
|---|---|---|---|---|
| **1.0** | 27/07/2012 | Création | D Cogny | D Bonnin |
| **1.1** | 5/11/2015 | Mise à jour avant publication | J.J. Milhem | NA |
| **1.2** | 23/11/2015 | Mise à jour 2.1 et 2.2 | Q Alexandre | NA |
| **1.3** | 21/07/2017 | Mise à jour pour prise en compte de la réglementation eIDAS | A. Borel<br>F. Da Silva | Comité Sécurité |

# Introduction

## 1.1 Présentation générale

Ce document décrit la politique de certification (PC) de l'Autorité de Certification Racine MediaCert de Worldline. Il s'agit de l'autorité de plus haut niveau au sein de l'Infrastructure à Gestion de Clés MediaCert mise en place par Worldline. Cette Infrastructure à Gestion de Clés (IGC), nommée MediaCert, est constituée de cette Autorité de Certification Racine à laquelle sont rattachées des Autorités de Certification filles spécialisées pour des besoins internes ou des besoins d'accompagnement de projets client, avec par exemple la fourniture de certificats d'accès à des extranets, de certificats de signature ou autre.

Note 1 : Cette AC vient en renouvellement anticipé d'une AC racine MediaCert créée en 2002.
Note 2 : Cette IGC et ses AC ne sont pas à but commercial.

## 1.2 Identification

Le nom de l'Autorité de Certification concernée par cette Politique de Certification est « MediaCert ».

Le n° **1.2.250.1.111** a été attribué par l'AFNOR à Worldline comme racine d'OID sous laquelle sont déclinés les OID des différentes AC. Les OID des AC sont de la forme 1.2.250.1.111.x.y.z où x, y et z sont :

- x : année de création de l'Autorité de Certification : 2012 => 12 ;
- y : numéro attribué à l'Autorité de Certification par Worldline d'après l'année de création ;
- z : version majeure de la PC.

L'OID attribué à cette Politique de Certification est : **1.2.250.1.111.12.4.1**.

Le *« Distinguished Name »* (DN) de l'Autorité de Certification Racine MediaCert est le suivant :

C = FR
O = Atos Worldline
OU = 0002 378901946
CN = AC Racine - Root CA - 2012

## 1.3 Composants de l'IGC

Cette IGC est constituée de plusieurs blocs fonctionnels, en particulier des fonctions d'AC et d'AE.

### 1.3.1 Fonctionnalité Autorité de Certification (AC)

L'AC assure les services de gestion de certificats des AC filles rattachées :

- le traitement des demandes de certificat ;
- la délivrance des certificats aux demandeurs ;
- le traitement des demandes de révocation ;
- la publication de son certificat et des LAR.

L'AC racine signe les certificats et les LAR qu'elle émet avec sa clé privée et en est responsable. Cette AC est par définition une AC auto-signée.

Ces fonctionnalités sont offertes par le logiciel de PKI utilisé en association avec un HSM pour la génération, le stockage de la clé privée et la signature des certificats et LAR.

#### 1.3.1.1 Fonction de génération des certificats

Cette fonction génère les certificats à partir des informations transmises par le Comité Sécurité sous forme de CSR et d'un gabarit de certificat défini lors de la configuration de l'AC racine.

#### 1.3.1.2 Fonction de génération des éléments secrets d'une AC fille

Sans objet. Les clés d'une AC fille sont générées à son niveau.

#### 1.3.1.3 Fonction de publication

Le certificat d'AC racine est transmis aux responsables, ou un de ses adjoints, des Autorités de Certification concernées qui mettent en œuvre des certificats d'une AC fille sous forme de chaine de certification contenant ce certificat racine et celui de l'AC fille utilisée.

#### 1.3.1.4 Fonction de gestion des révocations

Cette fonction traite les demandes de révocation qui sont soumises à l'AC. Il en résulte la publication immédiate d'une nouvelle LAR qui est transmise aux responsables des Autorités de Certification concernées.

### 1.3.2 Fonction Autorité d'enregistrement (AE)

Il n'y a pas à proprement parler d'entité administrative pour traiter des demandes de signature d'AC filles car cette racine ne signe que des AC internes à Worldline. Ceci est traité lors de la préparation des cérémonies de clés.

Le logiciel de PKI offre une interface graphique permettant aux administrateurs de soumettre une CSR et de récupérer le certificat correspondant qui est ensuite installé dans l'environnement technique de l'AC fille.

## 1.4 Usage des certificats

### 1.4.1 Domaines d'utilisation applicables

La bi-clé de cette AC racine ne sert qu'à signer des AC filles internes MediaCert Worldline et ses LAR émises à intervalle régulier.

### 1.4.2 Domaines d'utilisation interdits

Tout autre usage est interdit, par exemple la signature d'AC externes, de certificats de serveurs ou de personnes.

## 1.5 Gestion de la PC

Worldline est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC. A cette fin, un Comité Sécurité statue à échéances régulières, sur la nécessité d'apporter des modifications à la PC. Ce comité est constitué :

- d'au moins un représentant de l'AC ;
- du responsable sécurité de l'AC ;

Le contact habilité pour toute remarque, demande d'information complémentaire, réclamation ou remise de dossier de litige concernant la présente PC est :

**Comité "MediaCert "**
**Worldline**
**1, rue de la Pointe**
**Zone Industrielle A**
**59113 Seclin**
**France**
**dlfr-mediacert-ac-otu@atos.net**

## 1.6 Acronymes

Les acronymes utilisés dans ce document sont les suivants :

- **AC :** Autorité de Certification ;
- **AE :** Autorité d'Enregistrement ;
- **CN :** Common Name ;
- **CSR :** Certificate Signing Request ;
- **DN** : Distinguished Name ;
- **HSM :** Hardware Security Module ;
- **IGC** : Infrastructure de Gestion de Clés (PKI en Anglais) ;
- **KC :** Key Ceremony (Cérémonie de Clés) ;
- **LAR :** Liste des certificats d'Autorités Révoqués (CARL en Anglais) ;
- **OID :** Object Identifier ;
- **PC :** Politique de Certification ;
- **PKI :** Public Key Infrastructure ;
- **PV :** Procès-verbal ;
- **RSSI :** Responsable Sécurité des Systèmes d'Information.

# 2 Responsabilités concernant la mise à disposition des informations devant être publiées

## 2.1 Entités chargées de la mise à disposition des informations

Le comité MediaCert est en charge de la publication de cette PC.
Des administrateurs techniques pilotent les publications de LAR.

## 2.2 Informations devant être publiées

Le comité MediaCert publie la PC sur un disque partagé, accessible en interne par le personnel Worldline, ainsi que sur le site internet de Worldline (https://www.mediacert.com), à des fins de consultation par le public.

Les LAR émises par l'AC sont publiées par les administrateurs techniques sur un disque partagé, l'adresse de publication des LAR est également disponible dans le certificat de l'AC publiée sur le site internet de Worldline, à des fins de consultation par le public.

Les URLs pour accéder à cette PC ainsi qu'à la LAR sont disponibles dans les extensions des certificats délivrés par l'AC Racine conformément au chapitre 7.1 du présent document.

## 2.3 Délais et fréquences de publication

La Politique de Certification est publiée après validation interne au sein du Comité Sécurité.
Les LAR sont publiées dans les 24H après leur génération.

## 2.4 Contrôle d'accès aux informations publiées

La PC et les LAR sont accessibles librement et uniquement en lecture depuis la page web suivante définie au chapitre 2.2 du présent document.

Les éléments publiés sont signés de manière électronique afin d'être dument authentifiables.

L'accès en modification des informations est strictement limité aux fonctions d'administration internes habilitées de l'IGC qui disposent des droits d'écriture sur l'environnement partagé de dépôt de ces informations.

# 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.

Les champs *« issuer »* et *« subject »* des certificats sont identifiés par un *« Distinguished Name »* (DN) de type X.501 sous forme d'une « *PrintableString* » (chaîne imprimable).

### 3.1.2 Pseudonymisation

Sans objet.

### 3.1.3 Règles d'interprétation des différentes formes de nom

Sans objet.

### 3.1.4 Unicité des noms

Le champ « Common Name » (CN) est unique pour chaque AC fille.

Toute demande (hors renouvellement) ne respectant pas cette règle doit être refusée.
Durant toute la durée de vie de l'AC, un CN attribué à une AC fille ne peut donc être attribué à une autre AC.

L'unicité du « Distinguished Name » (DN) est quant à elle assurée par la présence du champ appelé « Serial Number in DN ».

### 3.1.5 Identification, authentification et rôle des marques déposées

Sans objet.

## 3.2 Validation initiale de l'identité

### 3.2.1 Méthode pour prouver la possession de la clé privée

La signature d'une CSR par la clé privée associée apporte cette garantie.

### 3.2.2 Validation de l'identité d'un organisme

Les données de nommage d'une AC fille à signer sont communiquées pour validation dans la phase de préparation de la cérémonie de clés.

### 3.2.3 Validation de l'identité d'un individu

Sans objet.

### 3.2.4 Informations non vérifiées

Les informations du certificat font l'objet d'une validation dans la phase de préparation de la cérémonie de clés.

### 3.2.5 Validation de l'autorité du demandeur

Le demandeur est une entité interne Worldline.

### 3.2.6 Certification croisée d'AC

Sans objet.

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

### 3.3.1 Identification et validation pour un renouvellement courant

L'identification et la validation pour un renouvellement courant d'un certificat d'AC fille sont effectuées conformément au § 3.2.

### 3.3.2 Identification et validation pour un renouvellement après révocation

L'identification et la validation pour un renouvellement suite à révocation d'un certificat d'AC fille sont effectuées conformément au § 3.2.

## 3.4 Identification et validation d'une demande de révocation

La révocation d'une AC fille peut être décidée après concertation entre :

- l'entité responsable de cette AC ;
- le directeur du comité MediaCert ;
- le RSSI en charge de la sécurité de l'AC Racine.

# 4 Exigences opérationnelles sur le cycle de vie des certificats

## 4.1 Demande de certificat

### 4.1.1 Origine d'une demande de certificat

La demande de certificat provient uniquement d'une entité interne.

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

Les demandes font l'objet d'une validation préalable de légitimité par le Comité MediaCert.

## 4.2 Traitement d'une demande de certificat

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

L'identification et la validation de la demande sont traitées lors de la phase de préparation de la cérémonie de clés par le comité MediaCert.

### 4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, le comité MediaCert informe l'entité à l'origine de la demande en précisant le motif (par ex une clé publique de longueur insuffisante).

### 4.2.3 Durée d'établissement du certificat

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

## 4.3 Délivrance du certificat

### 4.3.1 Actions de l'AC concernant la délivrance du certificat

Cette opération nécessite la réactivation de l'AC Racine et implique la présence de plusieurs rôles de confiance au sein de l'IGC à convoquer.

Après sa validation la CSR est soumise à l'AC Racine au travers d'une interface graphique lors d'une cérémonie de clés.

Les éléments de nommage sont affichés et comparés aux valeurs indiquées dans le script de la cérémonie de clés. S'ils sont cohérents, un gabarit de certificat est choisi et la demande est soumise à l'AC qui fournit le certificat en retour, sinon la demande est rejetée.

Le certificat est copié sur un support amovible pour être délivré manuellement après la séance.

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

La délivrance du certificat a lieu après la séance par la remise du Comité MediaCert du certificat à l'entité en charge de l'AC fille. Selon les cas cette remise pourra se faire via un support amovible en mains propres ou par mail.

## 4.4 Acceptation du certificat

### 4.4.1 Démarche d'acceptation du certificat

L'acceptation est tacite.

### 4.4.2 Publication du certificat

Il n'y a pas de publication dans l'environnement de l'AC racine.

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

Sans objet.

## 4.5 Usage de la bi-clé et du certificat

### 4.5.1 Utilisation de la clé privée et du certificat

L'utilisation de la clé privée d'une AC fille et du certificat associé est strictement limitée à la signature de certificats et de CRL au sein de cette AC selon l'usage prévu dans sa PC. Dans le cas contraire sa responsabilité pourrait être engagée.

Cet usage est par ailleurs indiqué via l'extension « Key_Usage » de son certificat.

### 4.5.2 Utilisation de la clé publique et du certificat par des tiers

Les tiers utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

## 4.6 Renouvellement d'un certificat

Le renouvellement sans changement des clés n'est pas autorisé.

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

Ce chapitre traite de la délivrance d'un nouveau certificat à une AC fille liée à la génération d'une nouvelle bi-clé.

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

Les causes de renouvellement sont diverses avec en premier lieu l'expiration. Les renouvellements anticipés sont également possibles, par exemple pour des raisons de maintenabilité technique ou de faiblesse d'une clé ou d'un algorithme utilisé dans le certificat courant.

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

L'origine est la même que pour une demande initiale. Cf. § 4.1.1.

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

La procédure est la même que pour une demande initiale. Cf. § 4.2.

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

La procédure est la même que pour une demande initiale. Cf. § 4.3.2.

### 4.7.5 Démarche d'acceptation du nouveau certificat

La procédure est la même que pour une demande initiale. Cf. § 4.4.1.

### 4.7.6 Publication du nouveau certificat

La procédure est la même que pour une demande initiale. Cf. § 4.4.2.

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

La procédure est la même que pour une demande initiale. Cf. § 4.4.3.

## 4.8 Modification du certificat

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

## 4.9 Révocation et suspension des certificats

### 4.9.1 Causes possibles d'une révocation

#### 4.9.1.1 Certificat d'une AC fille

Les causes possibles de révocation sont nombreuses, par exemple :

- une erreur détectée dans le contenu du certificat apparue après la cérémonie de clés ;
- la cessation d'activité ;
- une suspicion de compromission, une compromission, la perte ou le vol de sa clé privée ;
- évolutions réglementaires sur les algorithmes utilisés.

#### 4.9.1.2 Certificat de l'AC racine

Les causes possibles de révocation sont également nombreuses, en particulier :

- la cessation d'activité ;
- une suspicion de compromission, une compromission, la perte ou le vol de sa clé privée ;

Dans ce cas il faut préalablement révoquer toutes les Autorités de Certification filles et publier une dernière LAR avant l'arrêt définitif.

### 4.9.2 Origine d'une demande de révocation

Ce type de révocation ne peut être demandé qu'après concertation entre :

- l'entité responsable de cette AC.
- le comité MediaCert.
- le RSSI en charge de l'Autorité de Certification.

### 4.9.3 Procédure de traitement d'une demande de révocation

Cette opération nécessite la réactivation de l'AC Racine et implique la présence de plusieurs rôles de confiance au sein de l'IGC à convoquer.

La révocation est réalisée lors d'une cérémonie de clés sur l'AC racine via une interface graphique du logiciel de PKI. Il en résulte la publication immédiate d'une nouvelle LAR qui est mise à disposition de l'entité responsable de cette AC. Un PV de séance est également produit.

Si la révocation concerne la racine, il faut au préalable révoquer toutes les AC filles.

### 4.9.4 Délai pour formuler la demande de révocation

Dès que la décision est prise, les contacts sont pris avec les administrateurs pour organiser la séance de révocation.

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

Cette opération nécessite la réactivation de l'AC racine et implique la présence de plusieurs rôles à convoquer. Elle est réalisable dans les 48H ouvrés après la demande.

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

Il n'y a pas d'obligation systématique pour les applications utilisant des certificats MediaCert de vérifier les LAR et CRL.

La LAR est mise à disposition des applications tierces qui font cette vérification sous forme de fichier.

### 4.9.7 Fréquence d'établissement des LAR

Les LAR sont générées à chaque révocation ou par défaut tous les 12 mois. Cependant, une nouvelle LAR peut être publiée à la suite d'une révocation d'une AC fille.

### 4.9.8 Délai maximum de publication d'une LAR

Une LAR est publiée dans un délai maximum de 24 heures ouvrés suivant sa génération.

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

Service non proposé.

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

Sans objet.

### 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

En cas de compromission d'une clé d'AC fille, son entité responsable doit l'arrêter immédiatement sans attendre la séance de révocation.

### 4.9.13 Causes possibles d'une suspension

La suspension d'une AC n'est pas permise.

### 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'une AC

Sans objet.

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

Il n'y a pas de fonction d'information sur état des certificats autres que la publication de LAR. Les LAR sont publiées au format CRL v2 (RFC 5280) sur un internet, accessibles en protocole HTTP(s) à l'adresse :

- précisée au chapitre 2.2 de la présente PC ;
- précisée dans le certificat délivré par l'AC Racine comme spécifié au chapitre 7.1 de la présente PC.

## 4.11 Fin de la relation avec une AC fille

En cas de fin de relation, pour quelque raison que ce soit, le certificat de l'AC doit être révoqué.

## 4.12 Séquestre de clé et recouvrement

Il n'y a pas de séquestre d'une clé d'AC fille au niveau de l'AC racine.

La seule forme de séquestre est la sauvegarde de la clé de l'AC racine elle-même à des fins de reprise en cas de crash. Cette sauvegarde est encadrée par les procédures « constructeur » du HSM utilisé.

# 5 Mesures de sécurité non techniques

## 5.1 Mesures de sécurité physique

Worldline héberge cette AC racine dans un centre informatique offrant les garanties nécessaires en terme de contrôle d'accès, de sécurité incendie, de sauvegardes, …

Le serveur d'AC et son HSM sont installés dans des locaux dont les accès sont contrôlés (tracés, vidéo-surveillés) et réservés aux personnels habilités.

L'initialisation et l'activation de l'AC implique la présence de plusieurs rôle de confiance complémentaires entre eux.

## 5.2 Mesures de sécurité procédurales

### 5.2.1 Rôles de confiance

Les fonctions opérées sur l'AC Racine sont réparties sur plusieurs types d'intervenants afin de veiller à la séparation des connaissances pour les tâches sensibles.

Celle-ci est désactivée en dehors des cérémonies de clés pour lesquelles différents types d'intervenants dans l'organisation peuvent être impliqués suivant les opérations effectuées :

- les administrateurs systèmes ;
- les administrateurs HSM ;
- un auditeur système ;
- le maitre de cérémonie :
- les porteurs de secret ;
- le responsable de centre.

Leurs tâches respectives sont précisées dans les scripts de cérémonies de clés.

### 5.2.2 Nombre de personnes requises par tâches

Selon le type d'opérations effectuées, le nombre et le type de rôles et de personnes devant être présentes sont différents. Le besoin est le plus important pour la création de l'AC avec les phases de configuration des serveurs et HSM et d'installations de logiciel PKI qui impliquent également les administrateurs systèmes.

### 5.2.3 Identification et authentification pour chaque rôle

La vérification de l'identité des intervenants est généralement implicite car les intervenants sur cette IGC interne sont des collègues se connaissant. Dans le cas contraire (par exemple un collègue d'un site Worldline hors de France) le responsable du centre informatique demande une preuve d'identité.

### 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.

## 5.3 Mesures de sécurité vis-à-vis du personnel

### 5.3.1 Qualifications, compétences et habilitations requises

Le personnel opérant des rôles de confiance au sein de l'IGC MediaCert est informé de ses responsabilités relatives (document d'engagement, document DPC) ainsi que des procédures liées à la sécurité des systèmes et au contrôle du personnel, auxquelles il doit se conformer.

Le personnel d'encadrement est formé et sensibilisé à la sécurité et à la gestion des risques pour assumer pleinement ses responsabilités vis-à-vis de l'IGC MediaCert.

L'IGC MediaCert s'assure de la qualification et de la compétence de son personnel opérant des rôles de confiance.

### 5.3.2 Procédures de vérification des antécédents

Les personnels ne doivent notamment pas avoir de condamnation de justice ou être en situation de conflit d'intérêt en contradiction avec leurs attributions. Ils remettent à leur employeur une copie du bulletin n°3 de leur casier judiciaire dans le cadre de la procédure d'embauche ainsi que lors de la remise de leur engagement de responsabilité.

Le dossier de candidature du postulant est soumis à la validation du service Ressources Humaines.

La vérification des antécédents judiciaires est renouvelée tous les trois (3) ans. Dans cette optique, une tâche récurrente annuelle de vérification des antécédents judiciaires est mise en place.

Les personnels chargés d'opérer les services de Certification ne sont pas chargés des aspects commerciaux liés à ces services et sont dégagés de tout conflit d'intérêts qui pourraient influencer la manière de mener les opérations dont ils sont chargés et obérer la confiance. A cet égard, ils s'engagent à confirmer par écrit, lors de leur acceptation du rôle de confiance au sein de l'IGC MediaCert, l'absence de tout conflit d'intérêt lié à l'exercice de cette nouvelle activité.

### 5.3.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures de fonctionnement de l'AC.
Les personnels ont eu connaissance des implications des opérations dont ils ont la responsabilité via la sensibilisation sécurité.

### 5.3.4 Exigences et fréquence en matière de formation continue

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

### 5.3.5 Fréquence et séquence de rotation entre différentes attributions

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

### 5.3.6 Sanctions en cas d'actions non autorisées

Le règlement intérieur de Worldline indique que des sanctions disciplinaires administratives appropriées sont applicables en cas de faute (non-respect de la présente DPC, …). Ceci est notamment rappelé dans l'engagement de responsabilités signé par toute personne assumant un rôle de confiance au sein de l'IGC MediaCert.

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

Sans objet. Seul le personnel Worldline intervient dans les rôles de confiance sur ces applications.

### 5.3.8 Documentation fournie au personnel

Chaque personne dispose au minimum de la documentation relative aux procédures opérationnelles et aux outils spécifiques qu'il met en œuvre, ainsi que des politiques et pratiques générales de la composante au sein de laquelle il travaille.

## 5.4 Procédures de constitution des données d'audit

Toutes les opérations concernant l'AC sont tracées. Il s'agit de traces informatiques ou manuscrites. Ils permettent de garantir l'audibilité, la traçabilité et l'imputabilité opérations.

### 5.4.1 Type d'évènements à enregistrer

Les journaux d'événements comprennent explicitement l'identifiant de l'exécutant (logiciel ou opérateur) de l'opération, la date, le type d'opération et un descriptif.

#### 5.4.1.1 Traces informatiques de l'AC

Chaque composant journalise les événements et incidents le concernant. Ci-dessous figure une liste non-exhaustive :

- démarrage et arrêt des systèmes informatiques et des applications ;
- gestion des comptes utilisateur ;
- connexion des utilisateurs ;
- création des certificats ;
- révocation des certificats ;
- publication des LAR.

#### 5.4.1.2 Contrôle d'accès

Le contrôle d'accès aux locaux journalise également ses évènements sur son propre système.

#### 5.4.1.3 Traces manuscrites

Les journaux manuels concernent :

- les cérémonies de clés et leurs PV ;
- les créations de LAR ;
- la révocation ou le renouvellement d'une AC ;
- les interventions nécessitant l'accès aux locaux sensibles et aux coffres, par exemple la remise en service du HSM ou une restauration à partir des sauvegardes suite à une panne ;
- les mises au rebut.

### 5.4.2 Fréquence de traitement des journaux d'évènements

Les journaux de l'AC racine ne font pas l'objet d'un contrôle régulier. Ils sont utilisés uniquement pour des besoins d'enquête interne et d'audit.

### 5.4.3 Période de conservation des journaux d'évènements

Les journaux sont conservés pendant toute la durée de vie de l'AC.

### 5.4.4 Protection des journaux d'évènements

Les journaux tant informatiques que manuscrits sont protégés par un contrôle d'accès strict et limité aux seules personnes habilitées.

### 5.4.5 Procédure de sauvegarde des journaux d'évènements

Les journaux d'événements sont sauvegardés à la fin de chaque cérémonie des clés, juste avant la désactivation de l'AC.

### 5.4.6 Système de collecte des journaux d'évènements

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

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

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

### 5.4.8 Evaluation des vulnérabilités

L'AC étant désactivée en dehors des séances de clé, il n'y a pas d'analyse systématique et régulière des journaux. Ceci n'est effectué qu'en cas de besoin d'enquête interne.

## 5.5 Archivage des données

### 5.5.1 Types de données à archiver

L'archivage est réalisé afin d'assurer la traçabilité des opérations. Les données à archiver sont les suivantes :

- Pour l'AC :

- les demandes de certificat d'AC fille formulées ;
- les demandes de révocation ou de renouvellement;
- les certificats et LAR.

- Pour la plate-forme technique (serveur & HSM) :

- les documents techniques décrivant les configurations et les équipements informatiques ;
- les paramètres d'exploitation des logiciels ;
- les dossiers de procédure d'exploitation ;
- les journaux d'événement.

- Pour la documentation :

- les mains courantes d'accès aux locaux sensibles ;
- les manuels de cérémonie de clefs ;
- les versions et les révisions de la PC ;
- les engagements/cessations de responsabilité des rôles de confiance.

### 5.5.2 Période de conservation des archives

Elles sont conservées pendant la durée de vie de l'AC et 3 ans au-delà.

### 5.5.3 Protection des archives

Selon leur forme (papier ou électronique) et leur moyen de conservation la protection est assurée par les droits d'accès et éventuellement des outils de contrôle d'intégrité (cas des cartouches magnétiques par exemple).

### 5.5.4 Procédure de sauvegarde des archives

Les archives papier sont le plus souvent scannées et déposées dans des bases documentaires.

Les documents techniques d'exploitation sont également déposés dans des bases documentaires.

Les archives informatiques sont de deux types :

- les « tickets » ISMP ;
- les journaux d'évènement.

### 5.5.5 Exigences d'horodatage des données

L'horloge du serveur de l'AC racine est synchronisée sur une source externe fiable.

### 5.5.6 Système de collecte des archives

La collecte est organisée après chaque séance de clés sauf pour les « tickets » ISMP qui eux sont traités automatiquement.

### 5.5.7 Récupération et vérification des archives

Les versions électroniques sont récupérables quasiment immédiatement. Les versions papier (par exemple les mains courantes d'accès aux locaux sensibles) le sont dans un délai de 2 jours ouvrés.

## 5.6 Changement de clé d'AC

L'AC ne peut pas générer de certificat d'AC fille dont la date de fin serait postérieure à la date d'expiration de son certificat.

Elle doit être renouvelée au plus tard à son expiration ou avant l'échéance s'il faut par exemple évoluer vers des algorithmes plus forts, des longueurs de clés supérieures ou s'il faut signer une AC fille dont l'échéance souhaitée est postérieure à l'échéance de l'AC racine. Dans ce cas l'ancienne AC racine est maintenue pour pouvoir révoquer les AC qu'elle a signées et continuer à publier ses LAR. La nouvelle est utilisée pour signer et révoquer de nouvelles AC et publier ses LAR.

## 5.7 Reprise suite à compromission et sinistre

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

Les personnels Worldline sont sensibilisés au traitement des incidents dont les incidents de sécurité. Dans ce dernier cas et conformément à nos procédures spécifiques ils ouvrent un incident ISMP avec un code objet spécifique qui génère un « workflow » à destination de l'équipe sécurité. Celle-ci va coordonner l'analyse et les actions qui en découlent dont la communication vers les entités responsables des AC filles.

### 5.7.2 Procédures de reprise en cas de corruption des ressources informatiques

Worldline dispose de procédures, de sauvegardes, de contrats de maintenance et de matériels de rechange pour remettre l'AC en service en cas d'incident technique.

La clé privée qui constitue l'élément le plus sensible est conservée par précaution en deux exemplaires sur deux sites différents.

### 5.7.3 Procédures de reprise en cas de compromission de la clé privée

Si la clé privée de l'AC MediaCert est compromise ou est soupçonnée de l'être, si elle est détruite ou encore si l'algorithme utilisé est compromis :

- après enquête sur l'évènement, Worldline décide de la révocation ou non du certificat de l'AC Racine ;
- s'il est décidé de révoquer le certificat concerné de l'AC Racine :
    - tous les certificats délivrés par les AC filles et signés avec leur clé privée concernée sont révoqués ;
    - tous les certificats délivrés par l'AC Racine et signés avec la clé privée concernée sont révoqués.
- si un algorithme est compromis, il est alors remplacé ;
- une nouvelle bi-clé est générée et un nouveau certificat d'AC Racine correspondant est émis ;
- Worldline statue sur le plan de communication à destination :
    - des Autorités qui accréditent le certificat en question (Adobe, ANSSI, …) ;
    - des Abonnés et des utilisateurs de certificats des AC filles.

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

L'AC racine n'a pas de besoin de fonctionnement continu, elle est en effet désactivée la plupart du temps. Les sauvegardes en place permettent de reconstruire le service dans un délai raisonnable de quelques jours.

## 5.8 Fin de vie de l'IGC

### 5.8.1 Transfert d'activité

Sans objet.

### 5.8.2 Cessation d'activité

Si Worldline décidait d'interrompre cette activité MediaCert, elle en informerait ses partenaires avant la cessation de l'activité en respectant un préavis.

A l'échéance prévue, une séance de clés est organisée pour procéder à la révocation des AC filles (application du plan de cessation d'activité des AC filles), puis à la révocation du certificat de l'AC Racine MediaCert et à la destruction de sa clé privée et des secrets associés.

# 6 Mesures de sécurité techniques

## 6.1 Génération et installation de bi-clés

### 6.1.1 Génération des bi-clés de l'AC racine

La génération des bi-clés de l'AC est réalisée dans un HSM dont le niveau de qualification est décrit au chapitre 6.2.11 du présent document.

Cette génération a lieu lors d'une cérémonie de clés dans les locaux sécurisés de Worldline. Elle implique différents rôles de confiance pour l'activation du HSM et du logiciel de PKI utilisés.

### 6.1.2 Transmission de la clé privée d'une AC fille

Sans objet.

### 6.1.3 Transmission de la clé publique d'une AC fille

Elle est transmise sous forme de CSR au format PKCS#10 qui permet d'en contrôler l'intégrité.

### 6.1.4 Transmission de la clé publique de l'AC racine aux utilisateurs

Elle est transmise via son certificat racine lors des cérémonies de signature des AC filles en même temps que le certificat fille.

### 6.1.5 Taille des clés

Selon l'échéance de l'AC fille et l'enjeu dans l'usage des certificats émis la taille de ses clés pourra être de 2048 ou 4096 bits.

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

La qualité de la génération est vérifiée lors de la réception de la CSR par l'Autorité de Certification. Les tailles de clefs doivent correspondre au gabarit de l'AC fille concernée.

### 6.1.7 Objectifs d'usage de la clé

Les clés privées de l'AC racine et des AC fille est limité à la signature de certificats et de CRL. Ceci est encadré par l'extension *KeyUsage* avec les valeurs *keyCertSign* et *CRLSign*. Cette extension est critique.

## 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

La génération des bi-clés de l'AC est réalisée dans un HSM dont le niveau de qualification est décrit au chapitre 6.2.11 du présent document.

Il se trouve notamment dans les centres informatiques sécurisés de Worldline à Vendôme et Bruxelles.

### 6.2.2 Contrôle de la clé privée par plusieurs personnes

La génération et l'activation de la clé privée de l'AC mettent en œuvre un système de partage de secrets entre plusieurs rôles de confiance. Ces procédures sont détaillées dans le script de cérémonie de clés.

### 6.2.3 Séquestre de la clé privée

Les clés privées de l'AC racine ou des AC filles ne sont pas séquestrées.

### 6.2.4 Copie de secours de clé privée

La clé privée de l'AC racine est sauvegardée via les procédures du constructeur de HSM.
La sauvegarde a la forme d'un fichier contenant un cryptogramme de la clé privée chiffrée par la clé maitre du HSM.

### 6.2.5 Archivage de la clé privée

Les clés privées de l'AC racine et de ses AC filles ne sont pas archivées.

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

Ce transfert n'est possible que via les procédures du constructeur de sauvegarde/restauration. Cf. § 6.2.4.

### 6.2.7 Stockage de la clé privée dans un module cryptographique

La clé privée est stockée dans un HSM évalué comme défini au chapitre 6.2.11 ou chiffrée par la clé maîtresse du HSM en cas de sauvegarde externe, conformément aux procédures de sauvegarde du constructeur.

### 6.2.8 Méthode d'activation de la clé privée

La clé privée d'AC ne peut être activée qu'au cours d'une cérémonie de clés, en présence de plusieurs rôles de confiance et qui détiennent des données d'activation du HSM et des parties de sa clé maître.

### 6.2.9 Méthode de désactivation de la clé privée

Elle est désactivée via sa suppression du HSM après sauvegarde ainsi que la désinstallation du logiciel du HSM.

### 6.2.10 Méthode de destruction des clés privées

La destruction peut être opérée par un administrateur HSM après son activation. En complément toutes les sauvegardes doivent être détruites soit via un logiciel de suppression sûr soit par destruction matérielle du support amovible de sauvegarde.

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

Le HSM utilisé est certifié FIPS 140-2 L3.

## 6.3 Autres aspects de la gestion des bi-clés

### 6.3.1 Archivage des clés publiques

Les clés publiques de la racine et de chaque fille sont archivées parmi les données de l'IGC MediaCert.

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

L'AC racine ne peut pas émettre de certificat d'AC fille dont la durée de vie est supérieure à la sienne. Les durées de vie des bi-clés et des certificats sont notamment définies au sein même des certificats.

## 6.4 Données d'activation

### 6.4.1 Génération et installation des données d'activation

Les données d'activation du HSM sont générées lors de la cérémonie de clés d'initialisation de l'AC Racine.

### 6.4.2 Protection des données d'activation

Ces données sont sous la responsabilité des porteurs de secret qui disposent de coffres pour les conserver au sein d'un environnement sécurisé.

### 6.4.3 Autres aspects liés aux données d'activation

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

## 6.5 Mesures de sécurité des systèmes informatiques

### 6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Le serveur hébergeant l'AC racine répond aux objectifs de sécurité suivants :

- identification et authentification des utilisateurs pour l'accès au système ;
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle, …) ;
- gestion des comptes et droits des utilisateurs ;
- protection des accès par pare-feu interne ;
- traçabilité des opérations.

### 6.5.2 Niveau de qualification des systèmes informatiques

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

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

### 6.6.1 Mesures de sécurité liées au développement des systèmes

Sans objet dans la mesure où l'AC s'appuie uniquement sur des progiciels externes sans développement complémentaire.

### 6.6.2 Mesures liées à la gestion de la sécurité

Si des évolutions de certains progiciels sont nécessaires, ils sont testés au préalable sur un environnement de recette. Les changements qui en découlent sont pris en compte dans les manuels d'exploitation et tracés.

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

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

## 6.7 Mesures de sécurité réseau

Le serveur d'AC n'est connecté à aucun réseau en dehors des opérations de cérémonies de clés lors desquelles un réseau privé et fermé est spécialement monté.

## 6.8 Horodatage / Système de datation

L'horloge du serveur est synchronisée sur une source externe fiable.

# 7 Profils des certificats, OCSP et des LCR

## 7.1 Profil des certificats

Les certificats émis par l'AC racine contiennent les champs de base suivants :

- **Version** : version du certificat X.509 (v3) ;
- **Serial number** : numéro de série du certificat (valeur unique pour chaque certificat émis) ;
- **Signature** : OID de l'algorithme utilisé par l'AC pour signer le certificat ;
- **Issuer** : valeur du DN (X.500) de l'AC émettrice du certificat ;
- **Validity** : date d'activation et d'expiration du certificat ;
- **Subject** : valeur du DN (X.500) de l'équipement ;
- **Subject Public Key Info :** OID de l'algorithme et valeur de la clé publique de l'équipement ;
- **Extensions** : liste des extensions.

A ces champs s'ajoutent des extensions qui peuvent être critiques ou non critiques. Celles-ci sont une combinaison d'extensions provenant des CSR des AC filles et d'extensions imposées par le gabarit de certificat au niveau de l'AC racine.

### 7.1.1 Certificat de l'AC Racine de l'IGC Mediacert

L'ensemble de ces champs est signé par la clé privée de l'AC racine. Deux champs sont utilisés pour cette signature :

- **Signature** : OID de l'algorithme utilisé ;
- **Signature Value** : résultat de la signature.

Le certificat racine est défini ci-dessous. Il est présenté en deux parties : les champs de base et les extensions. Les informations décrites ci-dessous sont indicatives, les données du certificat racine faisant foi.

***Champs de base***

| **Champs** | | **Valeur** |
|---|---|---|
| Version | | V3 (Valeur : 2) |
| Serial number | | 66:a7:15:98:de:e3:46:da |
| Signature | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Issuer | C | FR |
| | O | Atos Worldline |
| | OI | 0002 378901946 |
| | CN | AC Racine – Root CA – 2012 |
| Validity | | 21 ans |
| Subject | C | FR |
| | O | Atos Worldline |
| | OU | 0002 378901946 |
| | CN | AC Racine – Root CA – 2012 |
| Subject Public Key Info | | RSA 4096 bits |

***Extensions***

| **Champs** | **Critique** | **Valeur** |
|---|---|---|
| Authority Key Identifier | Non | 11 28 8e f4 56 7b cf bd 80 cb 31 9d 42 82 ed 4a 5c ef 25 a7 |

| | | | |
|---|---|---|---|
| Subject Key Identifier | | Non | 11 28 8e f4 56 7b cf bd 80 cb 31 9d 42 82 ed 4a 5c ef 25 a7 |
| Key Usage | | Oui | keyCertSign, CRLSign |
| Basic Constraint | Certificate Authority | Non | vrai |
| | Maximum Path Length | | 4 |
| Certificate Policies | policyIdentifier | Non | 1.2.250.1.111.12.4.1 |
| | policyQualifierId | | 1.3.6.1.5.5.7.2.1 |
| | qualifier | | http://www.mediacert.com |
| CRL Distribution Points | | Non | http://root.mediacert.com/LatestCRL[1] |

### 7.1.2 Certificats des AC Filles

Le gabarit d'une AC Fille doit être décrit dans sa propre Politique de Certification. Il doit respecter l'ensemble des contraintes techniques définies dans la présente Politique de Certification.

## 7.2 Profil des LAR

Les LAR émises comprennent les champs suivants :

- **Version** : version du standard de CRL(v2 – RFC 5280) ;
- **Signature** : OID de l'algorithme utilisé par l'AC pour signer la LAR ;
- **Issuer** : valeur du DN (X.500) de l'AC émettrice de la LAR ;
- **This Update** : date de génération de cette mise à jour de la LAR ;
- **Next Update** : date de génération de la prochaine mise à jour de la LAR ;
- **Revoked Certificates** : liste des certificats révoqués avec leur numéro de série, la date de révocation et le motif ;
- **CRL Extensions** : liste des extensions.

L'ensemble de ces champs est signé par la clé privée de l'AC racine. Deux champs sont utilisés pour cette signature :

- **Signature** : OID de l'algorithme utilisé ;
- **Signature Value** : résultat de la signature.

Le gabarit utilisé est défini ci-dessous. Il est présenté en deux parties : les champs de base et les extensions.

***Champs de base***

| Champs | | Valeur |
|---|---|---|
| Version | | V2 (Valeur : 1) |
| Signature | | sha256WithRSAEncryption (1.2.840.113549.1.1.11) |
| Issuer | C | FR |
| | O | Atos Worldline |
| | OU | 0002 378901946 |
| | CN | AC Racine – Root CA – 2012 |
| This Update | | Date d'émission de la LCR |
| Next Update | | Date d'émission de la LCR + 12 mois |

[1] Cette URL est donnée à titre indicatif. L'URL qui fait foi est celle qui figure dans le certificat.

| | |
|---|---|
| Revoked Certificates | Liste des certificats d'AC révoqués |

***Extensions***

| Champs | Critique | Valeur |
|---|---|---|
| Authority Key Identifier | Non | 11 28 8e f4 56 7b cf bd 80 cb 31 9d 42 82 ed 4a 5c ef 25 a7 |
| CRL Number | Non | Numéro de la LAR |

## 7.3 Profil OCSP

L'AC racine ne met pas en œuvre de service OCSP.

# 8 Audit de conformité et autres évaluations

## 8.1 Fréquences et / ou circonstances des évaluations

Worldline procède à un contrôle de conformité par défaut tous les 2 ans impliquant une cérémonie de clefs..

## 8.2 Identités / qualifications des évaluateurs

L'audit est effectué par une entité indépendante de l'AC Racine MediaCert en charge des contrôles de conformité.

## 8.3 Relations entre évaluateurs et entités évaluées.

Cette entité est différente de celle qui administre l'AC Racine MediaCert.

## 8.4 Sujets couverts par les évaluations

Ces contrôles sont faits par sondage et visent principalement à vérifier le respect de cette PC.

## 8.5 Actions prises suite aux conclusions des évaluations

Les remarques sont prises en compte dans un délai raisonnable et au plus tard pour la prochaine séance de clés (signature ou révocation d'AC, publication de LAR).

## 8.6 Communication des résultats

L'audit fait l'objet d'un rapport interne.

# 9 Autres problématiques métiers et légales

## 9.1 Tarifs

Sans objet, il s'agit d'une IGC interne.

## 9.2 Responsabilité financière

Sans objet. La responsabilité éventuelle serait portée au niveau AC fille.

## 9.3 Confidentialité des données professionnelles

Worldline en tant que responsable de l'IGC MediaCert met en œuvre les moyens nécessaires pour assurer la protection des données confidentielles dont :

- la clé privée de l'AC racine ;
- les données d'activation de cette clé et du HSM utilisé ;
- les informations et documents techniques de l'AC.

## 9.4 Protection des données personnelles

Sans objet, les données traitées par l'IGC MediaCert ne contiennent aucune donnée personnelle.

## 9.5 Droits sur la propriété intellectuelle et industrielle

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

## 9.6 Interprétations contractuelles et garanties

L'AC Racine MediaCert s'assure de :

- la protection (intégrité et confidentialité) de la clé privée lors de la génération et durant toute la période de validité de la clé ainsi que des données d'activation ;
- l'utilisation des bi-clés et des certificats dans le cadre pour lesquelles elles ont été émises, conformément aux applications définies dans la présente PC au chapitre 1.4 ;
- la publication des informations publiques citées au chapitre 2.2 du présent document, de façon durable et sécurisée ;
- la soumission aux contrôles de conformité effectués par des auditeurs externes ou internes et la mise en œuvre de leurs préconisations ;
- la bonne documentation des procédures internes de fonctionnement et d'utilisation ;
- la maintenance de la cohérence entre la présente PC et la DPC qui lui est associée ;
- la sensibilisation du personnel de confiance à leurs engagements.

Worldline s'assure que la gestion des certificats est conforme aux exigences indiquées dans la PC et dans la présente DPC de l'IGC MediaCert.

## 9.7 Limite de garantie

Sans objet.

## 9.8 Limite de responsabilité

Sans objet.

## 9.9 Indemnités

Sans objet.

## 9.10 Durée et fin anticipée de validité de la PC

### 9.10.1 Durée de validité

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

### 9.10.2 Fin anticipée de validité

La mise en conformité suite à une évolution de la PC n'impacte pas les certificats déjà émis.

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

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

## 9.11 Notifications individuelles et communications entre les participants

En cas de changement significatif sur l'AC racine, les entités responsables des AC filles sont informées à l'avance, dans des délais raisonnables.

## 9.12 Amendements à la PC

Le Comité MediaCert est en charge de toute modification de la présente PC. La PC peut évoluer pour être en cohérence avec l'AC. En cas de changement majeur l'OID doit être modifié ce qui entraine un renouvellement anticipé de l'AC.

## 9.13 Dispositions concernant la résolution de conflits

Les conflits éventuels se règlent en interne entre :

- l'entité responsable de cette AC ;
- le comité MediaCert.

## 9.14 Juridictions compétentes

Sans objet.

## 9.15 Conformité aux législations et réglementations

Sans objet.

## 9.16 Dispositions diverses

Sans objet.

## 9.17 Autres dispositions

Sans objet.

# 10 Annexes

| DOCUMENTATION TECHNIQUE DE L'IGC MEDIACERT | |
|---|---|
| **Référence** | **Description** |
| [DPC] | Déclaration des Pratiques de Certification Racine IGC MediaCert<br>Autorité de Certification MediaCert<br>Référence : ROOT DPC 0021 |