POLITIQUE DE CERTIFICATION DES AC HORS-LIGNE DU TSP MEDIACERT

AUTEUR(S)	:	F. Da Silva
N° DE DOCUMENT	:	WLM-TSP-F104
VERSION	:	1.2
STATUT	:	Final
SOURCE	:	Worldline
DATE DU DOCUMENT	:	31 Décembre 2017
NOMBRE DE PAGES	:	51
PROPRIETAIRE	:	Comité MediaCert

Rôle	Nom	Signature	Date
Relecteur 1 – Resp. AC	Cyril Lootvoet	Cyril Lootvoet	18/09/2018
Relecteur 2 – RSSI	Nicolas Abrioux	Nicolas Abrioux	18/09/2018
Fonction d'assurance qualité	Franck Da Silva	Franck Da Silva	18/09/2018
Propriétaire du document	Comité MediaCert	Cyril Lootvoet	18/09/2018

CYRIL LOOTVOET

Digitally signed by CYRIL LOOTVOET
DN: C=FR, L=SECLIN, O=Atos Worldline, OU=fr01.awl.atosorigin.net, SN=LOOTVOET, G=CYRIL, CN=CYRIL LOOTVOET, OID.0.9.2342.19200300.100.1.1=A536912, E=cyril.lootvoet@worldline.com
Reason: Document validé par le Comité MediaCert
Location:
Date: 2018-09-18 16:24:40

Table des Matières

Liste des modifications

Version	Date	Description	Auteur(s)
0.1	31/11/2017	Initialisation du document	F. Da Silva N. Abrioux V. Dumond
1.0	29/03/2018	Validation du document en Réunion Sécurité	Comité MediaCert
1.1	05/07/2018	Ajout de raisons de révocation conformément à l'update de la 319 411-1 et 319 411-2	F. Da Silva
1.2	18/09/2018	Modification du gabarit de certificat des AC Intermédiaires	F. Da Silva

1 Introduction

1.1 Présentation générale

Le *Trust Service Provider* MediaCert, établi par Worldline, fournit un ensemble de Services de Confiance et est, par conséquent, soumis au règlement « eIDAS » n°910/2017 du Parlement européen et du Conseil européen en matière d'identification électronique et de services de confiance pour les transactions électronique au sein du marché intérieur.

Ce document décrit la Politique de Certification de deux AC opérées par le TSP MediaCert :

une AC Racine, visant à délivrer des Certificats à des AC intermédiaires, y compris l'AC Horodatage présentée dans le présent document et éventuellement à d'autres services de confiance ;

une AC Horodatage, fille de l'AC Racine, visant à délivrer exclusivement des Certificats de scellement à des unités d'horodatages, opérées par le TSP MediaCert.

Ces deux AC s'inscrivent au sein des services de confiance de MediaCert suivant le schéma ci-dessous.

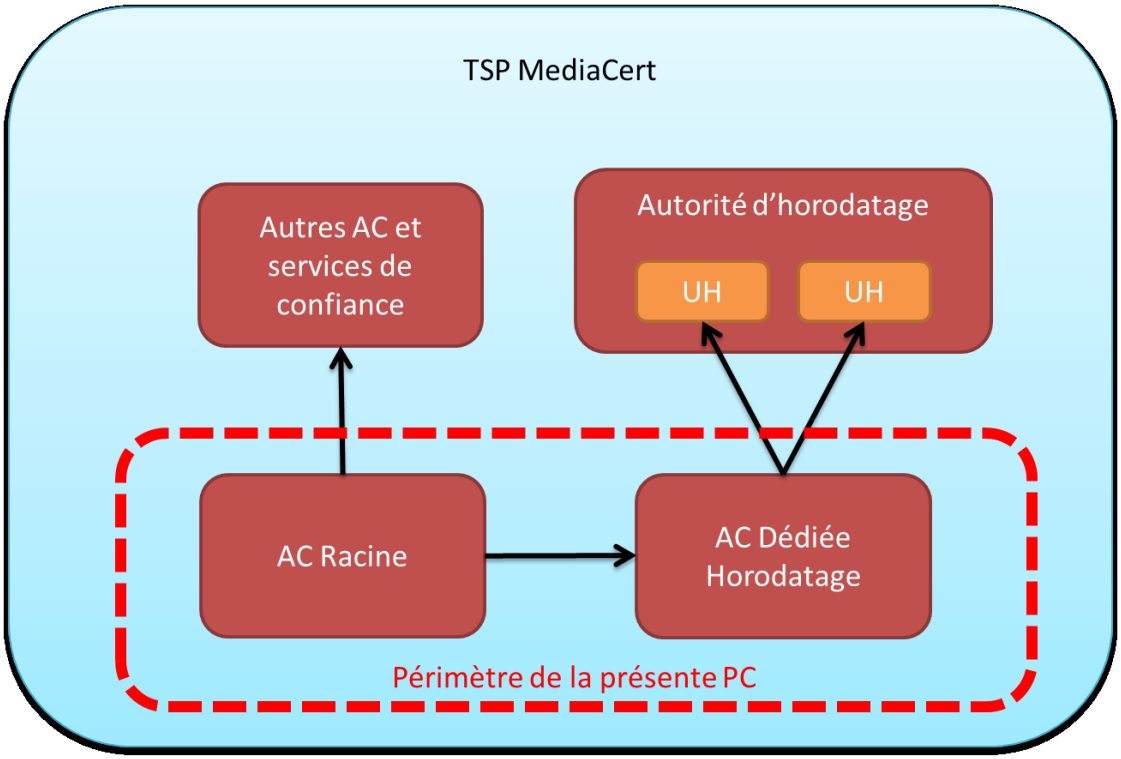

Figure 1 - Périmètre d'application de la présente PC-DPC

Dans ce cadre, le présent document présente :

les exigences auxquelles sont soumises chacune de ces AC hors lignes opérées par le TSP MediaCert ;

l'organisation mise en place pour assurer la fourniture des services ;

les mesures de sécurités appliquées.

Par ailleurs, étant des Services de Confiance de MediaCert, l'ensemble des exigences et des pratiques de la [PG] sont, sauf mention contraire, applicables au périmètre de ces AC hors lignes.

Celles-ci sont toutes les deux opérées dans un environnement hors-ligne.

La délivrance de Certificats aux porteurs de Certificats finaux par les AC Intermédiaires (hormis l'AC Horodatage) sera décrite dans les PC et DPC des AC Intermédiaires. Elle est, de ce fait, hors du périmètre du présent document.

L'AC Horodatage vise à être conforme aux exigences de la norme [ETSI 319 411-2] pour le niveau QCP.
L'AC Racine est opérée dans des conditions d'exploitation similaires mais ne vise pas de conformité particulière.

1.2 Identification du document

Le présent document est la politique de certification de l'AC Racine et de l'AC Horodatage MediaCert. Il contient également la partie publique de la Déclaration des Pratiques de Certification de ces deux AC.

Eléments	Valeur
Titre	Politique de Certification des AC hors-ligne du TSP MediaCert
Référence document	WLM-TSP-F104
OID	1.2.250.1.111.20.3.1.1 pour l'AC Racine 1.2.250.1.111.20.3.1.2 pour l'AC Horodatage
Version	1.2
Auteur	F. Da Silva

Les OID du présent document sont basés sur l'OID « **1.2.250.1.111.20.3** » : 1.2.250.1.111.20.3.**z.w** où :

- z : version majeure de la présente politique (ex : version 3.1 → 3) ;
- w : spécification des AC concernées par la présente PC avec :
  - AC Racine → w=1 ;
  - AC Horodatage → w=2.

Des informations complémentaires sont disponibles au sein de la Politique Générale [PG].

Ce présent document sera appelé « PC-DPC » tout le long du document.

Sauf mention contraire, les exigences du présent document sont applicables à ces deux (2) AC. Les exigences applicables à une seule AC sont précédées de la mention :

[Racine] pour l'AC Racine d'OID 1.2.250.1.111.20.3.1.1 ;

[Horodatage] pour l'AC Horodatage d'OID 1.2.250.1.111.20.3.1.2.

1.3 Entités intervenant dans l'IGC

1.3.1 Autorité de Certification

L'AC a en charge la fourniture des prestations de gestion des Certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuie pour cela sur une infrastructure technique : une Infrastructure de Gestion de Clés (IGC). Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats. Dans le cadre de ce document, nous nous intéressons uniquement aux AC opérées hors ligne par MediaCert. Ces autorités ont pour objectif de fournir des Certificats aux autres Services de Confiance opérés par le TSP MediaCert.

1.3.2 Autorité d'Enregistrement

L'Autorité d'Enregistrement est la composante de l'IGC en charge de l'identification des porteurs. Pour les AC dans le périmètre de cette PC-DPC, le TSP MediaCert opère elle-même sa propre Autorité d'Enregistrement et n'enregistrera comme porteur que des Services de Confiance opérés par le TSP MediaCert.

1.3.3 Porteurs de Certificats

Dans le cadre de cette PC-DPC, le porteur de Certificat est :

[Racine] un service de confiance du TSP MediaCert certifié par l'AC Racine telle qu'une Autorité de Certification dédiée à l'horodatage ou toute autre Autorité de Certification Intermédiaire ;

[Horodatage] une Unité d'Horodatage opérée par le Service d'Horodatage du TSP MediaCert.

Le porteur n'est pas, dans chacun des cas, une personne physique. Le porteur sera identifié dans le sujet du Certificat grâce :

au nom du service de confiance ;

[Racine] nom de l'ACI en tant que nom commun ;

[Horodatage] nom de l'unité d'horodatage ;

à l'organisation qui ne peut être que « Worldline ».

Pour réaliser la demande, le porteur de Certificat sera représenté par une personne physique, le Responsable de Certificat, dûment mandaté.

1.3.4 Utilisateurs de Certificats

Les Utilisateurs vérifient la validité du Certificat à l'aide :

des informations contenues dans le Certificat (date de validité, …) ;

d'informations complémentaires fournies par l'AC (statut de révocation du Certificat).

1.3.5 Autres participants

Sans objet.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

L'usage des Certificats diffère pour chacune des AC.

Les Certificats décrits dans la présente PC-DPC sont destinés exclusivement à un usage interne au TSP MediaCert. Il n'est donc pas délivré de Certificats de test pour des tierces parties. Le TSP MediaCert ne prévoit pas d'émettre des Certificats de tests depuis les environnements de production.

[Racine] Les Certificats émis par l'AC Racine sont uniquement destinés à certifier les Services de Confiance offerts par le TSP MediaCert. La présente PC-DPC n'envisage que la fourniture de Certificat d'AC Intermédiaire mais les versions futures de la présente PC-DPC pourraient envisager éventuellement d'autres profils de Certificats destinés à d'autres types de services de confiance si cela s'avérait nécessaire.

[Horodatage] Les Certificats émis par l'AC Horodatage du TSP MediaCert sont uniquement dédiés à des unités d'horodatage opérées par l'Autorité d'Horodatage du TSP MediaCert (AH) pour des opérations de scellement et d'émission de jetons d'horodatage.

1.4.2 Domaines d'utilisation interdit

Tout autre usage que celui défini dans le paragraphe précédent est interdit par la présente PC-DPC. De plus, le Certificat doit être utilisé dans la limite des lois et réglementations en vigueur (cf. chapitre 9.14).

1.5 Gestion de la PC

1.5.1 Entité gérant la politique

L'entité gérant la présente politique est indiquée dans la [PG].

1.5.2 Point de contact

Le point de contact est indiqué dans la [PG].

1.5.3 Entité déterminant la conformité des pratiques de la PC

Cette entité est décrite dans la [PG].

1.5.4 Procédure d'approbation de la conformité de la PC/DPC

La procédure d'approbation de la présente PC-DPC est décrite dans la [PG].

1.6 Définition et abréviations

1.6.1 Définitions

Une liste des principales définitions des termes techniques employés dans la présente PC-DPC est présentée ci-dessous :

Abonné : entité/organisation qui bénéficie d'un ou de plusieurs services de confiance délivrés par le TSP MediaCert.

Bi-clé : couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptographie basée sur des algorithmes asymétriques (RSA par exemple).

Certificat : élément de données normalisé X509 permettant d'associer une clé publique à son détenteur. Un Certificat contient des données comme l'identité du détenteur, sa clé publique, l'identité de l'organisme ayant émis le Certificat, la période de validité, un numéro de série, une empreinte (*thumbprint*) ou bien encore les critères d'utilisation. Le tout est signé par la clé privée de l'Autorité de Certification ayant émis le Certificat.

Service de Certification : service qui produit des Certificats et, plus généralement, assure leur gestion (fabrication, livraison, révocation, publication, journalisation, archivage) conformément à une politique de certification.

Service de Confiance : un service de confiance est un service électronique qui consiste en :

la délivrance de Certificats de signature électronique, de cachet électronique et d'authentification de site internet ; ou

la validation des signatures électroniques et des cachets électroniques ; ou

la conservation des signatures électroniques et des cachets électroniques ;

l'horodatage électronique ;

l'envoi recommandé électronique.

Service d'Horodatage : service qui produit des Contremarques de temps et plus généralement assure leur gestion conformément à une politique d'horodatage.

Titulaire / Porteur : désigne une entité, personne physique ou morale, à qui est destinée le Certificat émis par l'une des Autorités de Certification régies par la présente politique.

Utilisateur : désigne une entité, personne physique ou morale, amené à utiliser des Certificats émis par les AC régies par la présente PC-DPC afin d'en vérifier la validité ainsi que l'éventuel lien avec les données signées.

1.6.2 Acronymes

Une liste des acronymes employés dans la présente PG est présentée ci-dessous :

AC : Autorité de Certification ;
ACI : Autorité de Certification Intermédiaire ;
AFNOR : Association Française de Normalisation ;
AH : Autorité d'Horodatage ;
CSR : Certificate Signing Request ;
DN : Distinguished Name ;
DTPG : Documentation Technique des Pratiques Générales ;
EIDAS : Electronic IDentification And Signature ;
HSM : Ressource Cryptographique Matérielle (*Hardware Security Module*) ;

IGC : Infrastructure de Gestion de Clés (*Public Key Infrastructure*) ;
LCR : Liste des Certificats Révoqués ;
OID : Object IDentifier ;
PC-DPC : Politique de Certification – Déclaration des Pratiques de Certification ;
PH-DPH : Politique d'Horodatage – Déclaration des Pratiques d'Horodatage ;
PCRA : Plan de Continuité et de Reprise d'Activités ;
PG : Politique Générale du TSP MediaCert ;
PSI : Politique de Sécurité de l'Information de Worldline ;
RGPD : Règlement Général pour la Protection des Données ;
SIEM : Security Information & Event Management ;
SOC : Security Operation Center ;
SSI : Sécurité des Systèmes d'Information ;
TSP : Prestataire de Services de Confiance (*Trust Service Provider*) ;
UH : Unité d'Horodatage.

1.7 Références

1.7.1 Réglementations

Référence	Description
[CNIL]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004 Nota : la présente réglementation sera remplacée en 2018 par [RGPD]
[EIDAS]	REGLEMENT (UE) N°910 DU PARLEMENT EUROPEEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

1.7.2 Références réglementaires techniques

Référence	Description
[ETSI 119 312]	ETSI EN 119 312 v1.2.1 (2017-05) Electronic Signature and Infrastructures (ESI); Cryptographic Suites
[ETSI 319 401]	ETSI EN 319 401 v2.2.1 (2018-04) Electronic Signature and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI 319 411-1]	ETSI EN 319 411-1 v1.2.2 (2018-04) Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI 319 411-2]	ETSI EN 319 411-2 v2.2.2 (2018-04) Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[ISO 27001 : 2013]	ISO/IEC 27001 : 2013 Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information - Exigences
[ISO 27002 : 2013]	ISO/IEC 27002 : 2013 Code de bonnes pratiques pour le management de la sécurité de l'information
[RFC 3647]	Network Working Group – November 2003 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RGS B1]	Référentiel Général de Sécurité v2.0 - Annexe B1 (2014-02) Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) Mécanismes cryptographiques : règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques

1.7.3 Référentiel du TSP MediaCert

Référence	Description
[PG]	Politique Générale du TSP MediaCert TSP MediaCert Référence : WLM-TSP-F094 OID : 1.2.250.1.111.20.1.1

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

2.1 Entité chargée de la mise à disposition des informations

L'entité décrite dans le document [PG] au chapitre correspondant est l'entité chargée de mettre à disposition les informations devant être publiées décrites au sein du chapitre 2.2 du présent document. Le site de publication est décrit dans la [PG].

2.2 Informations devant être mises à disposition

Sur le périmètre du présent document, les informations publiées sont les suivantes :

la présente PC-DPC ;

la Liste des Certificats d'Autorité de Certification Révoqués (LAR) par l'AC Racine ;

la Liste des Certificats d'Unité d'Horodatage Révoqués (LCR) par l'AC Horodatage ;

le Certificat auto-signé de l'AC Racine en cours de validité ;

le Certificat de l'AC Horodatage en cours de validité.

La présente PC-DPC est publiée au format PDF/A.

2.3 Délais et fréquences de publication

L'ensemble des exigences et pratiques décrites dans la [PG] au chapitre correspondant s'appliquent.
Les exigences et pratiques complémentaires spécifiques de la présente section s'appliquent également.

Les politiques de certification sont remises à jour et publiées en cas de changement majeur et à minima tous les deux (2) ans.

Les Certificats de l'AC Racine sont diffusés ou mis en ligne préalablement à toute diffusion de Certificats d'AC intermédiaire ou de LAR.

Les Certificats de l'AC Horodatage sont diffusés ou mis en ligne préalablement à toute diffusion de Certificats d'Unité d'Horodatage ou de LCR.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des exigences et pratiques décrites dans la [PG] au chapitre correspondant s'appliquent.

3 Identification et authentification

3.1 Nommage

3.1.1 Types de noms

Les noms utilisés dans un Certificat sont décrits selon la norme [ISO/IEC 9594] (*Distinguished Name*), chaque Titulaire ayant un nom distinct (DN).

3.1.2 Nécessité d'utilisation de noms explicites

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

Les profils des Certificats sont décrits dans au chapitre 7.1.

3.1.3 Anonymisation ou pseudonymisation des porteurs

Les Certificats objets de la présente PC-DPC ne peuvent en aucun cas être anonymes. Les noms fournis pour l'établissement d'un Certificat ne peuvent en aucun cas être des pseudonymes.

3.1.4 Règles d'interprétation des différentes formes de noms

Le nom de l'AC est défini par le Comité MediaCert.

3.1.5 Unicité des noms

Un code distinctif ajouté assure le caractère unique du DN en cas d'homonymie. Ce code correspond à l'année de début de validité du Certificat d'AC.

En cas de Certificat d'AC devant être généré avec une même date de début de validité, un index supplémentaire unique est ajouté (2018-1, 2018-2 par exemple).

[Horodatage] Un identifiant unique assure le caractère unique du CN du Certificat des Unités d'Horodatage.

3.1.6 Identification, authentification et rôle des marques déposées

Pour les marques, dénominations sociales ou autres signes distinctifs, le TSP MediaCert n'effectue aucune recherche d'antériorité ou autre vérification. Il appartient au demandeur ou au Titulaire de vérifier que la dénomination demandée ne porte pas atteinte à des droits de propriété de tiers.

3.2 Validation initiale de l'identité

L'enregistrement d'un futur Titulaire se fait directement auprès de l'AE par une personne physique.

La demande est réalisée conformément à ce qui est définit au chapitre 4.1.

3.2.1 Méthode pour prouver la possession de la clé privée

[Racine] Le demandeur présente une CSR signée avec la clé privée de l'AC Intermédiaire concernée ou du Service de Confiance concerné.

[Horodatage] Le demandeur présente une CSR signée avec la clé privée de l'UH concernée.

3.2.2 Validation de l'identité d'un organisme

Comme définit au chapitre 3.2.5, seul le TSP MediaCert est destinataire des Certificats émis dans le cadre de la présente PC-DPC.

3.2.3 Validation de l'identité d'un individu

L'identité d'un individu autorisé à effectuer une demande de création de Certificat dans le cadre de la présente PC-DPC est assurée par le fait qu'il opère l'un des rôles de confiance suivant au sein TSP MediaCert :

Responsable du TSP ;

Responsable adjoint du TSP.

La vérification d'identité du demandeur est notamment réalisée lors de la remise de la demande de Certificat via un face à face physique (cf. chapitre 4.1.2).

[Racine] La validation de l'identité du demandeur est réalisée lors de la phase de préparation de la cérémonie des clés de l'AC Intermédiaire.

[Horodatage] La validation de l'identité du demandeur est réalisée lors de la phase de préparation de la cérémonie des clés de l'UH.

3.2.4 Informations non vérifiées du porteur

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

3.2.5 Validation de l'autorité du demandeur

[Racine] La présente version de la PC-DPC n'envisage que des émissions de Certificats à des AC Intermédiaires opérées par le TSP MediaCert. De ce fait, aucune vérification particulière n'est faite. Seul le TSP MediaCert est habilité à réaliser une demande de Certificat d'AC Intermédiaire.

[Horodatage] La présente version de la PC-DPC n'envisage que des émissions de Certificats à des UH opérées par le TSP MediaCert. De ce fait, aucune vérification particulière n'est faite. Seul le TSP MediaCert est habilité à réaliser une demande de Certificat d'UH.

3.2.6 Certification croisée d'AC

Sans objet.

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

Un nouveau Certificat ne peut pas être fourni sans renouvellement de la bi-clé correspondante. Le renouvellement se traduit alors par une nouvelle demande de Certificat et bénéficie des mêmes procédures que pour une demande initiale (cf. chapitre 3.2 de la présente PC-DPC).

3.3.1 Identification et validation pour un renouvellement courant

La procédure est identique à une demande initiale.

3.3.2 Identification et validation pour un renouvellement après révocation

La procédure est identique à une demande initiale.

3.3.3 Identification d'une demande de révocation

[Racine] La demande de révocation de clé pour une AC Intermédiaire signée par l'AC Racine ne peut émaner que d'une personne autorisée et est validée formellement avant prise en compte. Le Certificat de l'AC Racine étant un Certificat auto-signé, il ne peut pas être révoqué. En cas de compromission de la clé privée correspondante au Certificat de l'AC Racine, le TSP MediaCert réalisera l'ensemble des actions prévues en cas de compromission (cf. chapitre 5.7.3).

[Horodatage] La demande de révocation de clé pour une UH signée par l'AC Horodatage ne peut émaner que d'une personne autorisée et est validée formellement avant prise en compte (cf. chapitre 4.9).

4 Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Le demandeur de Certificat est le TSP MediaCert, représenté par Responsable du TSP MediaCert ou l'un de ses adjoints (cf. chapitre 3.2.3).

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

L'établissement d'une demande de Certificat doit être établi par le futur Titulaire. Cette demande doit contenir le formulaire de demande de création de Certificat, signé par le demandeur et remis en face à face au TSP 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 responsable du TSP MediaCert ou l'un de ses adjoints (cf. chapitre 3.2.3). Cette personne ne peut pas être la même personne que celle ayant fait la demande.

L'identification et la validation de la demande sont réalisées de la façon suivante :

l'identité physique du demandeur et son autorité sont vérifiées conformément aux exigences du chapitre 3.2 ;

le destinataire de la demande (cf. paragraphe ci-dessus) vérifie que le dossier de demande (cf. chapitre 4.1.2) est complet. Notamment que les CGU en vigueur lors de la demande sont signées par le TSP MediaCert.

L'AE conserve ensuite une trace des demandes de Certificat présentés (cf. chapitre 5.4.1).

4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, la personne ayant traité la demande informe le demandeur en précisant le motif.

4.2.3 Durée d'établissement du certificat

L'AC s'efforce de traiter la demande de Certificat dans un délai raisonnable. Néanmoins, il n'y a aucune restriction concernant la durée maximale ou minimale de traitement.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

La validation de la demande déclenche l'opération technique de génération du Certificat. Celle-ci contient les actions suivantes :

vérification que la demande de Certificat provient bien d'un membre de confiance du TSP MediaCert autorisé par la présente PC-DPC à effectuer une demande de Certificat ;

génération de la CSR ;

vérification technique de la CSR ;

soumission de la CSR à l'AC et génération du Certificat ;

vérification du Certificat,

délivrance du Certificat.

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

Le porteur du Certificat est notifié via une application interne à Worldline.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

L'acceptation du Certificat signé par l'AC est consignée sur le procès-verbal de la cérémonie des clés.

4.4.2 Publication du certificat

Le Certificat fait l'objet d'une publication sur le site de publication (cf. chapitre 2.2) avant tout utilisation en production de la clé privée associée.

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 Usage de la clé privée

4.5.1.1 Clé privée des AC

[Racine] La clé privée de l'AC Racine est utilisée pour:

signer son propre Certificat d'AC Racine (Certificat auto-signé) ;

signer les Certificats des AC Intermédiaires ou autres Services de Confiance ;

signer la liste des AC Intermédiaires révoquées (LAR).

[Horodatage] La clé privée de l'AC Horodatage est utilisée pour:

signer les Certificats d'UH ;

signer la liste des UH révoquées (LCR).

Ces usages sont explicitement définis dans les extensions des certificats.

4.5.1.2 Clé privée des porteurs

[Racine] La clé privée d'AC intermédiaire, associée à un Certificat émis par l'AC Racine est destinée à :

signer les Certificats des porteurs finaux ;

signer la liste des Certificats révoquées (CRL), le cas échéant ;

signer des Certificats de répondeurs OCSP, le cas échéant.

[Horodatage] La clé privée d'UH, associée à un Certificat émis par l'AC Horodatage est destinée à signer des Contremarques de temps. Ces usages sont explicitement définis dans les extensions des certificats.

4.5.2 Usage de la clé publique et du certificat

4.5.2.1 Clé publique et Certificat des AC

[Racine] Le Certificat de l'AC Racine est utilisé pour :

vérifier l'intégrité de la clé publique de l'AC Racine (Certificat auto-signé) ;

vérifier l'origine et l'intégrité des Certificats des AC Intermédiaires ;

vérifier l'origine et l'intégrité des LAR émises ;

[Horodatage] Le Certificat de l'AC Horodatage est utilisé pour :

vérifier l'origine et l'intégrité des Certificats d'UH;

vérifier l'origine et l'intégrité de la liste des UH révoquées (LCR);

4.5.2.2 Certificats des porteurs

[Racine] Les Certificats de l'AC Intermédiaire émis par l'AC Racine est destinée à :

valider les Certificats des porteurs finaux ;

valider la liste des Certificats révoquées (LCR), le cas échéant ;

valider les Certificats des répondeurs OCSP, le cas échéant.

[Horodatage] Le Certificat d'UH, émis par l'AC Horodatage est destinée à valider les contremarques de temps produites par cette UH.

4.6 Renouvellement d'un certificat

La notion de renouvellement de Certificat, au sens [RFC 3647], correspondant à la seule modification des dates de validité, n'est pas permise par la présente PC-DPC. Seule la délivrance d'un nouveau Certificat suite à changement de la bi-clé est autorisée.

4.6.1 Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au porteur de l'établissement du nouveau certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

4.7 Délivrance d'un nouveau Certificat suite au changement de la bi-clé

Conformément au [RFC 3647], ce chapitre traite de la délivrance d'un nouveau Certificat au porteur liée à la génération d'une nouvelle Bi-clé.

4.7.1 Causes possibles de changement d'une bi-clé

Les Bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques.

Par ailleurs, une Bi-clé et un Certificat peuvent être renouvelés par anticipation, suite à la révocation du Certificat du porteur (cf. chapitre 4.9, notamment le chapitre 4.9.1 pour les différentes causes possibles de révocation).

[Racine] Les Bi-clés et les Certificats correspondants des ACI, seront renouvelés au minimum tous les dix (10) ans.

[Horodatage] Les Bi-clés des UH seront renouvelés au minimum tous les ans.

4.7.2 Origine d'une demande d'un nouveau certificat

[Racine] La demande d'un nouveau Certificat est à l'initiative de l'AC Intermédiaire.

[Horodatage] La demande d'un nouveau Certificat est à l'initiative de l'AH.

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

La procédure est identique à la demande initiale. L'identification et la validation d'une demande de fourniture d'un nouveau Certificat sont précisées au chapitre 4.2 ci-dessus. Pour les actions de l'AC, se référer au chapitre 4.3.1.

4.7.4 Notification au porteur de l'établissement du nouveau certificat

La procédure est identique à la demande initiale (cf. chapitre 4.3.2).

4.7.5 Démarche d'acceptation du nouveau certificat

La procédure est identique à la demande initiale (cf. chapitre 4.4.1).

4.7.6 Publication du nouveau certificat

La procédure est identique à la demande initiale (cf. chapitre 4.4.2).

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

La procédure est identique à la demande initiale (cf. chapitre 4.4.3).

4.8 Modification du certificat

La présente PC-DPC n'autorise pas la modification d'un Certificat. Il faudra révoquer ledit Certificat puis faire une nouvelle demande auprès de l'AC.

4.8.1 Causes possibles de modification d'un certificat

Sans objet.

4.8.2 Origine d'une demande de modification d'un certificat

Sans objet.

4.8.3 Procédure de traitement d'une demande de modification d'un certificat

Sans objet.

4.8.4 Notification au porteur de l'établissement du Certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du Certificat modifié

Sans objet.

4.8.6 Publication du Certificat modifié

Sans objet.

4.8.7 Notification par l'AC aux autres entités de la délivrance du Certificat modifié

Sans objet.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

[Racine] Il peut exister plusieurs causes de révocation de Certificat d'une AC Intermédiaire :

- les informations d'une ACI figurant dans son Certificat ne sont plus correctes ;
- le Certificat n'est plus conforme à la PC-DPC auquel il est sujet ;
- l'ACI n'a pas respecté les modalités applicables d'utilisation du Certificat ;
- l'ACI n'a pas respecté ses obligations découlant de la présente PC-DPC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement de l'ACI ;
- la clé privée de l'ACI est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- l'ACI demande explicitement la révocation du Certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur et/ou de son support) ;
- la cryptographie employée n'assure plus la liaison entre le sujet et la clé publique ;
- cessation d'activité de l'ACI ;
- cessation d'activité de la présente AC.

[Horodatage] Il peut exister plusieurs causes de révocation de Certificat d'une UH :

- les informations d'une UH figurant dans son Certificat ne sont plus correctes ;
- le Certificat n'est plus conforme à la PC-DPC auquel il est sujet ;

- l'AH n'a pas respecté les modalités applicables d'utilisation du Certificat ;
- l'AH n'a pas respecté ses obligations découlant de la présente PC-DPC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement de l'AH ;
- la clé privée de l'UH est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- l'AH demande explicitement la révocation du Certificat (notamment dans le cas d'une destruction ou altération de la clé privée de l'UH et/ou de son support) ;
- la cryptographie employée n'assure plus la liaison entre le sujet et la clé publique ;
- cessation d'activité de l'AH ;
- cessation d'activité de la présente AC.

Pour l'ensemble des AC régies par la présente PC-DPC, lorsqu'une des circonstances ci-dessus se réalise et que l'AC intéressée en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau Certificat notamment), le Certificat concerné doit être révoqué.

4.9.2 Origine d'une demande de révocation

[Racine] Une demande de révocation de Certificat d'ACI ne peut émaner que :

- du responsable du TSP MediaCert ou de l'un de ses adjoints ;
- d'un responsable légal de l'entité opérant l'ACI, ou d'une personne mandaté par celui-ci ;
- par les autorités judiciaires via une décision de justice.

[Horodatage] Une demande de révocation de Certificat d'UH ne peut émaner que :

- du responsable du TSP MediaCert ou de l'un de ses adjoints ;
- d'un responsable légal de l'entité opérant l'AH, ou d'une personne mandaté par celui-ci ;
- par les autorités judiciaires via une décision de justice.

4.9.3 Procédure de traitement d'une demande de révocation

Une demande de révocation de Certificat réceptionnée par l'AC doit au moins contenir les informations suivantes :

- le numéro de série du Certificat à révoquer ;
- le nom associé au Certificat à révoquer (DN complet) ;
- le nom et la qualité du demandeur de la révocation ;
- la cause de révocation.

La demande est alors, dès réception, authentifiée et contrôlée par l'AC. L'AC transmet alors à la fonction de gestion des révocations la demande correspondante qui procède alors à la révocation, puis communique ce nouveau statut à la fonction d'information sur l'état des Certificats.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Dès que le porteur a connaissance qu'une des causes possibles de révocation citées au chapitre 4.9.1, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

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

Le délai maximum de traitement d'une demande de révocation d'un Certificat est de 24h.

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

L'utilisateur d'un Certificat est tenu de vérifier, avant son utilisation, l'état de la chaîne de Certificats correspondante jusqu'au Certificat de l'AC Racine. Il pourra utiliser, à cette fin, le dernier statut de révocation publié.

4.9.7 Fréquence d'établissement des LAR/LCR

[Racine] Les LAR sont générées tous les six (6) mois. Elles ont une durée de validité de un (1) an.

[Horodatage] Les LCR sont pré-générées tous les ans. Elles sont publiées toutes les vingt-quatre (24) heures. Elles ont une durée de validité de sept (7) jours.

4.9.8 Délai maximum de publication des LAR/LCR

Les LAR et LCR sont publiées le plus rapidement possible après la date d'établissement. Au maximum le délai de publication des LCR sera de soixante (60) minutes.

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

Sans objet.

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

Pour les Certificats émis, outre les exigences du chapitre 4.9.3, la révocation suite à une compromission de la clé privée fera l'objet d'une notification à l'organisme de contrôle dans les vingt-quatre (24) heures conformément aux exigences de [eIDAS].

4.9.13 Causes possibles d'une suspension

La suspension de Certificats n'est pas autorisée dans la présente PC-DPC.

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 Révocation et suspension des certificats

4.10.1 Caractéristiques opérationnelles

Le TSP MediaCert fournit aux utilisateurs de Certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un Certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'AC Racine), c'est-à-dire de vérifier également les signatures des Certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR et l'état du Certificat de l'AC Racine.

Les LCR / LAR sont publiés à l'adresse spécifié au sein de la [PG]. Cette adresse est notamment disponible au sein des Certificats émis.

[Horodatage] Une LCR contient la liste des Certificats d'Unité d'Horodatage révoqués, qu'ils soient expirés ou non. Elle contient notamment la date de son émission ainsi que la date d'émission de la prochaine LCR.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des Certificats est disponible 24h/24h, 7j/7j. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de huit (8) heures.

4.10.3 Dispositifs optionnels

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

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

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC émettrice et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

4.12 Séquestre de clé et recouvrement

Les clefs privées des porteurs ne sont pas séquestrées par l'AC.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

5 Mesures de sécurité non-techniques

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

En particulier, l'ensemble des locaux hébergeant des systèmes impliqués dans le cadre de la génération et de la révocation des Certificats sont opérés dans un environnement qui protège physiquement les services contre les menaces de compromission dues à un accès non-autorisé aux systèmes ou aux données. Le périmètre de la zone sécurisé est clairement identifié et ne peut être accédé par des personnels ou des organisations tierces non-autorisées.

5.1.2 Accès physique

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.1.3 Alimentation électrique et climatisation

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.1.4 Vulnérabilité aux dégâts des eaux

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.1.5 Prévention et protection incendie

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.1.6 Conservation des supports

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.1.7 Mise hors service des supports

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.1.8 Sauvegardes hors site

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.2.2 Nombre de personnes requises par tâche

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.2.3 Identification et authentification pour chaque rôle

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.2.4 Rôles exigeant une séparation des attributions

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.3.2 Procédures de vérification des antécédents

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.3.3 Exigences en matière de formation initiale

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.3.4 Exigences et fréquence en matière de formation continue

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.3.6 Sanctions en cas d'actions non autorisées

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

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

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.3.8 Documentation fournie au personnel

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.4 Procédure de constitution des données d'audit

5.4.1 Type d'événements à enregistrer

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

En plus des événements décrits dans la |PG], la présente politique impose aux AC de son périmètre de collecter les données d'audit suivantes :

- tous les événements relatifs à la sécurité, en particulier :
    - les changements de politique de sécurité des systèmes ;
    - les démarrages et arrêts des systèmes ;
    - les pannes matérielles et logicielles ;
    - les tentatives d'accès aux systèmes.
- tous les événements relatifs à l'enregistrement des porteurs, en particulier :
    - réception d'une demande de Certificat (initiale et renouvellement) ;
    - validation / rejet d'une demande de Certificat ;
    - événements liés aux clés de signature et aux Certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction, ...) ;
    - génération des Certificats des porteurs ;
    - publication et mise à jour des informations liées à l'AC (PC-DPC, Certificats d'AC, conditions générales d'utilisation, etc.) ;
    - réception d'une demande de révocation ;
    - validation / rejet d'une demande de révocation ;
    - génération puis publication des LAR et LCR.

Concernant la procédure d'enregistrement, l'AC conserve également :

- l'identité de la personne en rôle de confiance ayant réalisé la demande de Certificat ;
- l'original du formulaire de demande de Certificat ;
- l'identité de la personne en rôle de confiance ayant réalisé l'enregistrement.

L'AC étant opéré hors-ligne, les exigences sur l'activité des éléments réseau n'est applicable qu'à la fonction de publication.

Le dossier d'enregistrement comportant des données personnelles du porteur, la conservation fait l'objet de mesures de sécurité conforme au chapitre 9.4 du présent document.

5.4.2 Fréquence de traitement des journaux d'événements

Les journaux d'évènements des AC ne sont pas traités du fait qu'elles soient hors ligne.

5.4.3 Période de conservation des journaux d'événements

Les journaux d'événements ayant vocation à être conservés sont archivés. La durée d'archivage de ces informations est spécifiée au chapitre 5.5.2 du présent document.

5.4.4 Protection des journaux d'événements

Les journaux d'évènements sont protégés dans les mêmes conditions que celles définies au chapitre 5.5.3 du présent document.

5.4.5 Procédure de sauvegarde des journaux d'événements

La procédure de sauvegarde des journaux d'évènements des AC est interne et spécifié dans le document DTPC.

5.4.6 Système de collecte des journaux d'événements

Le système de collecte des journaux d'évènements des AC est interne et spécifié dans le document DTPC.

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

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.4.8 Évaluation des vulnérabilités

Les vulnérabilités sont évaluées au cours d'une analyse de risque (cf. chapitre sur l'analyse de risque dans la [PG]). Le contrôle des journaux des événements fonctionnels est réalisé à la demande en cas de litige, ou pour analyse de comportement de l'IGC.

5.5 Archivage des données

Des dispositions en matière d'archivage sont mises en place par l'AC. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

5.5.1 Types de données à archiver

Les données à archiver sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC-DPC ;
- les DTPC ;
- les dossiers d'enregistrement ;

- les Certificats émis ;
- les LAR et LCR émises ou publiées ;
- les différents engagements signés par le Comité MediaCert ;
- les journaux d'événements des différentes entités de l'IGC (cf. chapitre 5.4.1).

5.5.2 Période de conservation des archives

Les périodes de conservations minimales sont les suivantes :

Version	Auteur(s)
5 ans après la fin de vie de l'AC	les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ; les PC-DPC; les DTPC ; les Certificats émis ; les LAR et LCR émises ou publiées ; les différents engagements signés par le Comité MediaCert.
7 ans après l'expiration du Certificat associé	les dossiers d'enregistrement ; les éléments du cycle de vie du Certificat (génération, révocation, ...).
10 ans après leur génération	Autres données d'audits (par exemple, démarrages et arrêts des systèmes)

5.5.3 Protection des archives

Les moyens de protection des archives mis en œuvre par le TSP MediaCert dans le cadre de ses AC hors ligne diffèrent selon le type de donnée.

Les archives numériques sont protégés grâce à des systèmes physiques sécurisés de type coffre-fort ou armoire forte dont les accès sont contrôlés et protégés de la même manière que le sont les données d'activation des clés privées d'AC (cf. chapitre 6.4.2).

Les archives documentaires numériques sont protégées grâce à un coffre-fort numérique dont les accès sont contrôlés par le TSP MediaCert.

Les archives manuscrites sont protégés grâce à des systèmes physiques sécurisés de type coffre-fort ou armoire forte dont les accès sont contrôlés par le TSP MediaCert.

5.5.4 Procédure de sauvegarde des archives

Les procédures de sauvegardes des archives sont internes et sont spécifiées dans le document DTPC.

5.5.5 Exigences d'horodatage des données

L'horloge des systèmes des AC est synchronisée avec une source de temps définie au sein de la DTPC. Cette synchronisation est effectuée avant chaque utilisation de ces systèmes.

5.5.6 Système de collecte des archives

Le système de collecte des archives d'évènements des AC est interne et est spécifié dans le document DTPC.

5.5.7 Procédures de récupération et de vérification des archives

La procédure de récupération des archives des AC est interne et est spécifiée dans le document DTPC. L'accès aux archives est sujet à des restrictions (cf. chapitre 6.4.2).

Les archives seront rendues disponibles en cas de réquisition judiciaire.

5.6 Changement de clé d'AC

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 de l'AC doit être supérieure à celle des Certificats qu'elle signe.

Au regard de la date de fin de validité de ce Certificat, son renouvellement sera demandé dans un délai au moins égal à la durée de vie des Certificats signés par la clé privée correspondante

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée sera utilisée pour signer des Certificats

Le Certificat 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 la compromission et sinistre

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

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de l'IGC. Le responsable du TSP MediaCert doit en être informé immédiatement. Il devra alors s'assurer du traitement de l'anomalie. S'il estime que l'incident a un niveau de gravité important, il demandera une révocation immédiate du Certificat. Si celle-ci a lieu, il publiera l'information de révocation du Certificat dans la plus grande urgence, voire immédiatement. Il le fera via le site public du TSP MediaCert et/ou via une notification par courrier électronique à l'ensemble des clients. Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors le responsable du TSP MediaCert publiera l'information via le site public et notifiera par courrier électronique l'ensemble de ses clients impactés. Tous les Certificats concernés seront alors révoqués.

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

Le TSP MediaCert dispose d'un plan de continuité d'activité (cf. chapitre 5.7.4) permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC-DPC, des engagements de l'AC dans sa propre PC-DPC notamment en ce qui concerne les fonctions liées à la publication et / ou la révocation des certificats. Ce plan est testé au minimum une (1) fois tous les deux (2) ans.

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

La compromission d'une clé d'infrastructure ou de contrôle d'une composante est traitée dans le plan de continuité de la composante (cf. chapitre 4.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC Intermédiaire ou d'UH, le Certificat correspondant sera immédiatement révoqué : cf. chapitre 4.9.
Dans le cas d'une compromission de la clé d'AC Racine, le TSP MediaCert indiquera publiquement que les Certificats et informations de révocation délivrés en utilisant cette clé peuvent ne plus être valables. Le Certificat concerné sera immédiatement révoqué : cf. chapitre 4.9.

5.7.4 Capacités de continuité d'activité suite à un sinistre

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

5.8 Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de Certificats donnée seulement).

La cessation partielle d'activité sera progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier Certificat émis.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la révocation des Certificats et la publication des LAR / LCR conformément aux engagements pris dans sa PC-DPC. Un plan de cessation d'activité est alors appliqué par l'AC concernée. Ce plan est régulièrement tenu à jour et comporte notamment les actions citées ci-dessous.

L'AC prend les dispositions suivantes en cas de cessation de service :

- la notification des entités affectées ;
- le transfert de ses obligations à Worldline ;
- la gestion du statut de révocation pour les Certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC prendra les dispositions suivantes :

- informer (par exemple par récépissé) tous les porteurs des Certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant ;

- s'interdire de transmettre la clé privée lui ayant permis d'émettre des Certificats ;
- révoquer son Certificat ;
- révoquer tous les Certificats qu'elle a signés et qui seraient encore en cours de validité ;
- prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante (la clé nominale et ses éventuelles sauvegardes).

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clé des AC

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

Les exigences et pratiques complémentaires spécifiques de la présente section s'appliquent également.

Cérémonie des clés

[Racine] La cérémonie de génération des clés d'AC Racine est réalisée en présence d'un huissier de justice.

Module cryptographique

[Racine] Les clés de signature d'AC Racine sont générées et mises en œuvre dans un module cryptographique ayant fait l'objet d'une évaluation sécuritaire comme défini au chapitre 6.2.11 du présent document.

[Horodatage] Les clés de signature d'AC Horodatage sont générées et mises en œuvre dans un module cryptographique ayant fait l'objet d'une évaluation sécuritaire comme défini au chapitre 6.2.11 du présent document.

6.1.1.2 Clé des porteurs

[Horodatage] Les clés associés aux Certificats émis par l'AC sont obligatoirement générées et utilisées dans un module cryptographique ayant fait l'objet d'une évaluation sécuritaire de niveau au moins EAL4 du référentiel critères communs (ISO/IEC 15408) et ayant fait l'objet d'une qualification au niveau renforcé par l'ANSSI.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet.

6.1.3 Transmission de la clé publique à l'AC

La clé publique est transmise en interne par l'opérateur de confiance l'ayant généré au cours d'une cérémonie de clés.

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

[Racine] La clé publique d'AC Racine est enveloppée dans un Certificat racine auto-signé. Sa diffusion s'accompagne de l'empreinte numérique du Certificat ainsi que d'une déclaration précisant qu'il s'agit bien d'une clé publique de l'AC Racine. La clé publique de l'AC Racine, ainsi que les informations correspondantes (certificat, empreintes numériques, déclaration

d'appartenance) pourront aisément être récupérées par les utilisateurs de Certificats via le site web du TSP MediaCert (cf. chapitre 2.2).

[Horodatage] La clé publique de l'AC Horodatage est certifiée par l'AC Racine. Elle est publiée sur le site de web du TSP MediaCert (cf. chapitre 2.2).

6.1.5 Tailles des clés

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

Les exigences et pratiques complémentaires spécifiques définies ci-dessous s'appliquent également.

6.1.5.1 Taille des clés d'AC

Périmètre	Fonction de hachage	Algorithme	Taille
AC Racine	SHA256	RSA	4096 bits
AC Horodatage	SHA256	RSA	4096 bits

6.1.5.2 Taille des clés des porteurs

Périmètre	Fonction de hachage	Algorithme	Taille
AC Intermédiaire	SHA256	RSA	4096 bits
UH	SHA256	RSA	2048 bits

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

L'équipement de génération de Bi-clés utilisé pour la génération des paramètres des Bi-clés des AC est un module cryptographique configuré pour répondre à ces exigences. Les Bi-clés ne peuvent être générées que sur un module conforme à cette exigence, ou d'un niveau cryptographique et sécuritaire supérieur.

6.1.7 Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC Racine et d'ACI et du Certificat associé est strictement limitée à la signature de Certificats, de LCR / LAR (cf. chapitre 1.4).

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 Standards pour les modules cryptographiques

[Racine] Les clés de signature d'AC Racine sont générées et mises en œuvre dans un module cryptographique sécurisé répondant au niveau de qualification défini au chapitre 6.2.11 du présent document.

[Horodatage] Les clés de signature d'AC Horodatage sont générées et mises en œuvre dans un

module cryptographique ayant fait l'objet d'une évaluation sécuritaire dont le niveau est défini au chapitre 6.2.11 du présent document.

6.2.1.2 Mesures de sécurité pour les modules cryptographiques

Le TSP MediaCert s'assure de la sécurité physique et logicielle des modules cryptographiques utilisés. En particulier, il héberge ce matériel dans des zones d'accès contrôlées et hors ligne. Le TSP MediaCert s'assure de la sécurité des modules cryptographiques tout au long de leur cycle de vie, en particulier, lors de leur mise en place, lors des cérémonies des clés, lors de leur utilisation, et ce jusqu'à leur fin de vie.

6.2.2 Contrôle de la clé privée par plusieurs personnes

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

De plus, le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets.

6.2.3 Séquestre de la clé privée

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

6.2.4 Copie de secours de la clé privée

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

Par ailleurs, les clés privées des AC régis par la présente PC-DPC n'étant pas en permanence activées au sein du module cryptographique, ces clés privées font l'objet de copies de secours hors d'un module cryptographique. Cette copie de secours est réalisée sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement utilisé offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuie sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique. Les supports de stockages des copies de secours sont stockés dans un coffre-fort. Le contrôle des opérations de chiffrement / déchiffrement est conforme aux exigences du chapitre 6.2.2.

6.2.5 Archivage de la clé privée

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

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

Le transfert vers / depuis le module cryptographique ne se fait que pour la génération des copies de sauvegardes. Ceci se fait sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.7 Stockage de la clé privée dans un module cryptographique

Le stockage des clés privées des AC régies par la présente PC-DPC est réalisé de la même manière que le stockage des clés de secours (cf. chapitre 6.2.4).

6.2.8 Méthode d'activation de la clé privée

L'activation des clés privées d'AC se fait dans un module cryptographique et est contrôlée via des données d'activation (cf. chapitre 6.4). La clé privée étant désactivée après chaque opération cryptographique (cf. chapitre 6.2.9), un quorum de porteurs de secrets devront être présents afin de réaliser l'activation de la clé avant chaque opération.

6.2.9 Méthode d'activation de la clé privée

La clé privée de l'AC est désactivée après chaque opération cryptographique par réinitialisation du module cryptographique.

6.2.10 Méthode de destruction des clés privées

La destruction définitive d'une clé privée d'AC est réalisée par la destruction des moyens de restauration de la clé privée :

- la destruction de de la clé privée et de toutes les copies de secours, et
- la destruction des moyens d'activation de la clé privée.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs de création de signature

[Racine] Le module cryptographique utilisé par l'AC Racine régis par la présente PC-DPC a fait l'objet d'une évaluation sécuritaire de niveau FIPS 140-2 de niveau 3.

[Horodatage] Le module cryptographique utilisé par l'AC Horodatage régis par la présente PC-DPC a fait l'objet d'une évaluation sécuritaire de niveau FIPS 140-2 de niveau 3.

[Horodatage] Par ailleurs, le module cryptographique utilisé par le service d'horodatage doit faire l'objet d'une évaluation sécuritaire de niveau au moins EAL4 du référentiel critères communs (ISO/IEC 15408) et ayant fait l'objet d'une qualification par l'ANSSI.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques des AC ainsi que les clés publiques incluses dans les Certificats émis sont archivées pour la période indiquée en 5.5.2.

6.3.2 Durées de vie des bi-clés et des certificats

6.3.2.1 Durées de vie des bi-clés et des Certificats des AC

[Racine] La clé de l'AC Racine et le Certificat associé ont une durée de vie de vingt (20) ans.

[Horodatage] La clé de l'AC Horodatage et le Certificat associé ont une durée de vie de dix (10) ans.

6.3.2.2 Durées de vie des bi-clés et des Certificats des porteurs

La fin de validité d'un Certificat d'AC doit être postérieure à la fin de vie des Certificats qu'elle émet.

[Racine] Les clés des AC intermédiaires et les Certificats émis par l'AC Racine ont une durée de vie maximale de dix (10) ans.

[Horodatage] Les clés des UH ont une durée de vie de 1 an. Les Certificats associés ont une durée de vie de 3 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

6.4.2 Protection des données d'activation

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

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

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.
Par ailleurs, les AC dans le périmètre du présent document étant opérées hors-ligne, certaines mesures de sécurité de la [PG] ne sont applicables qu'à certaines fonctions particulières de l'AC. Par exemple, les mesures de sécurité réseaux sont applicables à la fonction de publication mais pas à la fonction de génération des Certificats.

6.5.2 Niveau de qualification des systèmes informatiques

Sans objet.

6.6 Mesures de sécurité liées au développement des systèmes

6.6.1 Mesures liées à la gestion de la sécurité

Tous les développements réalisés par le TSP MediaCert et impactant l'IGC sont documentés et réalisés via un processus de manière à en assurer la qualité. La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau est documentée et contrôlée. De plus, le TSP MediaCert opère un cloisonnement entre les environnements de développement, de test, de pré-production et de production. Ceci permet d'assurer une mise en production de qualité.

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

Toute évolution significative d'un système d'une composante de l'IGC est testée et validée avant déploiement. Ces opérations sont réalisées par du personnel de confiance.

6.7 Mesures de sécurité réseau

Les AC dans le périmètre de la présente PC-DPC sont des AC hors ligne. Elles n'ont pas d'accès en entrée ou en sortie au réseau public. Les exigences de la [PG] restent cependant applicables aux fonctions de publication.

6.8 Horodatage / Système de datation

Les AC dans le périmètre de la présente PC-DPC sont des AC hors ligne. Leur horloge est synchronisée manuellement avant toute utilisation. Les exigences de la [PG] restent cependant applicables aux fonctions de publication.

7 Profil des Certificats et LCR

7.1 Profils des certificats

7.1.1 Certificats de l'AC Racine

7.1.1.1 Champs de base du certificat

Le tableau suivant présente les champs de base :

Champ	Valeur
Version	2 (pour version 3)
SerialNumber	Généré automatiquement lors de la Cérémonie de Clé
Signature	Sha256WithRSAEncryption
Issuer	• CN = MediaCert Root CA 2018 • O = Worldline • OU = 0002 378901946 • C = FR
Subject	Identique à l'issuer (Certificat auto-signé)
Validity	• notBefore: date de création • notAfter: notBefore + 20 ans
Subject Public Key Info	RSA 4096 bits

7.1.1.2 Extensions du certificat

Le tableau suivant présente les extensions :

Champ	OID	Criticité	Valeur
Subject Key Identifier	2.5.29.14	Non	[RFC 5280] méthode [0] : identifiant de la clé publique contenue dans le Certificat
Key Usage	2.5.29.15	Oui	keyCertSign, CRLSign
Basic Constraint	2.5.29.19	Non	CA: true Maximum Path Length : absent

7.1.2 Certificat d'AC Intermédiaire

7.1.2.1 Champs de base du certificat

Le tableau suivant présente les champs de base :

Champ	Valeur
Version	2 (pour version 3)
SerialNumber	Généré automatiquement lors de la Cérémonie de Clé
Signature	Sha256WithRSAEncryption
Issuer	• CN = MediaCert Root CA 2018 • O = Worldline • OU = 0002 378901946 • C = FR
Subject	• CN = 'Nom de l'AC Intermédiaire'

Champ	Valeur
	• O = Worldline • OU = 0002 378901946 • C = FR • *(facultatif)* SNU = Numéro de série unique du DN [1]
Validity	• notBefore : date de création • notAfter : notBefore + 10 ans
Subject Public Key Info	RSA 4096 bits

L'AC s'assure que le CN de l'AC Intermédiaire est unique.

7.1.2.2 Extensions du certificat

Le tableau suivant présente les extensions :

Champ	OID	Criticité	Valeur
Authority Key Identifier	2.5.29.35	Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier	2.5.29.14	Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage	2.5.29.15	Oui	keyCertSign, CRLSign
Certificate Policies	2.5.29.32	Non	Policy Identifier : anyPolicy (2.5.29.32.0) Policy Qualifier Id : 1.3.6.1.5.5.7.2.1 Qualifier : https://www.mediacert.com
Basic Constraint	2.5.29.19	Non	CA: true Maximum Path Length : 0
CRL Distribution Points	2.5.29.31	Non	fullName: http://www.mediacert.com/rootCA2018/rootCA2018.crl reason : Absent cRLIssuer : Absent
Authority Information Access	1.3.6.1.5.5.7.1.1	Non	accessMethod : id-ad-caIssuers accessLocation: http://www.mediacert.com/rootCA2018/rootCA2018.crt

7.1.3 Certificats de l'AC Horodatage

7.1.3.1 Champs de base du certificat

Le tableau suivant présente les champs de base :

Champ	Valeur

[1] Ce SERIALNUMBER est utilisé pour différencier les différentes ACT. Il s'agit d'un compteur incrémenté à chaque émission d'une nouvelle ACT. Il est construit de la manière suivante :

SERIALNUMBER =

- *1 :* représente l'Autorité de Certification Technique 1 ;
- *2 :* représente l'Autorité de Certification Technique 2 ;
- …

Il n'est pas obligatoire. Le choix de son insertion est libre au décideur.

Version	2 (pour version 3)
SerialNumber	Généré automatiquement lors de la Cérémonie de Clé
Signature	Sha256WithRSAEncryption
Issuer	• CN = MediaCert Root CA 2018 • O = Worldline • OU = 0002 378901946 • C = FR
Subject	• CN = MediaCert Timestamp CA 2018 • O = Worldline • OU = 0002 378901946 • C = FR
Validity	• notBefore : date de création • notAfter : notBefore + 10 ans
Subject Public Key Info	RSA 4096 bits

7.1.3.2 Extensions du certificat

Le tableau suivant présente les extensions :

Champ	OID	Criticité	Valeur
Authority Key Identifier	2.5.29.35	Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier	2.5.29.14	Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage	2.5.29.15	Oui	keyCertSign, CRLSign
Certificate Policies	2.5.29.32	Non	• Policy Identifier : anyPolicy (2.5.29.32.0) • Policy Qualifier Id : 1.3.6.1.5.5.7.2.1 • Qualifier : https://www.mediacert.com
Basic Constraint	2.5.29.19	Non	• CA: true • Maximum Path Length : 0
CRL Distribution Points	2.5.29.31	Non	• fullName: http://www.mediacert.com/rootCA2018/rootCA2018.crl • reason : Absent • cRLIssuer : Absent
Authority Information Access	1.3.6.1.5.5.7.1.1	Non	• accessMethod : id-ad-caIssuers • accessLocation: http://www.mediacert.com/rootCA2018/rootCA2018.crt

7.1.4 Certificat d'UH

7.1.4.1 Champs de base du certificat

Le tableau suivant présente les champs de base :

Champ	Valeur
Version	2 (pour version 3)
SerialNumber	Généré automatiquement par l'AC émettrice
Signature	Sha256WithRSAEncryption

Champ	Valeur
Issuer	• CN = MediaCert Timestamp CA 2018 • O = Worldline • OU = 0002 378901946 • C = FR
Subject	• CN = MediaCert Timestamp Unit xxx • O = Worldline • OI = SI:FR-378901946 • C = FR
Validity	• notBefore : date de création • notAfter : notBefore + 3 ans
Subject Public Key Info	RSA 2048 bits

L'AC s'assure que le CN de l'UH est unique en incrémentant le compteur XXX à chaque demande. Le premier Certificat aura donc l'index 001, le second 002 etc.

7.1.4.2 Extensions du certificat

Le tableau suivant présente les extensions :

Champ	OID	Criticité	Valeur
Authority Key Identifier	2.5.29.35	Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier	2.5.29.14	Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage	2.5.29.15	Oui	digitalSignature (0)
Certificate Policies	2.5.29.32	Non	Policy Identifier : 1.2.250.1.111.20.3.1.2 Policy Qualifier Id : référence à la PC-DPC (id-qt-cps:1.3.6.1.5.5.7.2.1) Qualifier : https://www.mediacert.com
Basic Constraint	2.5.29.19	Non	CA : false Maximum Path Length : absent
Extended Key Usage	2.5.29.37	Oui	KeyPurposeId : id-kp-timeStamping (1.3.6.1.5.5.7.3.8)
CRL Distribution Points	2.5.29.31	Non	fullName: http://www.mediacert.com/timestampCA2018/timestampCA2018.crl reason : Absent cRLIssuer : Absent
Authority Information Access	1.3.6.1.5.5.7.1.1	Non	accessMethod : id-ad-caIssuers (1.3.6.1.5.5.7.48.2) accessLocation: http://www.mediacert.com/timestampCA2018/timestampCA2018.crt

7.2 Liste de Certificats Révoqués

7.2.1 LAR de l'AC Racine

7.2.1.1 Champ de base

Champ	Valeur
Version	1 (pour version 2)
Signature	SHA256WithRSA
Issuer	CN = MediaCert Root CA 2018 O = Worldline OU = 0002 378901946 C = FR
Validity	1 an
Revoked Certificates	• Serial Number • Revocation Date

7.2.1.2 Extensions

Champ	Criticité	Valeur
Authority Key Identifier	non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
CRL Number	non	Défini par l'outil

7.2.2 LCR de l'AC Horodatage

7.2.2.1 Champ de base

Champ	Valeur
Version	1 (pour version 2)
Signature	SHA256WithRSA
Issuer	CN = MediaCert Timestamp CA 2018 O = Worldline OU = 0002 378901946 C = FR
Validity	7 jours
Revoked Certificates	• Serial Number • Revocation Date

7.2.2.2 Extensions

Champ	Criticité	Valeur
Authority Key Identifier	non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
CRL Number	non	Défini par l'outil

8 Audit de conformité et autres évaluations

8.1 Fréquences et / ou circonstances des évaluations

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

Les AC dans le périmètre de la présente PC-DPC ne font pas l'objet d'audit de conformité externe, ni de qualification au sens du règlement [eIDAS].

8.2 Identités / qualifications des évaluateurs

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

8.3 Relations entre évaluateurs et entités évaluées

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

8.4 Sujets couverts par les évaluations

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

8.5 Actions prises suite aux conclusions des évaluations

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9 Autres problématiques métiers et légales

9.1 Tarif

Les AC dans le périmètre de la présente PC-DPC peuvent facturer leur service à l'exception du service de mise à disposition du statut des certificats, qui est mis à disposition à titre gratuit.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.2.2 Autres ressources

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.2.3 Couverture et garantie concernant les entités utilisatrices

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

En particulier, sur le périmètre de la présente PC-DPC, les informations suivantes sont considérées comme confidentielles :

- la DTPC ;
- les clés privées de l'AC ;
- les données d'activation associées aux clés privées d'AC ;
- tous les secrets de l'IGC ;
- les journaux d'événements des composantes de l'IGC ;
- les dossiers d'enregistrement des porteurs ;
- les causes de révocations ;

9.3.2 Informations hors du périmètre des informations confidentielles

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.4.2 Informations à caractère personnel

Sur le périmètre de la présente PC-DPC, le dossier d'enregistrement du porteur est considéré comme une information à caractère personnel. Un accès aux données personnelles est mis en place conformément à la [PG].

9.4.3 Responsabilité en termes de protection des données personnelles

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.4.4 Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne sont pas divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.4.6 Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5 Droits sur la propriété intellectuelle et industrielle

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC-DPC de l'AC et les documents qui en découlent ;
- respecter et appliquer la partie de la DTPC leur incombant (cette partie doit être communiquée à la composante correspondante) ;
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre 8) ;

- respecter les accords ou contrats qui les lient entre elles ou aux porteurs ;
- documenter leurs procédures internes de fonctionnement, mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1 Autorités de Certification

Le TSP MediaCert, en tant qu'Autorité de Certification, est responsable de :

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

Le TSP MediaCert, en tant qu'Autorité de Certification, est responsable, sauf à démontrer qu'il n'a commis aucune faute intentionnelle ou négligence, des préjudices causés aux utilisateurs, si :

- les informations contenues dans le Certificat ne correspondent pas aux informations d'enregistrement ;
- celui-ci n'a pas fait procéder à l'enregistrement de la révocation d'un certificat et n'a pas publié cette information conformément à ses engagements.

9.6.2 Autorités d'Enregistrement

Le TSP MediaCert opérant, sur le présent périmètre, sa propre Autorité d'Enregistrement, se reporter au chapitre 9.6.1.

9.6.3 Porteurs de Certificats

Le porteur a le devoir de :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du Certificat ;
- protéger ses données d'activation de clé privée ;
- respecter les conditions d'utilisation du service ;
- informer l'AC de toute modification concernant les informations contenues dans son Certificat ;
- demander le renouvellement de son Certificat avec un délai raisonnable avant son expiration ;
- faire, sans délai, une demande de révocation de son Certificat en cas de compromission ou de suspicion de compromission de ses données d'activation ou de sa clé privée.

9.6.4 Utilisateurs de certificats

Les utilisateurs des Certificats doivent :

- vérifier et respecter l'usage pour lequel un Certificat a été émis ;
- pour chaque Certificat de la chaîne de certification, du Certificat du porteur jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du Certificat considéré et contrôler la validité de ce Certificat (dates de validité, statut de révocation).

9.6.5 Autres participants

Sans objet.

9.7 Limite de garantie

Sans objet.

9.8 Limite de responsabilité

Le TSP MediaCert ne pourra pas être tenu pour responsable d'une utilisation non-autorisée ou non-conforme des données d'authentification, des Certificats, des LAR/LCR, ainsi que de tout autre équipement ou logiciel mis à disposition.
Le TSP MediaCert décline sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les Certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le Porteur. De plus, dans la mesure des limitations de la loi française, le TSP MediaCert ne saurait être tenu responsable :

- d'aucune perte financière ;
- d'aucune perte de données ;
- d'aucun dommage indirect lié à l'utilisation d'un Certificat ;
- d'aucun autre dommage.

En toute hypothèse, la responsabilité du TSP MediaCert sera limitée, tous faits générateurs confondus et pour tous préjudices confondus, au montant payé au TSP MediaCert pour l'accès au service et ce, dans le respect et les limites de la loi applicable.

9.9 Indemnités

Sans objet.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

La PC-DPC doit rester en application au moins jusqu'à la fin de vie du dernier Certificat émis au titre de cette PC-DPC.

9.10.2 Fin anticipée de validité

Cette PC-DPC reste en application jusqu'à la publication d'une nouvelle version.

9.10.3 Effets de la fin de validité et clauses restant applicables

Sans objet.

9.11 Amendements à la PC

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.12 Dispositions concernant la résolution de conflits

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.13 Juridictions compétentes

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.14 Conformité aux législations et réglementations

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.15 Disposition diverses

9.15.1 Accord global

Sans objet.

9.15.2 Transfert d'activités

Sans objet.

9.15.3 Conséquences d'une clause non valide

Sans objet.

9.15.4 Application et renonciation

Sans objet.

9.15.5 Force majeure

L'ensemble des exigences et pratiques décrites dans la [PG] s'applique.

9.15.6 Autres dispositions

Sans objet.