PUBLIC

POLITIQUE DE CERTIFICATION - DECLARATION DES PRATIQUES DE CERTIFICATION DES AC EN LIGNE

AUTEUR(S)	:	F. Da Silva
N° DE DOCUMENT	:	WLM-OTU-F002
VERSION	:	4.0
STATUT	:	Final
SOURCE	:	Worldline
DATE DU DOCUMENT	:	23 avril 2019
NOMBRE DE PAGES	:	96

TSP MediaCert

Digitally signed by TSP MediaCert
DN: CN=TSP MediaCert, O=Worldline, E=dl-mediacert-tsp@worldline.com, C=FR
Reason: I am approving this document
Location:
Date: 2019-04-26 11:16:46

Rôle	Nom	Signature	Date
Relecteur 1 – Resp. adjoint TSP	Fanny Lesecq	Fanny Lesecq	23/04/2019
Relecteur 2 – RSSI	Didier Sobkowiak	Didier Sobkowiak	23/04/2019
Fonction d'assurance qualité	Fanny Lesecq	Fanny Lesecq	23/04/2019
Propriétaire du document	Comité MediaCert	Guillaume Bailleul	23/04/2019
Approbateur – Resp. TSP	Guillaume Bailleul	Guillaume Bailleul	23/04/2019

Table des Matières

Table des Matières 2

Liste des modifications 4

1 Introduction 7

1.1 Présentation générale 7
1.2 Identification 8
1.3 Entités intervenant dans l'Infrastructure à Gestion de Clés 10
1.4 Catégories de Certificats 15
1.5 Usage des Certificats 17
1.6 Gestion de la PC 17
1.7 Définitions et acronymes 18

2 Responsabilités concernant la mise à disposition des informations devant être publiées 24

2.1 Entités chargées de la mise à disposition des informations 24
2.2 Informations devant être publiées 24
2.3 Délais et fréquences de publication 24
2.4 Contrôle d'accès aux informations publiées 24

3 Identification et authentification 25

3.1 Nommage 25
3.2 Validation initiale d'identité 26
3.3 Identification et validation d'une demande de renouvellement de clés 33
3.4 Identification et validation d'une demande de révocation 34

4 Exigences opérationnelles sur le cycle de vie des Certificats 35

4.1 Demande de création d'un Certificat 35
4.2 Traitement d'une demande de création d'un Certificat 36
4.3 Délivrance du Certificat 38
4.4 Acceptation du Certificat 38
4.5 Usages de la Bi-clé et du Certificat 39
4.6 Renouvellement d'un Certificat 40
4.7 Délivrance d'un nouveau Certificat suite au changement de la Bi-clé 40
4.8 Modification d'un Certificat 41
4.9 Révocation et suspension d'un Certificat 42
4.10 Fonctions d'information sur l'état des Certificats 47
4.11 Fin de la relation entre l'Abonné et l'AC 48
4.12 Séquestre de clé et recouvrement 48

5 Mesures de sécurité non techniques 49

5.1 Mesures de sécurité physique 49
5.2 Mesures de sécurité procédurales 49
5.3 Mesures de sécurité vis-à-vis du personnel 50
5.4 Procédures de constitution des données d'audit 51
5.5 Archivage des données 52
5.6 Changement de Bi-clé d'AC 54
5.7 Reprise suite à compromission et sinistre 54

5.8 Fin de vie de l'IGC 55

6 Mesures de sécurité techniques 57

6.1 Génération et installation des Bi-clés 57
6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques 59
6.3 Autres aspects de la gestion des Bi-clés 62
6.4 Données d'activation 63
6.5 Mesures de sécurité des systèmes informatiques 63
6.6 Mesures de sécurité des systèmes durant leur cycle de vie 63
6.7 Mesures de sécurité réseau 64
6.8 Horodatage / Système de datation 64

7 Profil des Certificats et LCR 65

7.1 Profils des certificats 65
7.2 Profil des LCR 80
7.3 Profil des OCSP 81

8 Audit de conformité et autres évaluations 84

8.1 Fréquences et/ou circonstances des évaluations 84
8.2 Identités / qualifications des évaluateurs 84
8.3 Relations entre évaluateurs et entités évaluées 84
8.4 Sujets couverts par les évaluations 84
8.5 Actions prises suite aux conclusions des évaluations 84
8.6 Communication des résultats 84

9 Autres problématiques métiers et légales 85

9.1 Tarifs 85
9.2 Assurance 85
9.3 Confidentialité des données professionnelles 85
9.4 Protection des données personnelles 89
9.5 Droits sur la propriété intellectuelle et industrielle 89
9.6 Interprétations contractuelles et garanties 89
9.7 Limite de garantie 93
9.8 Limite de responsabilité 93
9.9 Indemnités 94
9.10 Durée et fin anticipé de validité de la PC 94
9.11 Notifications individuelles et communications entre les participants 94
9.12 Amendements à la PC 94
9.13 Dispositions concernant la résolution de conflits 95
9.14 Juridictions compétentes 95
9.15 Conformité aux législations et réglementations 95
9.16 Dispositions diverses 95
9.17 Autres dispositions 96

Liste des modifications

Version	Date	Description	Auteur(s)
1.0	24/12/2012	Version publique initiale	C. Brunet
1.1	08/04/2013	Evolution suite remarque lors de l'audit initial ETSI 102 042 : • 4.9.2.1 : reformulation des origines de la révocation • 5.8.2 : précision sur CRL étendue en cas de cessation d'activité	C. Brunet
1.2	22/11/2013	Evolution suite ajustement contrat : • 3.2.3.1 : explications complémentaires sur la conservation des données hors utilisation dans le Certificat • 5.5.2 : modification sur les durées de conservation des dossiers d'enregistrement. • 9.6.4 : le terme « immédiatement » est remplacé par « dans les meilleurs délais » • 9.9, 9.13, 9.14, 9.16.5 : modification de la référence aux contrats Client/AWL	C. Brunet
1.3	01/02/2015	Evolutions suite changement de nom de la société et modification gabarit de Certificat : • Tout le document : Atos Worldline est remplacé par Worldline (à noter qu'il s'agit de la même société avec le même Siret) • 7.1.2.3 : modification dans des valeurs indiquées dans les champs DN et Subject alt name et key usage	C. Brunet
2.0	07/11/2016	Evolutions suite aux retours d'audit • Modification du §3.2.3.1 pour Validation de l'identité d'un titulaire de Certificat à usage unique par identification externe et pour le cas du titulaire appartenant à l'Organisation de l'Abonné, reformulation de l'exigence de contrôle de l'identité du titulaire. • Ajout des procédures et raisons de destruction des Bi-clés AC au §6.3.4 • Changer « opérateur » pour « pilote » • Homogénéisation des limites de garantie par rapport aux CGU (§9.7) • Modification du §4.9.3.2 pour décrire la procédure de révocation d'un Certificat Organisation • Ajout des méthodes garantissant le suivi du délai de révocation (§4.9.3.2 et §5.7.3) • Ajout des §5.2.5 et §5.2.6 et modification du §5.3.6 pour conformité de l'AC aux exigences du 7.4.3 • Ajout du §5.4.6 sur les procédures de restitution et de contrôle de restitution des journaux d'évènements • Modification de §5.2.4 sur les rôles exigeant une séparation des attributions • Ajout des OID des Certificats de test (§1.2.2) et ajout des descriptions (§7.1.2.4 et §7.1.2.5) • Ajout de l'oid de la PC OTU dans les gabarits de tous les Certificats • Ajout du §4.9.10 sur l'archivage des LCR • Ajout de la description du monitoring de la	V. Dumond C. Lootvoet A. Brugnot J.J. Milhem

Version	Date	Description	Auteur(s)
		page Mediacert (§2.4.2) • Ajout d'une référence à la signature des documents de l'AC pour leur assurer un contrôle d'authenticité (§2.4.3) • Révision du §5.3.2 sur la vérification des antécédents judiciaires • Modification des gabarits et des OID pour suivre le changement de version de la PC (§1.2.2, §7.1.2.2, §7.1.2.3, §7.1.2.4, §7.1.2.5) • Ajout d'une mention de la non vérification du mail lors de la demande de Certificat au §3.2.4 • Correction du § 7.1.5 Contraintes sur les noms qui affectent l'attribut CN et également GN et SN le cas échéant pour les Certificats Organisation • Modification du §9.12.2 sur les circonstances selon lesquelles l'OID doit être changé • Ajout de définitions manquantes • Reformulations et précisions concernant le contrat, le dossier d'abonnement, les obligations de l'abonné, l'identification du Titulaire, la validation d'une Organisation • Ajout d'une étape d'acceptation du Certificat par le Titulaire d'un Certificat OTU • Ajout engagement pratiques non-discriminatoire au §9.6	
2.1	02/02/2017	• Modification des informations du titulaire à relever, vérifier et conserver par l'AC (§3.2.3.1) • Révision des profils de LCR (§7.2) • Révision des gabarits de Certificats (§7.1) • Modification de la durée du préavis d'information en cas de modification de la PC (§9.11)	C. Lootvoet
3.0	09/06/2017	Réécriture pour prise en compte des contraintes réglementaires eIDAS	F. Lesecq V. Dumond
3.1	21/07/2017	Prise en compte des remarques de l'audit eIDAS	F. Lesecq F. Da Silva
3.2	18/09/2018	Intégration du document à la structure documentaire du TSP MediaCert, c'est-à-dire mise en cohérence avec la PG Ajout de causes de révocations en cohérence avec la mise à jour de l'ETSI EN 319 411-1 (v1.2.2) Suppression de l'obligation de publication en ligne • des anciennes versions de PC-DPC • des versions anglaises des politiques Ajout d'une spécification liée au RGPD et à la conservation des informations d'identification d'un individu titulaire d'un Certificat OTU Exceptionnellement, cette version ne fera pas l'objet d'une publication car elle n'introduit pas de nouveaux éléments et une nouvelle version (avec intégration d'une nouvelle AC au présent document) sera publiée dans les mêmes délais (plus d'information dans le PV de validation de la réunion sécurité)	F. Da Silva
3.3	18/09/2018	Ajout d'une AC au périmètre du présent document. L'impact étant seulement l'ajout de deux gammes et la spécification du niveau d'identification leur étant	F. Da Silva V. Dumond

Version	Date	Description	Auteur(s)
		associé. Cette PC-DPC devient alors la PC-DPC des « AC en ligne ». Prise en compte des remarques/écarts détectés lors de l'audit de surveillance 2018 de l'AC OTU. Revue pour cohérence avec le RGPD.	
3.4	12/10/2018	Prise en compte des remarques/écarts détectés lors de l'audit de certification 2018 de l'AC OTU LCP : • changement de la description du contenu d'une LCR • clarification de l'énumération des moyens de validation des consentements • revue des conditions de révocation de Certificats à usage unique	F. Da Silva
3.5	23/04/2019	Revue des conditions de révocation de Certificats à usage unique (prolongement de la modification faite en v3.4) Modification de la description du contenu d'une LCR (annule la modification faite en v3.4) Suppression de la référence à l'article 40 (droits de la personne) Evolution des versions des normes dans le référentiel	F. Da Silva
4.0	23/04/2019	Nouvelle structure : dans le cadre du DRP, l'AC OTU est divisée en deux AC (AC OTU & AC ORG)	F. Da Silva J. Steux

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°910/2014 du Parlement européen et du Conseil européen en matière d'indentification électronique et des services de confiance pour les transactions électroniques au sein du marché intérieur.

Ce document décrit la Politique de Certification de plusieurs Autorités de Certification dites « en ligne », non qualifiées, opérées par le TSP MediaCert pour régir l'ensemble du cycle de vie (création, émission, utilisation, …) des Certificats de signature à usage unique (aussi appelés « *One Time Usage* ») mis en œuvre dans le cadre de souscription en ligne, mais également celui des Certificats cachets électroniques utilisés pour sceller des données électroniques afin de garantir leur origine et leur intégrité :

- l'Autorité de Certification dénommé « AC OTU LCP » ;
- l'Autorité de Certification dénommé « AC OTU » ;
- l'Autorité de Certification dénommé « AC ORG ».

Ces AC sont opérées exactement de la même manière (sur le plan organisationnel, technique, infrastructure, …), possèdent le même parc matériel et logiciel. Toutefois, elles divergent sur différents sujets :

Sujet de différenciation	AC OTU	AC ORG	AC OTU LCP
Usage de la bi-clé / du Certificat	Certificat de signature électronique (cf. chapitre 1.5.1.1)	Certificat de scellement électronique (cf. chapitre 1.5.1.1)	Certificat de signature électronique (cf. chapitre 1.5.1.1)
Identification du futur titulaire de Certificat à usage unique	requiert un niveau d'identification pour la fourniture de Certificats à usage unique plus strict que celui défini par le niveau LCP mais moins strict que celui défini par le niveau NCP d'où sa gamme dénommée « renforcé » (cf. chapitre 1.2.1);	X	requiert un niveau d'identification pour la fourniture de Certificats à usage unique conforme au niveau LCP d'où sa gamme dénommée « standard » (cf. chapitre 1.2.1).

Ce document présente dans ce cadre :

- les exigences auxquelles sont soumises chacune de ces AC en ligne opérées par le TSP MediaCert ;
- les usages pour lesquels les Certificats sont émis ;
- la gestion de ces Certificats dans leur cycle de vie ;
- les mesures de sécurité autour de l'Infrastructure de Gestion de Clés ;
- les obligations et exigences portant sur les différents acteurs.

En plus de décrire la Politique de Certification, ce document décrit la Déclaration des Pratiques de Certification. Il s'agit là de l'énoncé des pratiques auxquelles les Autorités de Certification en ligne ont recours dans la gestion des Certificats qu'elles émettent.

Par ailleurs, étant un Service de Confiance de délivré par le TSP MediaCert, l'ensemble des exigences et des pratiques de la [PG] sont, sauf mention contraire, applicables au périmètre de ces AC en ligne.

1.2 Identification

1.2.1 Identification du document

Eléments	Valeur
Titre	Politique de Certification - Déclaration des Pratiques de Certification des AC en ligne
Référence document	WLM-OTU-F002
OID	1.2.250.1.111.20.5.4
Version	4.0
Auteur	F. Da Silva

L'OID du présent document est basé sur l'OID « **1.2.250.1.111.20.5** » : 1.2.250.1.111.20.5.**z**.**w** où :

- z : version majeure de la présente politique (ex : version 3.1 → 3) ;
- w : type du Certificat utilisé par les AC en ligne.

Comme le sous-entend la description ci-dessus, les AC en ligne ont défini un OID pour chacun des types de Certificats qu'elles délivrent comme suit :

Scope	Gamme de certificat	Conformité et niveau de sécurité ciblé	OID
AC OTU	Certificats à usage unique *« renforcé »*	[ETSI EN 319 411-1] niveau LCP *(non qualifié)*	1.2.250.1.111.20.5.4.1
	Certificats à usage unique de test *« renforcé »*	[ETSI EN 319 411-1] niveau LCP *(non qualifié)*	1.2.250.1.111.20.5.4.3
AC ORG	Certificats d'Organisation	[ETSI EN 319 411-1] niveau LCP *(non qualifié)*	1.2.250.1.111.20.5.4.2
	Certificats d'Organisation de test	[ETSI EN 319 411-1] niveau LCP *(non qualifié)*	1.2.250.1.111.20.5.4.4
AC OTU LCP	Certificats à usage unique *« standard »*	[ETSI EN 319 411-1] niveau LCP *(non qualifié)*	1.2.250.1.111.20.5.4.5
	Certificats à usage unique de test *« standard »*	[ETSI EN 319 411-1] niveau LCP *(non qualifié)*	1.2.250.1.111.20.5.4.6

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

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

1.2.2 Identification des Autorités de Certification

Sauf mention contraire, les exigences du présent document sont applicables aux AC définies au chapitre 1.1 du présent document. Les exigences applicables à une seule AC sont précédées de la mention :

- [AC OTU LCP] pour l'AC OTU LCP ;
- [AC OTU] pour l'AC OTU ;
- [AC ORG] pour l'AC ORG.

Celles-ci sont rattachées à des Autorités de Certification Racine Worldline dont les informations nécessaires sont les suivantes :

Scope	Eléments	Valeur
AC OTU et AC ORG	*OID* de la PC-DPC	1.2.250.1.111.20.3.1
	OID de l'AC émettrice	1.2.250.1.111.20.3.1.3
	Distinguish Name (DN) de l'AC Racine	C = FR O = Worldline OU = 0002 378901946 CN = MediaCert Trust CA 2019
AC OTU LCP	*OID* de la PC-DPC	1.2.250.1.111.20.3.1
	OID de l'AC émettrice	1.2.250.1.111.20.3.1.1
	Distinguish Name (DN) de l'AC Racine	C = FR O = Worldline OU = 0002 378901946 CN = MediaCert Root CA 2018

La structure des Chaînes de Certification des AC en ligne est la suivante :

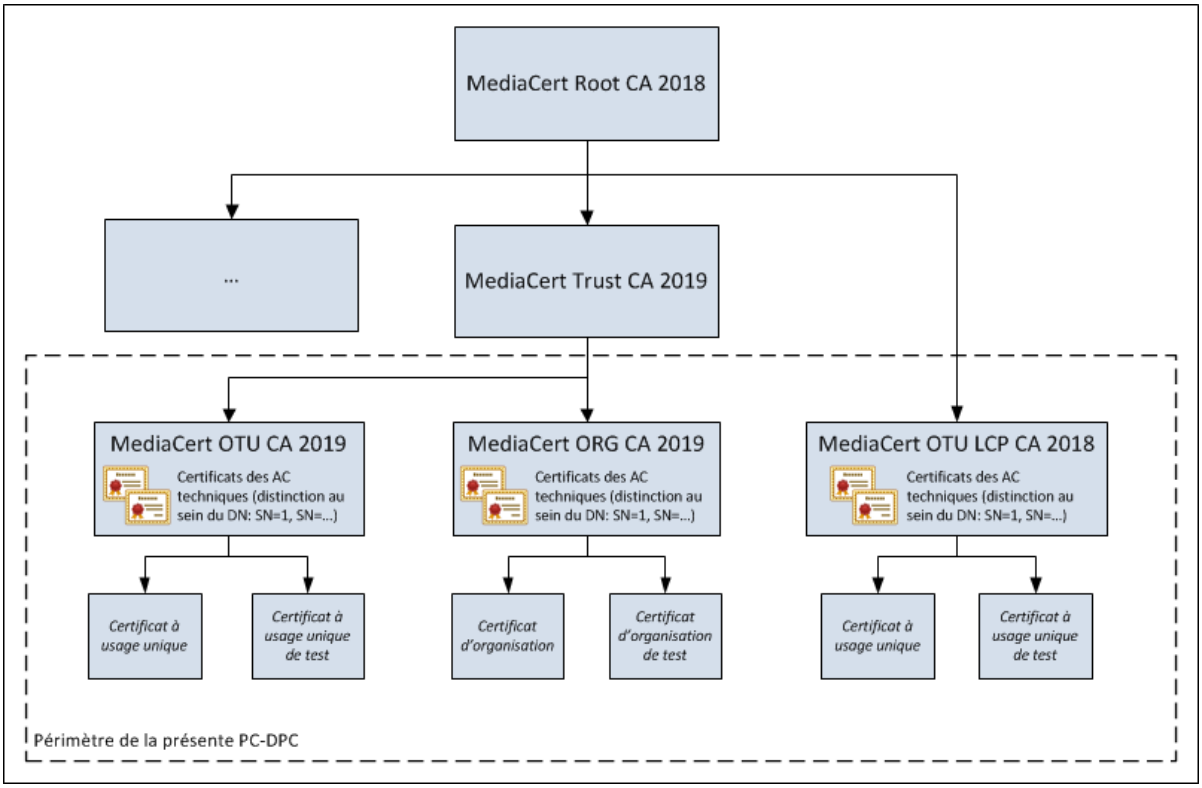

Figure 1 – Chaînes de Certification des AC en ligne

1.3 Entités intervenant dans l'Infrastructure à Gestion de Clés

L'Infrastructure à Gestion de Clés est constitué d'un ensemble de moyens techniques, humains, documentaires et contractuels dédiés en vue de gérer le cycle de vie des Certificats électroniques délivrés par l'Autorité de Certification. Elle assure, par le biais de systèmes de cryptographie asymétrique, un environnement sécurisé pour les échanges électroniques.

Les AC s'appuient sur cette infrastructure technique. Les prestations de l'IGC sont le résultat de différents services qui correspondent aux différentes étapes du cycle de vie des Bi-clés et des Certificats. Pour cela, les IGC concernées sont constituée d'un certain nombre d'entités comme présenté par le schéma fonctionnel en Figure 2.

La décomposition fonctionnelle des IGC concernées par la présente PC-DPC est la suivante :

- Service d'enregistrement ;
- Service de génération de Certificats ;
- Service de remise de Certificats ;
- Service de révocation de Certificats ;
- Service d'information sur l'état des Certificats.

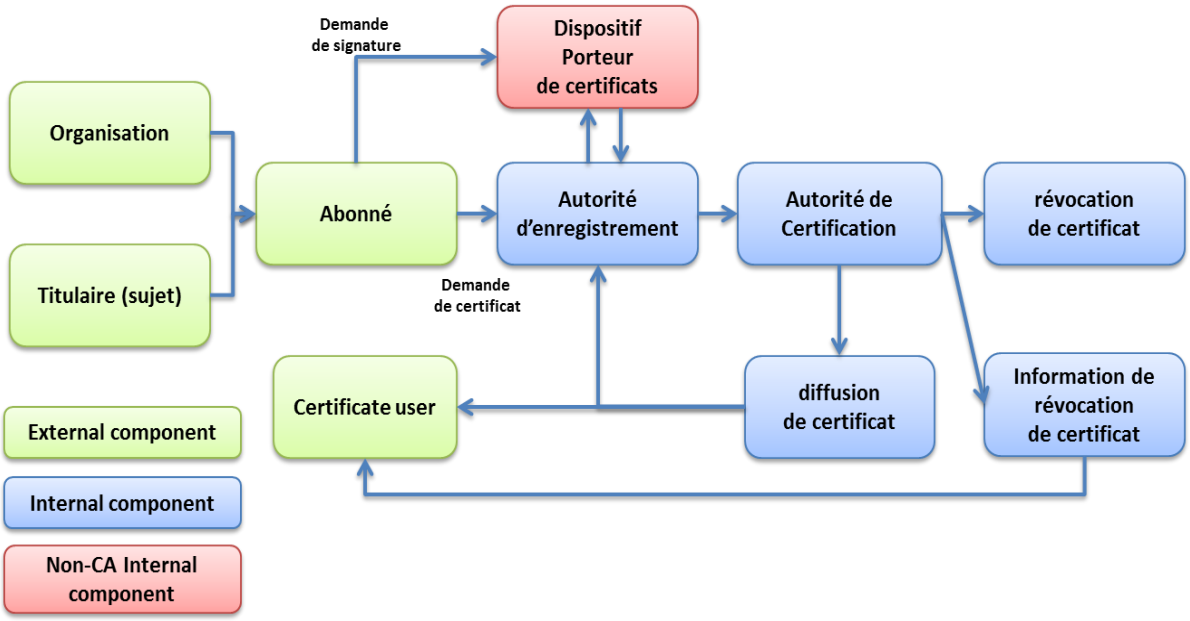

Figure 2 – Schéma fonctionnel des IGC opérant les AC en ligne

1.3.1 Autorité de Certification

Une Autorité de Certification désigne une entité capable de produire les Certificats à la demande du Service d'enregistrement. Cette entité a en charge le cycle de vie complet des Certificats (création, publication, …).

Les Autorités de Certification en ligne sont représentées par un Responsable d'Autorité désigné au sein de Worldline. Ce Responsable d'Autorité a pour subordonnés des Responsables d'Autorité Adjoints, désignés par le Responsable lui-même.

1.3.1.1 Service de génération

Ce service génère les Certificats à partir :

- des informations transmises par l'Autorité d'Enregistrement ; et
- de la clé publique du Certificat provenant de la fonction de génération des éléments secrets.

Ces Certificats sont signés électroniquement avec la clé privée de l'AC cible et ne peuvent être utilisés que pour les usages décrits au chapitre 1.5.1.1 du présent document.

1.3.1.2 Service de diffusion

Une fois les Certificats générés, ils sont transmis à l'Autorité d'Enregistrement qui transmet par la suite le Certificat au Dispositif Porteur de Certificats.

1.3.1.3 Service de révocation

Ce service révoque les Certificats à partir d'une demande de révocation préalablement fournie. Les résultats sont diffusés via les services d'information sur l'état des Certificats.

1.3.1.4 Service d'information sur l'état des Certificats

Ce service fournit aux utilisateurs de Certificats des informations sur l'état des Certificats (révoqués, suspendus, …). Cette fonction est mise en œuvre via des modes de publication régulièrement mis à jour : Listes de Certificats Révoqués (LCR), Liste d'Autorités Révoquées (LAR), répondeur OCSP.

1.3.2 Autorité d'Enregistrement

L'Autorité d'Enregistrement est l'entité interlocutrice des unités clientes (Abonnés) qui lui transmettent des demandes de création ou de révocation de Certificats. Elle prend donc en charge les opérations suivantes :

- authentification de l'Abonné qui procède à la demande de création de Certificat ;
- vérification du contenu des demandes de création de Certificat ;
- [AC OTU][AC OTU LCP] vérification de la bonne application de la politique d'identification par les Abonnés dans le cadre d'émission de Certificats à usage unique ;
- [AC ORG] vérification de l'identité du futur Titulaire de Certificat d'Organisation ;
- enregistrement des demandes de création et de révocation de Certificat ;
- acceptation ou refus des demandes de création et de révocation de Certificat ;
- fourniture des Certificats au Dispositif Porteur de Certificats ;
- archivage des demandes de création et de révocation de Certificat.

Pour rendre ces services, les AC opèrent leur propre Autorité d'Enregistrement (par ailleurs, il s'agit de la même) qui s'appuie sur un service disposant des moyens techniques et humains qui lui permettent d'assurer la gestion du cycle de vie des Certificats qu'elles émettent et qui constituent à ce titre un point d'accès unique à ces Autorités de Certification (serveurs permettant la transmission des demandes et la livraison des Certificats).

1.3.3 Dispositif Porteur de Certificats

Dans le cadre de cette présente PC-DPC, le Dispositif Porteur de Certificats n'est pas assimilé au Titulaire du Certificat.

En effet, le Dispositif Porteur de Certificats désigne ici une entité logicielle et matérielle hébergée par Worldline qui stocke le Certificat et la clé privée du Titulaire ou d'une Organisation.

Pour chaque Certificat généré par les AC, le Dispositif Porteur de Certificats est responsable des fonctions suivantes :

- génération de la Bi-clé ;
- stockage sécurisé de la Bi-clé ;

- génération de la demande de Certification (CSR), contenant les informations de l'utilisateur préalablement transmises par l'Abonné ;
- utilisation de la clé privée et du Certificat dans les cas d'usage décrits au chapitre 1.5 ;
- destruction de la clé privée comme décrit au chapitre 6.2.10.2 de ce document ;

Le Dispositif Porteur de Certificats assure une conservation sécurisée et un contrôle exclusif pour le compte du Titulaire ou de l'Organisation des éléments secrets.

Le contrôle exclusif sur les Certificats est assuré :

- par les caractéristiques de sécurité du boitier cryptographique (protection des secrets stockés) ;
- par une isolation réseau interdisant à tout serveur non autorisé de se connecter à ces boitiers.

Le dispositif porteur de Certificat peut disposer de deux (2) types de Certificats :

- Certificat à usage unique : cf. chapitre 1.4.1 ;
- Certificat d'Organisation : cf. chapitre 1.4.2.

1.3.4 Bénéficiaire de Certificats

La fourniture de Certificats par les AC en ligne nécessite la souscription préalable d'un abonnement aux services de ces Autorités de Certification. Cela passe par la signature d'un Contrat d'Abonnement avec le TSP MediaCert. Ce contrat précise le type de Certificat que l'Abonné souhaite mettre en œuvre :

- [AC OTU][AC OTU LCP] Certificat de signature *One Time Usage* émis au nom d'une personne physique (Titulaire) en vue de pouvoir signer des Documents (cf. chapitre 1.5.1.1) ; et/ou
- [AC ORG] Certificat d'Organisation émis au nom d'une Organisation en vue de pouvoir sceller des Documents au nom de son Organisation ou d'Organisation mandante (cf. chapitre 1.5.1.1).

1.3.4.1 [AC OTU][AC OTU LCP] Service de signature électronique

S'il s'agit de signer des données électroniques, les deux (2) AC en ligne produisent alors des Certificats à usage unique (cf. chapitre 1.4.1).
Dans le cadre des Certificats à usage unique, la demande de création de Certificat à l'Autorité d'Enregistrement est faite par l'Abonné au moyen d'un processus technique décrit au chapitre 3.2.5.1. L'Abonné, dans ce cas :

- doit être identifié auprès de l'Autorité d'Enregistrement (cf. chapitre 3.2.2.1) ;
- doit préalablement à la demande de création de Certificat pour le Titulaire, l'avoir identifié de telle manière que le Certificat émis puisse reposer sur une identité fiable et vérifiée (cf. chapitre 3.2.3.1) ;

- doit avoir obtenu du Titulaire les consentements requis nécessaires pour pouvoir effectuer une requête auprès de l'AE en vue de demander la génération d'un Certificat à usage unique (cf. chapitre 3.2.3.1).

1.3.4.2 [AC ORG] Service de scellement électronique

S'il s'agit de sceller des données électroniques au nom d'Organisations rattachées à l'Abonné, légalement ou par convention, l'AC produit alors des Certificats d'Organisation (cf. chapitre 1.4.2). En effet, l'Organisation, via l'Abonné, utilisera alors un Certificat opéré par Worldline, pour garantir l'intégrité des documents et authentifier leur origine.

Un Certificat d'Organisation peut faire référence à la personne qui la représente légalement, statutairement ou par convention. Soit :

- le représentant légal figurant sur l'extrait KBIS de l'Organisation ;
- une personne dûment autorisée, que ce soit à titre conventionnel ou statutaire, pour représenter l'Organisation et figurer sur le Certificat.

Dans tous les cas, la personne désignée doit être dûment habilitée par les organes compétents au sein de l'Organisation pour pouvoir figurer sur le Certificat.

La personne qui dispose du droit de faire figurer son identité au sein du Certificat devra en justifier auprès de l'Autorité d'Enregistrement pour pouvoir agir comme représentant de l'Organisation. Si l'Organisation n'est pas l'Abonné et qu'elle habilite l'Abonné à agir pour son compte, l'Abonné devra justifier auprès de l'Autorité d'Enregistrement de ses droits à agir au nom de cette Organisation ainsi que les droits de la personne désignée à faire figurer son identité au sein du Certificat à représenter l'Organisation.

Le représentant de l'Abonné est seul habilité à formuler des demandes de Certificat auprès de l'Autorité d'Enregistrement.

Un représentant de l'Abonné doit donc être désigné par écrit auprès de l'Autorité d'Enregistrement. Ce représentant de l'Abonné peut être :

- le représentant légal de l'Abonné (tel qu'il figure sur un extrait KBIS de l'Abonné datant de moins de trois (3) mois) ;
- son représentant conventionnel (tel qu'il figure par exemple sur les statuts) ;
- un représentant habilité par le représentant légal à représenter l'Abonné dans le cadre de l'exécution du Contrat d'Abonnement.

Bien que l'Abonné et l'Organisation soient dans la plupart des cas une seule et même entité, il est possible de les différencier. Par exemple, un Abonné peut souhaiter utiliser un nom de marque plutôt que le nom de l'entreprise abonnée. En outre, dans le cas de filiales multiples d'un groupe, il est possible que l'Abonné et l'Organisation ne portent pas le même nom.

Dans tous les cas, l'Abonné devra démontrer le droit qu'il détient (propriété du nom, document KBIS, mandat, …) à indiquer un nom d'Organisation différent du sien.

L'Abonné, via son représentant légal ou statutaire, peut désigner formellement par écrit un ou plusieurs représentants adjoints d'Abonné également habilités à le représenter. Il doit pour cela en informer l'Autorité d'Enregistrement et leur conférer les pouvoirs nécessaires.

1.3.5 Utilisateurs de Certificats

L'utilisateur d'un Certificat est la personne physique ou morale qui utilise les informations d'un Certificat qu'elle reçoit à des fins décrites au chapitre 1.5.1.1.

Il appartient aux utilisateurs de vérifier la validité du Certificat, à minima avant utilisation, à l'aide :

- des informations contenues dans le Certificat (date de validité, …) ;
- d'informations complémentaires fournies par l'AC telles que sur le statut de révocation du Certificat (cf. chapitre 4.10).

A noter que la signature d'un Document est principalement exploitée par les produits fournis par la société ADOBE™, tels qu'Acrobat Reader©. Ces produits disposent de fonctions de visualisation de la signature du document.

D'autres produits de visualisation de Document ne disposent pas tous des fonctions de visualisation de signature.

1.3.6 Autre participants

Des moyens humains complètent le dispositif :

- exploitants des systèmes informatiques (maintien en condition opérationnelle) ;
- équipes en charge du maintien en conformité.

1.4 Catégories de Certificats

Les AC en ligne délivrent un certain nombre de Certificats :

- [AC OTU LCP] L'AC produit deux (2) types de Certificats ;
- [AC OTU] L'AC produit deux (2) types de Certificats ;
- [AC ORG] L'AC produit deux (2) types de Certificats.

Chaque type de Certificat se distingue notamment par son OID (cf. chapitre 1.2.1).

1.4.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Un Certificat à usage unique est produit dynamiquement par les Autorités de Certification lors du processus de signature électronique initié par l'Abonné à la demande d'une personne physique (Titulaire).

Ce Titulaire peut être une personne physique agissant pour ses propres besoins ou pour les besoins de son Organisation et pour laquelle il est dûment habilité à signer.

Ce Certificat est utilisé au cours d'une session unique de signature (signature des différents Documents d'un contrat pour le Titulaire) par le Dispositif Porteur de Certificats. Il dispose d'une durée de vie très courte comme décrit au chapitre 6.3.2.

L'Abonné transmet la demande de Certificat à usage unique à l'Autorité d'Enregistrement au moyen d'un message signé électroniquement par l'Abonné. Ce message contient :

- les données d'identification du Titulaire ;
- un Cachet électronique permettant de garantir l'intégrité des données d'identification, ainsi que l'identité de l'Abonné.

Une fois la demande de Certificat à usage unique de l'Abonné contrôlée et validée par l'Autorité d'Enregistrement, le Certificat est délivré par l'AC cible qui signe le Certificat contenant l'identité du Titulaire figurant sur le Certificat, vérifiée par l'Abonné.

En effet, l'Abonné est responsable des données d'identification transmises dans la demande à l'Autorité d'Enregistrement et qui permettent de créer un Certificat contenant des données vérifiés du Titulaire.

La clé privée du Titulaire est générée dans un équipement sécurisé et dédiée conformément aux informations données au chapitre 6.2.1.1 de ce document.

Une fois que le Certificat à usage unique a été utilisé pour le Titulaire à la demande de l'Abonné, la clé privée correspondante est détruite dans le HSM comme décrit au chapitre 6.2.10.2. Le Certificat reste toutefois accessible dans le document signé.

1.4.2 [AC ORG] Certificats d'Organisation

Le Certificat d'Organisation est délivré sur demande de l'Abonné à Worldline, pour le compte de ou des Organisations pour lesquelles l'Abonné est habilité à demander un scellement de Documents (conformément à l'utilisation définie au chapitre 1.5.1.1). Ce service est opéré par Worldline dans ses propres locaux.

La demande de ce type de Certificat est opérée selon une procédure se déroulant entre un représentant habilité de l'Abonné et un Opérateur d'Enregistrement Worldline. Les informations à fournir pour la demande sont détaillées au chapitre 4.1.2.2 de ce document.

La présente PC-DPC ne formule pas d'exigences de face à face mais se réserve le droit de procéder à des vérifications complémentaires du type contre appel.

La clé privée d'une Organisation est générée dans un équipement sécurisé et dédié conformément aux informations données au chapitre 6.2.1.1.

1.4.3 Certificats de test

A des fins techniques (test de présence et de fonctionnement du service), de démonstration et de recette des modifications apportées sur le système d'information de production, il est permis d'émettre des Certificats de test sous les AC de production.

L'Abonné peut en effet émettre une demande de création de Certificat de test auprès de l'Autorité d'Enregistrement, pour son propre usage ou pour un Titulaire.

Les Certificats de tests ne peuvent en aucun cas servir à engager le Titulaire, l'Abonné ou Worldline comme un Certificat de production. Toutefois, les obligations de protection et d'utilisation du Certificat pour le Titulaire, l'Abonné et les AC sont identiques à celles définies pour les Certificats de production.

Pour ces Certificats de test, l'attribut « *CommonName* » du champ « *Subject* » doit impérativement être préfixé par la valeur « TEST » (cf. chapitres 7.1.8, 7.1.9 et 7.1.10). Ces Certificats doivent être révoqués dès lors que leur usage n'est plus nécessaire.

Les limitations d'usage et d'engagement de responsabilité applicables aux Certificats de production s'appliquent également aux Certificats de test.

1.5 Usage des Certificats

1.5.1 Domaines d'utilisation applicables

1.5.1.1 Bi-clés et Certificats porteur

La présente PC-DPC traite des Bi-clés et des Certificats électroniques associés à ces Bi-clés, gérés par le Dispositif Porteur de Certificats (défini au chapitre 1.3.3 ci-dessus), afin que les Titulaires des Certificats électroniques puissent, dans le cadre de procédure de souscription ou de transmission dématérialisée :

- [AC OTU][AC OTU LCP] signer électroniquement un Document avec un Certificat à usage unique ;
- [AC ORG] sceller électroniquement un Document avec un Certificat Organisation.

1.5.1.2 Bi-clés et Certificats d'AC et de composantes

Les Bi-clés des AC servent exclusivement à signer des Certificats et des LCR dont les gabarits sont définis au chapitre 7 du présent document.
Leur Certificat est signé par l'Autorité de Certification de niveau supérieur comme décrit au chapitre 1.2.2 de ce document.

1.5.2 Domaines d'utilisation interdits

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 9.15).
Le TSP MediaCert ne pourra être tenu pour responsable de tout détournement d'usage tel que spécifiés.

1.6 Gestion de la PC

1.6.1 Entité gérant la PC

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

1.6.2 Point de contact

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

1.6.3 Entité déterminant la conformité d'une DPC avec cette PC

Cette entité est décrite dans la [PG].

1.6.4 Procédure d'approbation de la conformité de la DPC

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

1.7 Définitions et acronymes

1.7.1 Principales définitions

Une liste des principales définitions des termes techniques employés dans cette PC est présentée ci-dessous.

Abonné : entité Signataire du Contrat d'Abonnement avec le TSP MediaCert pour la délivrance par les AC en ligne :

- [AC ORG] de Certificats d'Organisation à la demande de personnes dûment habilitées au sein de l'Abonné qui lui sont rattachées légalement et/ou conventionnellement ;
- [AC OTU][AC OTU LCP] de Certificats à usage unique au nom des Titulaires tels que définis dans la présente PC-DPC que l'Abonné aura préalablement identifiés ou qui auront été identifiés sous sa responsabilité par des personnes dûment habilitées qui lui sont rattachées conventionnellement.

L'Abonné est en relation directe avec l'AE et assure pour elle un certain nombre de vérifications concernant notamment l'identité et éventuellement les attributs des Titulaires utilisateurs de Certificats.
En ce qui concerne les Certificats à usage unique, l'Abonné est mandaté par les Titulaires pour effectuer une demande en leur nom de Certificats.

Authentification : un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique.

Autorité de Certification (AC) : autorité chargée de l'application de la présente PC-DPC, désigne également l'entité technique qui produit les Certificats à la demande du Service d'enregistrement et plus généralement assure leur gestion (fabrication, livraison, révocation, publication, journalisation, archivage) conformément à cette PC-DPC. Plus d'informations au chapitre 1.3.1.

Autorité de Certification Technique (ACT) : Autorité de Certification agissant sous le nom de l'Autorité de Certification OTU, de l'Autorité de Certificat ORG ou de l'Autorité de Certification OTU LCP.

Autorité d'Enregistrement (AE) : autorité en charge de la réception des demandes de Certificat de l'Abonné, de la vérification de ces demandes, de l'archivage de ces demandes et de leur transmission à l'Autorité de Certification. Le terme désigne également l'entité technique en charge de mettre en œuvre le Service d'enregistrement. Plus d'informations au chapitre 1.3.2.

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).

Cachet électronique : des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières. On parle ici aussi de « Certificat d'Organisation ».

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 (*digest*) ou bien encore les critères d'utilisation. Le tout est signé par la clé privée de l'AC ayant émis le Certificat.

Certificat d'AC fille : catégorie de Certificats délivrés par l'AC Racine pour signer les Certificats d'AC fille et les listes de révocation des AC filles.

Certificat ORG : ou Certificat d'Organisation ou Cachet électronique ; cf. chapitre 1.4.2.

Certificat OTU (One Time Usage) : ou Certificat à usage unique ; cf. chapitre 1.4.1.

Certificat porteur : catégorie de Certificats délivrés par une AC fille à des Titulaires ou à des Organisations. Le Certificat à usage unique et le Certificat Organisation sont des Certificats porteurs.

Chaîne de Certification : ensemble des Certificats nécessaires pour valider la filiation d'un Certificat délivré à une entité.

Composant de l'IGC : plates-formes matérielles (ordinateurs, HSM, lecteur de carte à puce) et produits logiciels jouant un rôle déterminé au sein de l'IGC.

Contrat d'Abonnement : contrat signé entre l'AC et l'Abonné et constitué des documents auxquels il réfère.

Déclaration des pratiques de Certification (DPC) : identifie les pratiques (Organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de Certification électronique aux usagers et en conformité avec la ou les politiques de Certification qu'elle s'est engagée à respecter.

Demande de Certificat : demande formulée par l'Abonné à l'Autorité d'Enregistrement en vue d'obtenir un Certificat pour une personne physique ou morale liée à l'Abonné. Cette personne physique ou morale est préalablement identifiée et authentifiée par l'Abonné ou par les personnes dûment habilitées à cet effet sous la responsabilité de ce dernier. Elle comprend un ensemble d'informations devant être fournies par l'Abonné au Service d'enregistrement en accompagnement de la demande de Certificat.

Dispositif Porteur de Certificats : composant logiciel qui obtient un (ou des) Certificat(s) de l'AC. Ces Certificats sont utilisés selon les applications et les types de Certificats pour des usages définis au chapitre 1.5.1.
Le Dispositif Porteur de Certificat est composé de serveurs et de boitiers cryptographiques opérés conjointement à l'AC. Il garantit le contrôle exclusif des Bi-clés et des Certificats aux porteurs.

Document : document statique électronique au format PDF.

Dossier d'enregistrement électronique : containeur de données au format électronique, il est destiné à contenir l'ensemble des données transmises par un Abonné lors d'une demande de création de Certificat (informations pour le Certificat, données d'identification du Titulaire, …). Ces données sont archivées dans un système d'archivage à vocation probatoire, il est consultable à tout moment par l'AC.

Gabarit d'un Certificat : donnée informatique résultant de l'acte d'enregistrement d'un Abonné demandeur de Certificat auprès du Service d'enregistrement et qui est ensuite transmise à l'Autorité de Certification pour signature.

Hash ou empreinte numérique : désigne le résultat d'une fonction de calcul effectuée sur un contenu numérique de telle sorte qu'une modification même infime de ce contenu, entraîne la modification de l'empreinte. Le hash sert à l'identification de données et à la vérification de l'intégrité des données dans le temps.

Identification électronique : processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique, une personne morale ou bien un personne physique représentant une personne morale.

Lightweight Certificate Policy (LCP) : politique de Certification définie par [ETSI EN 319 411-1] offrant une qualité de service moins onéreuse que le NCP (nécessitant des exigences de politique moindres) à utiliser lorsqu'une évaluation des risques ne justifie pas la charge supplémentaire de satisfaire à toutes les exigences du NCP (ex : identification en face à face).

Normalized Certificate Policy (NCP) : politique de Certification définie par [ETSI EN 319 411-1] qui répond aux meilleures pratiques généralement reconnues par les TSP émettant des Certificats.

Organisation : entité représentant notamment une entreprise, une administration publique, etc. ou pouvant faire référence à un nom de marque ou de société pour laquelle un Certificat d'Organisation ou de Cachet électronique va être délivré à la demande d'un Abonné.

Moyen d'identification électronique : élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne.

Partie prenante : dans le contexte de cette PC-DPC, la partie prenante est l'entité qui utilise le Certificat qu'elle reçoit (ici par le biais d'une signature électronique. Cette signature est associée à un Document).

PDF : format de fichier informatique créé par ADOBE Systems® et dont la spécificité est de préserver la mise en forme définie par son auteur.

Politique de Certification (PC) : document publié décrivant l'ensemble des règles et exigences auxquelles l'AC se conforme dans la mise en place et la fourniture de prestations de confiance. Il indique notamment l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Il identifie aussi les obligations et exigences portant sur les différents acteurs, ainsi que celles pesant sur toutes les composantes intervenant dans la gestion du cycle de vie des Certificats.
La politique de Certification est identifiée par un OID.

Service d'enregistrement : cf. Autorité d'Enregistrement.

Service de gestion des révocations : cf. chapitre 1.3.1.3.

Service d'information sur l'état des Certificats : cf. chapitre 1.3.1.4.

Session de signature : opération comprise entre la demande de signature et la restitution du ou des documents signés par la personne physique ou morale désignée dans la demande. Plusieurs signatures successives peuvent être réalisées avec un même Certificat dans une Session de signature.

Signataire : une personne physique identifiée dans un ou plusieurs documents électroniques et qui crée une signature électronique pour ce ou ces documents.

Signature électronique : suivant le Règlement Européen eIDAS, il s'agit de données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le Signataire utilise pour signer.

Suivant le code civil Français, la signature sert à identifier la personne qui l'appose, à manifester son consentement et à garantir l'intégrité de l'acte auquel elle s'attache.

Il est rappelé que la signature électronique mise en œuvre dans la présente PC-DPC ne répond pas à la définition de la signature qualifiée. Suivant le Règlement Européen eIDAS, l'effet juridique et la recevabilité d'une signature électronique comme preuve en justice ne peuvent être refusés au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature électronique qualifiée.

Titulaire : personne physique identifiée dans le Certificat comme le détenteur de ce Certificat. La génération et l'utilisation exclusive de la clé privée associé à la clé publique indiquée dans le Certificat est confiée au Dispositif Porteur de Certificats.

Utilisateur : cf. Partie Prenante.

1.7.2 Acronymes

Les acronymes utilisés dans la présente PC-DPC sont les suivants :

- **AC :** Autorité de Certification ;
- **AC OTU :** Autorité de Certification délivrant les Certificats décrit dans cette PC-DPC ;
- **ACR :** Autorité de Certification Racine ;
- **AE :** Autorité d'Enregistrement ;
- **AH :** Autorité d'Horodatage ;
- **CC :** Critères Communs (*Common Criteria*) ;
- **CN :** *Common Name* ;
- **CSR :** *Certificate Signing Request* ;
- **DN :** *Distinguished Name* ;
- **DPC :** Déclaration des Pratiques de Certification ;
- **ETSI :** *European Telecommunications Standards Institute* ;
- **HSM :** Ressource Cryptographique Matérielle (*Hardware Security Module*) ;
- **KC :** Cérémonie de Clés (*Key Ceremony*) ;
- **IGC (PKI) :** Infrastructure de Gestion de Clés (*Public Key Infrastructure*) ;
- **LAR :** Liste des Certificats d'Autorités de Certification Révoqués ;
- **LCR :** Liste des Certificats Révoqués ;
- **OCSP :** Protocole de Vérification de Certificat en ligne (*Online Certificate Status Protocol*) ;
- **OE** : Opérateur d'Enregistrement ;
- **OID :** *Object Identifier* ;
- **PC :** Politique de Certification ;
- **PSI :** Politique de Sécurité de l'Information ;
- **RSSI :** Responsable Sécurité des Systèmes d'Informations ;
- **RFC :** *Request For Comment* ;
- **RSA :** *Rivest Shamir Adelman* ;
- **SHA :** *Secure Hash Algorithm* ;
- **URL :** *Uniform Resource Locator* ;
- **UTC :** Temps Universel Coordonné (*Universal Time Coordinated*).

1.7.3 Références

1.7.3.1 Réglementation

Référence	Description
[CNIL]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée

Référence	Description
[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

1.7.3.2 Réglementation technique

Référence	Description
[RFC 3647]	Network Working Group – November 2003 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[RFC 5280]	Network Working Group – May 2008 Internet X.509 Public Key Infrastructure and Certificate Revocation List (CRL) Profile
[RFC 6960]	IETF – June 2013 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP
[ETSI TS 119 312]	ETSI TS 119 312 v1.2.2 (2018-09) Electronic Signature and Infrastructures (ESI); Cryptographic Suites
[ETSI EN 319 401]	ETSI EN 319 401 v2.2.1 (2018-04) Electronic Signature and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	ETSI EN 319 411-1 v1.2.2 (2018-04) Electronic Signature and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing Certificates; Part 1: General requirements
[ETSI EN 319 412-2]	ETSI EN 319 412-2 v2.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); Certificates Profiles; Part 2: Certificate profile for Certificates issued to natural persons
[ETSI EN 319 412-3]	ETSI EN 319 412-3 v1.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); Certificates Profiles; Part 3: Certificate profile for Certificates issued to legal persons

1.7.3.3 Documentation interne

Référence	Description
[DTPC]	Documentation Technique des Pratiques de Certification Autorités de Certification en ligne Référence : WLS-OTU-F003
[CGA]	Conditions Générales d'Abonnement au service de signature électronique OTU et/ou cachet électronique Autorités de Certification en ligne Référence : WLS-OTU-F008

Référence	Description
[CGS]	Conditions Générales des Services Autorités de Certification en ligne Référence : WLS-OTU-F022
[PCA]	Plan de Cessation d'Activité Autorités de Certification en ligne Référence : WLS-OTU-F028
[PCRA]	Plan de Continuité et de Reprise d'Activité Autorités de Certification en ligne Référence : WLS-OTU-F029
[PESV]	Protocole d'Externalisation des Sauvegardes de Vendôme Worldline Référence : Protocole d'Externalisation des Sauvegardes de Vendôme
[PG]	Politique Générale du TSP MediaCert TSP MediaCert Référence : WLM-TSP-F094 OID : 1.2.250.1.111.20.1.1
[PGI]	Politique de Gestion des Incidents Worldline Référence : WLM-SEC-0008
[PTVDP]	Procédure de Traitement des Violations de Donnés Personnelles Worldline Référence : WLP-DPO-F017

1.7.3.4 Documentation externe

Référence	Description
[Notification ANSSI]	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) Formulaire de déclaration d'un incident de sécurité relatif à un produit ou un service qualifié

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

2.1 Entités chargées 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 publiées

Les informations publiées par les AC en ligne sur le site web du TSP MediaCert sont les suivantes :

- la présente PC-DPC ;
- les conditions générales des services (CGS) en cours de validité ;
- les conditions générales d'abonnement (CGA) en cours de validité ;
- les conditions générales de vente (CGV) en cours de validité ;
- les listes des Certificats révoqués (LCR) ;
- le Certificat des AC en ligne en cours de validité ;
- les Certificats de la gamme de test.

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

Les URLs pour accéder à cette PC-DPC ainsi qu'à la LCR et au répondeur OCSP sont disponibles dans les extensions des Certificats délivrés par les AC conformément au chapitre 7.1 du présent document.

La politique de gestion de preuve (PGP) est rendue disponible à l'Abonné sur demande électronique (via e-mail) au point de contact défini au chapitre 1.6.2 du présent document.

2.3 Délais et fréquences de publication

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

Par ailleurs, les politiques de certification sont régulièrement mises à jour et publiées, notamment en cas de changement majeur (cf. chapitre 9.11 et 9.12).

Le délai et la fréquence de publication des informations sur l'état des Certificats sont respectivement indiqués aux chapitres 4.9.8 et 4.9.7 du présent document. De plus, les Certificats des AC sont publiés suite à leur génération et avant toute Certification.

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 sont conformes aux spécifications de la norme X.500.

Dans chaque Certificat conforme à la norme X509, les champs « *Issuer* » (AC émettrice) et « *Subject* » (sujet) sont identifiés par un « *Distinguished Name* » (DN) de type X.501 sous forme d'une « *PrintableString* » (chaîne imprimable).

3.1.2 Nécessité d'utilisation de noms explicites

3.1.2.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Dans le cas de Certificat à usage unique, les Certificats émis au nom du Titulaire dans le cadre de la présente PC-DPC contiennent le prénom et nom figurant dans les justificatifs d'identité valides présentés par le Titulaire.

3.1.2.2 [AC ORG] Certificats d'Organisation

Dans le cas de Certificat d'Organisation, les Certificats émis contiennent :

- le nom de l'Abonné ; et
- le nom de l'Organisation ; et
- le prénom et nom figurant dans les justificatifs d'identité valides présentés par la personne habilité par l'Abonné à représenter cette Organisation ; ou
- le nom de l'unité dans l'Organisation à laquelle est destiné le Certificat.

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 de différentes formes de nom

L'interprétation d'informations telles que le champ « *Distinguish Name* » est indiquée dans chaque gabarit de Certificat au chapitre 7 de cette PC-DPC.

3.1.5 Unicité des noms

Le « *Distinguished Name* » (DN) est unique pour chaque Titulaire ou Organisation. Toute demande de l'Abonné ne respectant pas cette règle est refusée par l'Autorité d'Enregistrement (cf. chapitre 4.2.1). Durant tout le cycle de vie des AC et après leur cessation d'activité, un « *Distinguished Name* » (DN) attribué à un Titulaire ou à une Organisation par ces AC ne peut donc être attribué à un autre Titulaire ou une autre Organisation.

Les règles appliquées pour obtenir cette unicité sur les DN sont les suivantes :

- [AC OTU][AC OTU LCP] pour les Certificats à usage unique, l'unicité est garantie par :
    - l'identifiant du container de trace dans le champ « Common Name » du DN ; et
    - le champ « SERIALNUMBER » du DN ;
- [AC ORG] pour les Certificats d'Organisation, l'unicité est garantie par :
    - le champ « *Organisation ID* » du DN qui doit être unique pour chaque Organisation. Cela est notamment vérifiée par l'AE lors de l'acceptation de la demande de création ; et
    - le champ « SERIALNUMBER » du DN.

Plus d'informations concernant la construction de certain de ces champs sont disponibles au niveau du chapitre 7.1 de ce document.

3.1.6 Identification, authentification et rôle des marques déposées

Les informations sont disponibles au chapitre 3.2.2.2 de la présente PC-DPC.

3.2 Validation initiale d'identité

3.2.1 Méthode pour prouver la possession de la clé privée

3.2.1.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Dans le cadre d'une utilisation sur une courte période (cf. chapitre 6.3.2), le contrôle de possession de la clé privée est réalisé au moyen d'une vérification cryptographique de bas niveau d'une première signature produite au moyen de la clé privée.

Si la vérification échoue, alors :

- le Document n'est pas signé ;
- la clé privée est détruite (cf. chapitre 6.2.10.2) ;
- l'Abonné qui a fait la demande reçoit un message d'erreur l'informant de l'échec de cette demande.

Le Titulaire du Certificat n'est pas soumis à cette preuve de possession.

3.2.1.2 [AC ORG] Certificat d'Organisation

La preuve de la possession de la clé privée fournie par le Dispositif Porteur de Certificats est garantie lors de la génération de la demande par la signature du message avec la clé privée qui correspond à la clé publique contenue dans le message PKCS#10 (CSR) envoyé à l'Autorité d'Enregistrement.

Ces formats de requête intègrent une signature par la clé privée correspondante afin de garantir l'intégrité et la preuve de la possession de la clé privée.

L'individu habilité dans le Certificat n'est pas soumis à cette preuve de possession.

3.2.2 Validation de l'identité des organismes

3.2.2.1 Validation d'un Abonné

La validation de l'identité d'un Abonné nécessite de suivre les étapes décrites ci-après et de recueillir l'ensemble des informations requises. L'Autorité d'Enregistrement conserve l'ensemble des documents transmis lors de la souscription de l'Abonné au Service.

Signature du Contrat d'Abonnement

Le statut d'Abonné est conditionné à la mise en place préalable d'une relation contractuelle entre l'Abonné et le TSP MediaCert. Il s'agit du Contrat d'Abonnement au service de signature électronique à usage unique et/ou Cachet électronique. La signature de ce Contrat d'Abonnement atteste notamment de l'acceptation des obligations de l'Abonné qui lui sont décrites dans ce document au chapitre 9.6.3.1 ainsi que dans les Conditions Générales d'Abonnement [CGA] (documents joints au Contrat d'Abonnement).

Désignation ou nomination de représentants au sein de l'Abonné

Un représentant de l'Abonné doit alors être désigné auprès de l'Autorité d'Enregistrement afin qu'il devienne l'interlocuteur de celle-ci pour les demandes de Certificats d'Organisation. Ce représentant de l'Abonné peut être :

- le représentant légal de l'Abonné (tel qu'il figure sur un extrait KBIS de l'Abonné datant de moins de trois mois) ;
- son représentant conventionnel (tel qu'il figure par exemple sur les statuts) ;
- un représentant habilité (délégation, pouvoir ou mandat) par le représentant légal à représenter l'Abonné dans le cadre de l'exécution du Contrat d'Abonnement.

L'Abonné, via son représentant légal ou statutaire, peut désigner formellement par écrit (via la fiche d'information du représentant adjoint de l'Abonné aux AC en ligne fournie par l'Autorité d'Enregistrement) un ou plusieurs représentants adjoints d'Abonné également habilités à le représenter. Il doit pour cela en informer l'Autorité d'Enregistrement et leur conférer les pouvoirs nécessaires.

Fourniture de la documentation nécessaire lors de la souscription au Contrat d'Abonné

Par ailleurs, lors de la souscription du Contrat d'Abonnement, le représentant de l'Abonné désigné doit fournir :

- les Conditions Générales d'Abonnement [CGA] qu'il aura paraphé ou fait parapher par le responsable légal de l'Organisation ;
- la fiche d'information du représentant de l'Abonné aux AC en ligne, fournie par l'Autorité d'Enregistrement, dûment complétée et signée par le représentant de l'Abonné. Cette fiche contient entre autre l'adresse physique de l'Abonné et une adresse e-mail valide de son représentant, permettant de le contacter. Cette adresse e-mail sera entre autre utilisée pour transmettre les informations lors de la création de Certificats d'Organisation ; et
- la politique d'identification qu'il met en œuvre, en respectant les prescriptions et recommandations qui lui ont été faites par l'Autorité d'Enregistrement, uniquement dans le cas où il souhaite souscrire au service de Certificats à usage unique. Celle-ci doit être

validée par l'AE et peut être contrôlée par l'AE conformément à ce qui est écrit au chapitre 3.2.3.1 ; et

- une copie d'un document officiel d'identité en cours de validité au moment de la contractualisation comportant une photographie d'identité parmi les documents définis ci-après : carte nationale d'identité, passeport ou titre de séjour ; et

- un extrait KBIS datant de moins de trois (3) mois au moment de la contractualisation, ou les statuts publiés en vigueur de l'Organisation à laquelle il appartient, comportant son nom et sa qualité et tous documents valides nécessaires à justifier ses pouvoirs ;

- s'il ne figure pas sur l'extrait de KBIS datant de moins de trois (3) mois, ou sur les statuts publiés en vigueur de cette Organisation, il devra être dûment habilité par le représentant légal de l'Abonné dans le cadre d'un pouvoir écrit pour le représenter avec la nature exhaustive des pouvoirs qui lui sont conférés.

L'ensemble de ces éléments sont par ailleurs cité dans une notice qui est fourni à l'Abonné avec le Contrat d'Abonnement.

3.2.2.2 [AC ORG] Validation d'une Organisation

La validation d'une Organisation comme bénéficiaire des services repose sur la validation préalable de l'identité de l'Abonné (cf. chapitre 3.2.2.1). Elle se fait lors de la réception d'une demande de création de Certificat, l'interlocuteur de l'AC étant uniquement l'Abonné.

Comme décrit au chapitre 1.3.4.2, une Organisation est représentée par un individu habilité : le représentant de l'Organisation. Les informations concernant l'Organisation à faire parvenir à l'Autorité d'Enregistrement par l'Abonné lors d'une demande de création de Certificat sont les suivantes :

Dans le cas où l'Organisation et l'Abonné sont deux entités différentes

- toute pièce, valide lors de la demande de création de Certificat, permettant de démontrer le droit et le pouvoir de l'Abonné à faire figurer le nom de l'Organisation dans le Certificat.

Dans tous les cas

- si les Conditions Générales d'Abonnement [CGA] ont évoluées depuis la contractualisation ou la dernière demande de création de Certificat, ledit document à jour est à retourner paraphé par le représentant légal ou par le représentant de l'Abonné habilité ;

- une demande de création de Certificat, signée et datée par représentant légal, par le représentant de l'Abonné ou bien l'un de ses adjoints, spécifiant :

    - le nom de l'Abonné à faire figurer sur le Certificat électronique ; et

    - le nom de l'Organisation à faire figurer sur le Certificat électronique ; et

    - le nom et prénom de l'individu habilité à représenter l'Organisation et identifié dans le Certificat ; ou

    - le nom de l'unité dans l'Organisation à laquelle est destiné le Certificat.

Ce droit de l'Abonné à faire figurer le nom de l'Organisation dans le Certificat repose sur l'ensemble des éléments qui suivent :

- toute pièce, valide lors de la demande de création de Certificat, attestant de l'existence de l'Organisation (extrait de KBIS datant de moins de trois (3) mois ou, original ou copie de

tout acte ou extrait de registre officiel datant de moins de trois (3) mois constatant la dénomination, la forme juridique, l'adresse du siège social et l'identité des associés et dirigeants sociaux mentionnés aux 1° et 2° de l'article R. 123-54 du code de commerce ou de leurs équivalents en droit étranger, …) ;

- en effet, lorsque l'identité d'un individu vient à devoir figurer dans le Certificat, l'Abonné doit transmettre à l'Autorité d'Enregistrement :
    - toute pièce, valide lors de la demande de création de Certificat, permettant de démontrer l'appartenance de l'individu habilité à l'Organisation ;
    - une copie de document officiel d'identité en cours de validité de l'individu habilité parmi les documents suivants :
        - carte nationale d'identité ;
        - passeport ;
        - titre de séjour.

      L'Autorité d'Enregistrement conserve cette copie.
    - l'adresse postale, une adresse e-mail et un numéro de téléphone permettant à l'Autorité d'Enregistrement de contacter cet individu habilité.

La présente PC-DPC ne formule pas d'exigences en matière d'identification en face à face physique. Toutefois, l'Autorité d'Enregistrement pourra peut procéder à des vérifications complémentaires.

3.2.3 Validation de l'identité d'un individu

3.2.3.1 [AC OTU][AC OTU LCP] Certificat à usage unique

La demande de création de Certificat au nom d'un Titulaire est réalisée par l'Abonné auprès de l'Autorité d'Enregistrement.
Cette demande est réalisée sous forme électronique car elle doit être signée, au moyen d'une signature électronique, par le demandeur (cf. chapitre 3.2.5.1). Elle contient à minima les données du Titulaire suivantes :

- son prénom et son nom ;
- sa date et son lieu de naissance.

L'Abonné peut également préciser pour le dossier d'enregistrement :

- la civilité du Titulaire ;
- l'adresse postale du Titulaire ;
- le numéro de téléphone du Titulaire ;
- l'adresse mail du Titulaire.

L'Abonné peut compléter les informations portées ci-dessus par des informations connues au préalable et propres au futur Titulaire, permettant de l'identifier au sein d'une base de données préétablie.

Seules les informations « prénom et nom » du Titulaire figurent dans les Certificats produits par les AC. Cependant, l'ensemble des informations susvisées sont conservées par l'Autorité d'Enregistrement dans le dossier d'enregistrement au format électronique associé à l'émission du Certificat, conformément au chapitre 5.4 de ce présent document, ceci dans le but d'appuyer la preuve d'identification.

La conservation de ces données est nécessaire car elles sont fournies pour la constitution du dossier d'enregistrement qui est associé à chaque émission de Certificat. Ce dossier d'enregistrement rassemble les données citées ci-dessus, décrivant les processus et données d'identification du client final (Titulaire).

Le chapitre 3.1.5 du présent document définit par ailleurs la manière dont l'unicité du « *Distinguished Name* » dans les Certificats à usage unique est garantie.

Politique d'identification
L'Abonné doit préciser à l'AE par écrit, lors de sa contractualisation avec le TSP MediaCert dans le cadre de l'émission de Certificats à usage unique, la politique d'identification qu'il a mis en place (cf. chapitre 3.2.2.1, section *« Fourniture de la documentation nécessaire lors de la souscription au Contrat d'Abonné »*) afin de vérifier l'identité civile déclarée par le futur Titulaire.

Les procédés d'identifications contenus dans cette politique doivent s'appuyer a minima sur la vérification d'un document officiel en cours de validité comportant la photographie du Titulaire (carte nationale d'identité, passeport ou titre de séjour) ou sur tout autre procédé officiel valide permettant ou ayant permis, préalablement à la délivrance de Certificat, de vérifier l'identité déclarée d'un Titulaire. Plus particulièrement :

- [AC OTU LCP] les contrôles de l'identité du futur Titulaire pourront se faire de manière automatisés permettant de vérifier l'identité déclarée du Titulaire ;

- [AC OTU] les contrôles de l'identité du futur Titulaire devront être réalisés par des opérateurs afin de pouvoir vérifier l'identité du Titulaire de manière physique.

Dans tous les cas, au cours du processus d'identification, les contrôles de l'identité du futur Titulaire devront s'appuyer sur des documents d'identité valides légalement, lesquels peuvent être présentés dans certains pays, sous forme électronique. En effet, dans certains Etats, l'étape d'identification peut être réalisée sur la base d'une carte d'identité électronique ou peut s'appuyer sur d'autres Moyens d'identification électroniques reconnus valide légalement pour réaliser une identification fiable. Dans ce cadre, l'Abonné vérifie que le Titulaire est bien détenteur d'une carte d'identité électronique valide ou possède d'autres Moyens d'identification électroniques reconnus valides légalement pour réaliser une identification fiable.

Ces documents d'identité sous forme physique ou électroniques servent à conforter les données d'identification que l'Abonné a recueillie préalablement auprès du Titulaire, l'émission d'un Certificat à usage unique s'inscrivant dans le processus de signature électronique.

Les mentions à relever, vérifier et conserver sont notamment les prénoms, noms, date et lieu de naissance de la personne, ainsi que la nature et la date de délivrance du document.

L'Autorité d'Enregistrement se réserve le droit d'apprécier la fiabilité du procédé d'identification mis en place et de ne pas délivrer de Certificat si la politique d'identification de l'Abonné est évaluée comme n'apportant pas un niveau suffisant de fiabilité. L'AE procédera notamment à des contrôles réguliers de cette politique en réalisant des échantillonnages conformément à la procédure d'échantillonnage de l'AE. En cas d'écarts avec ladite procédure, l'Abonné s'engage à établir un plan d'action avec le TSP MediaCert pour résorber lesdits écarts. La non-application de ce plan d'action ou le constat d'écarts lors de la campagne d'échantillonnage suivante pourront

conduire à une désactivation du service de Signature électronique utilisant des Certificats à usage unique.

La politique d'identification mentionnée ci-dessus est complétée par le descriptif du procédé qui sera utilisé par le Titulaire pour consentir à procéder à une signature électronique au moyen du Certificat à usage unique (Politique de recueil des consentements).
Cette politique de recueil des consentements détaille, pour chacun des consentements à obtenir dans le cadre de la mise en œuvre de cette signature électronique, l'identification du moyen par lequel le Titulaire va exprimer son accord. Avant de pouvoir signer électroniquement, le Titulaire doit, en effet :

- prendre connaissance des conditions d'utilisation de la signature électronique et de ses obligations telles que décrites par l'Abonné dans un support durable mis à sa disposition sous une forme lisible et explicite ;
- consentir à la signature, sous forme électronique, dans le cadre de la transaction à laquelle il est partie en acceptant les termes et conditions, relatives à l'utilisation du Certificat à usage unique ;
- accepter la tenue d'un registre par l'Autorité d'Enregistrement lui permettant de traiter et conserver les renseignements d'identité utilisés nécessaire à la génération du Certificat à usage unique, pendant la durée fixée par l'exercice de sa mission et des audits y relatifs ;
- dans le cadre de contrôles automatisés de son identité, donner son accord l'automatisation dudit contrôle ;
- confirmer la validité des informations contenues dans le Certificat ;
- en conséquence de ce qui précède, donner mandat express à l'Abonné pour que celui-ci puisse procéder auprès de l'Autorité d'Enregistrement à une demande de Certificat à usage unique pour qu'il puisse signer. Il est précisé que dans ce cadre, les consentements donnés par le Titulaire enclenchent une demande automatisée au nom de l'Abonné de signature électronique auprès de l'Autorité d'Enregistrement.

Les procédés de validation de l'expression et du recueil du consentement du Titulaire choisis par l'Abonné peuvent être parmi les suivants :

- une capture électronique de signature manuscrite du Titulaire ;
- l'envoi d'un code OTP reçu par SMS sur le téléphone portable personnel du Titulaire.

La liste qui figure ci-dessus est à considérer uniquement à titre d'exemple et n'est pas exhaustive.

Le procédé d'identification étant décrit par l'Abonné, il lui appartient de :

- le mettre en œuvre ou de le faire mettre en œuvre sous sa responsabilité. Si des personnes sont désignées et habilitées par l'Abonné pour réaliser cette identification sous sa responsabilité, cela doit alors être stipulé par l'Abonné dans la politique d'identification qu'il fournit à l'Autorité d'Enregistrement ;
- transmettre à l'AE, dans un dossier d'enregistrement électronique, les données d'identifications capturées ainsi que les justificatifs d'identité qui lui ont été fournis lors de la mise en œuvre du processus de signature électronique.

Exceptions au principe de transmission des éléments justifiant l'identité des Titulaires à l'AE

L'Abonné transmet donc à l'Autorité d'Enregistrement les copies numériques de l'ensemble des éléments utilisés pour la vérification de l'identité du futur Titulaire, excepté dans les cas suivants :

- le titulaire appartient à l'Organisation de l'Abonné. En effet, il n'y a pas lieu pour l'Abonné de procéder à un contrôle supplémentaire d'identité si l'Abonné a mis à la disposition du futur Titulaire un moyen d'authentification fiable et accepté par l'AE, notamment pour accéder à sa boîte mail professionnelle ou pour se connecter à l'application requérant la signature de celui-ci.

  Dans ce cadre, l'Abonné doit demander au futur Titulaire d'assurer la sécurisation de son ordinateur, de sa boîte mail professionnelle et de ses identifiants.

  L'AE est amenée à s'assurer que le Titulaire appartenait bien à l'Organisation de l'Abonné au moment de la signature en réalisant des contrôles par échantillonnage comme cité en amont dans ce chapitre.

- l'Abonné conserve les éléments de vérification de l'identité du futur Titulaire d'identité pour le compte de l'AE. Dans ce cadre, l'Abonné doit conserver ces éléments de façon sécurisée. L'AE procédera alors aux déclarations nécessaires auprès de la CNIL en vue de pouvoir répondre aux obligations qui pèsent sur les Autorités de Certification vis-à-vis de leurs auditeurs.

  L'AE est amenée à s'assurer que le contrôle de l'identité du futur Titulaire a effectivement été mis en œuvre par l'Abonné en réalisant des contrôles par échantillonnage comme cité en amont dans ce chapitre.

3.2.3.2 [AC OTU] Certificat d'Organisation

Les informations sont disponibles au chapitre 3.2.2.2, section *« Concernant le droit de l'Abonné à faire figurer le nom de l'Organisation dans le Certificat »*.

3.2.4 Informations non-vérifiées

Les Certificats émis par les Autorités de Certification conformément à cette PC-DPC ne comportent pas d'informations non vérifiées à l'exception de l'e-mail et du champ *Organization Unit* (OU) correspondant au nom d'unité de l'Organisation au sein du *Distinguished Name* (DN) du *Subject*.

3.2.5 Validation de l'autorité du demandeur

Qu'il s'agisse d'un Certificat à usage unique ou d'un Certificat d'Organisation, la demande est effectuée par l'Abonné qui se doit d'être préalablement identifié avant toute demande de création de Certificat, la validation initiale d'un Abonné étant décrite au chapitre 3.2.2.1.

Lors de chaque demande de création de Certificat, l'Abonné s'authentifie auprès de l'Autorité d'Enregistrement et du Dispositif Porteur de Certificats. L'authentification se fait différemment selon le type de Certificat demandé.

3.2.5.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Lors d'une demande de création de Certificat à usage unique et de signature auprès de l'Autorité d'Enregistrement (qui contacte alors le Dispositif Porteur de Certificats), l'Abonné doit s'authentifier et signer électroniquement la demande.

L'authentification de l'Abonné se fait alors par Certificat. Ce Certificat doit être émis par une Autorité de Certification approuvée par le TSP MediaCert comme décrit dans le document [DTPC].

3.2.5.2 [AC ORG] Certificat d'Organisation

Lors d'une demande de création de Certificat d'Organisation auprès de l'Autorité d'Enregistrement de la part du représentant de l'Abonné, l'authentification de celui-ci est effectuée par l'Autorité d'Enregistrement.

L'authentification de l'Abonné se fait alors par une demande manuscrite signée. L'authenticité de cette demande est vérifiée par l'AE à l'aide de la signature présente sur la copie du justificatif d'identité, conservée par l'AE, ainsi qu'un faisceau d'éléments lié à la relation commerciale que Worldline entretient avec l'Abonné.

3.2.6 Critères d'interopérabilité

La présente PC-DPC ne formule aucune exigence à ce sujet.

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

3.3.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Dans le cadre de la présente PC-DPC, il n'existe pas de fonction de renouvellement des clés pour cette catégorie de Certificat. En effet, comme le nom l'indique, ce type de Certificat est à usage unique.

3.3.1.1 Identification et validation pour un renouvellement courant

Sans objet.

3.3.1.2 Identification et validation pour un renouvellement après révocation

Sans objet.

3.3.2 [AC ORG] Certificats d'Organisation

Pour cette catégorie de Certificat, une demande de renouvellement des clés est traitée comme une demande initiale de création. Par conséquent, un nouveau Certificat Organisation ne peut pas être fourni sans renouvellement également de la Bi-clé correspondante (cf. chapitre 4.6).

3.3.2.1 Identification et validation pour un renouvellement courant

Sans objet.

3.3.2.2 Identification et validation pour un renouvellement après révocation

Sans objet.

3.4 Identification et validation d'une demande de révocation

3.4.1 [AC OTU][AC OTU LCP] Certificat à usage unique

Dans le cadre de l'utilisation d'un Certificat ayant une durée de vie aussi courte (cf. chapitre 6.3.2), la révocation ne peut intervenir que lors de son utilisation au cours d'une Session de signature. C'est pourquoi le Certificat d'un Titulaire ne peut être révoqué que sur la demande du Dispositif Porteur de Certificats (cf. chapitre 4.9.2.1).

Cette demande est donc transmise par le Dispositif Porteur de Certificats à l'Autorité d'Enregistrement qui redirige ensuite la demande vers l'Autorité de Certification émettrice du Certificat concerné par la révocation. Celle-ci valide automatiquement la demande et effectue alors la révocation en direct.

Toute demande de révocation de Certificat à usage unique provenant du Dispositif Porteur de Certificats est considérée comme valide.

3.4.2 [AC ORG] Certificat d'Organisation

Un Certificat d'Organisation peut être révoqué par :

- l'individu habilité et désigné dans le Certificat en question, ou une personne explicitement habilitée et désignée par lui. La demande est alors transmise à l'Autorité d'Enregistrement qui la redirige, vers l'Autorité de Certification pour validation et exécution si la demande est en règle ;

- l'Autorité de Certification émettrice du Certificat.

L'identification est alors procédée comme définie au chapitre 4.9.3.2.

4 Exigences opérationnelles sur le cycle de vie des Certificats

4.1 Demande de création d'un Certificat

4.1.1 Origine d'une demande

4.1.1.1 [AC OTU][AC OTU LCP] Certificats à usage unique

La création d'un Certificat à usage unique ne peut être demandée que par un Abonné identifié auprès de l'Autorité d'Enregistrement (cf. chapitre 3.2.2.1). L'Abonné s'oblige, avant de procéder à toute demande auprès de l'AE, à procéder, ou faire procéder sous sa responsabilité, à l'identification du futur Titulaire ainsi qu'à recueillir les consentements du Titulaire tels que décrits au chapitre 3.2.3.1 afin que celui-ci puisse bénéficier du présent service.

4.1.1.2 [AC ORG] Certificats d'Organisation

La création d'un Certificat d'Organisation ne peut être demandée que par un Abonné identifié auprès de l'Autorité d'Enregistrement via son représentant ou son représentant adjoint, conformément au chapitre 3.2.2.1.

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

4.1.2.1 [AC OTU][AC OTU LCP] Certificats à usage unique

L'ensemble des informations qui doivent faire partie à minima de la demande sont précisées au chapitre 3.2.3.1 de la présente PC-DPC.

La demande est établie par l'Abonné sur la base d'informations qu'il aura collectées à partir de sources fiables et de justificatifs valides auprès du Titulaire (cf. chapitre 4.1.1.1).

L'Abonné s'engage vis-à-vis de Worldline au travers du Contrat d'Abonnement à :

- informer l'Autorité d'Enregistrement, par écrit, de ses procédés d'identification des futurs Titulaires qu'elle souhaite mettre en œuvre via la fourniture de sa Politique d'Identification ;
- mettre en œuvre lesdits procédés d'identification du futur Titulaire, définis dans sa politique d'identification conformément au chapitre 3.2.3.1 et les appliquer avant de procéder toute demande de création de Certificat au nom du futur Titulaire ;
- informer le futur Titulaire des différentes étapes qu'il devra suivre en vue de l'attribution d'un Certificat à son nom afin de pouvoir signer électroniquement le document ou les documents qui lui seront présentés par l'Abonné et, à cette fin, obtenir l'accord préalable du futur Titulaire au choix de la signature électronique pour signer ces documents et aux obligations qui découlent de ce choix tels que précisés au chapitre 3.2.3.1 dont celui notamment de donner pouvoir à l'Abonné pour faire les demandes de Certificat à usage unique au bénéfice du Titulaire auprès de l'Autorité d'Enregistrement et d'accepter le traitement de ses données personnelles par l'AE et l'AC ;
- en conséquence de ce qui précède, informer le futur Titulaire des traitements réalisés de ses informations personnelles par l'AE et l'AC et à cette fin obtenir les consentements nécessaires préalables de celui-ci au traitement et à la conservation de ses données dans le cadre de la génération du Certificat à usage unique et de la gestion de preuves ;

- fournir l'ensemble des informations nécessaires à l'émission du Certificat.

Une fois la demande transmise à l'Autorité d'Enregistrement et validée, celle-ci la transmet à l'Autorité de Certification pour la génération du Certificat à usage unique au nom du Titulaire.

Le TSP MediaCert ne peut être tenu responsable si l'Abonné et/ou le Titulaire ne respectent pas les engagements qu'ils ont acceptés pour bénéficier du service de signature électronique.

Le TSP MediaCert se réserve la possibilité de refuser l'émission d'un Certificat à usage unique s'il s'avère que les obligations du Titulaire, lié à l'Abonné, ou/et les obligations de l'Abonné ne sont pas respectées.

4.1.2.2 [AC ORG] Certificats d'Organisation

L'ensemble des informations qui doivent faire partie à minima de la demande sont précisées au chapitre 3.2.3.2 de la présente PC-DPC.

La demande est établie par le représentant d'Abonné à travers un dossier de demande de création de Certificat d'Organisation. Ce dossier est complété par le représentant habilité de l'Organisation puis est transmis à l'Autorité d'Enregistrement qui procède au traitement de la demande comme défini au chapitre 4.2.1.2 du présent document.

Le TSP MediaCert ne peut être tenue responsable si l'Abonné ne respecte pas les engagements qu'il a acceptés dans le cadre du Contrat d'Abonnement.

Le TSP MediaCert se réserve la possibilité de refuser l'émission d'un Certificat d'Organisation s'il s'avère que les obligations de l'Abonné ne sont pas respectées.

4.2 Traitement d'une demande de création d'un Certificat

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

4.2.1.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Une fois la demande de l'Abonné reçue par l'Autorité d'Enregistrement, celle-ci procède aux opérations suivantes :

- vérification de l'identité de l'Abonné (cf. chapitre 3.2.2.1) : l'AE vérifie les informations transmises par l'Abonné et vérifie que celui-ci est effectivement connu de celle-ci ;
- vérification de la demande : l'AE vérifie que la demande de l'Abonné est signée électroniquement en son nom ;
- validation des consentements et des données d'identité du Titulaire : l'AE valide la présence des informations nécessaires (cf. chapitre 3.2.3.1). La signature de la demande, réalisée par l'Abonné, atteste quant à elle de la validité des informations fournies pour figurer dans le Certificat.

Une fois que ces opérations ont été effectuées, si tout est correct alors l'Autorité d'Enregistrement émet la demande de génération du Certificat à l'AC cible et conserve une trace de la demande de l'Abonné archivée au format numérique.

[AC OTU LCP] L'AC génèrera alors un Certificat contenant les données d'identité du titulaire comme défini au chapitre 7.1.5 du présent document.

[AC OTU] L'AC génèrera alors un Certificat contenant les données d'identité du titulaire comme défini au chapitre 7.1.6 du présent document.

Sinon, la demande est rejetée (cf. chapitre 4.2.2.1).

4.2.1.2 [AC ORG] Certificats d'Organisation

Une fois la demande du représentant de l'Abonné reçue par l'Autorité d'Enregistrement, celle-ci procède aux opérations suivantes :

- validation des données d'identification de l'Organisation et de l'individu la représentant au sein de l'Organisation (cf. chapitre 3.2.2.2) : complétion, unicité et exactitude des informations ;
- vérification de la complétude du dossier de demande de création de Certificat d'Organisation : l'AE s'assure notamment de disposer d'une information lui permettant de contacter le futur Titulaire du Certificat.

Une fois que ces opérations ont été effectuées, si tout est correct alors l'Autorité d'Enregistrement émet la demande de génération du Certificat à l'AC et conserve une trace de la demande du représentant de l'Abonné archivée au format numérique.

Sinon, la demande est rejetée (cf. chapitre 4.2.2.2).

4.2.2 Acceptation ou rejet de la demande

4.2.2.1 [AC OTU][AC OTU LCP] Certificats à usage unique

L'acceptation ou le rejet est faite automatiquement.

En cas de rejet de la demande, l'Autorité d'Enregistrement en informe l'Abonné par le biais d'une notification technique à la requête de l'Abonné. La notification comprend la justification du rejet. Une nouvelle demande doit être faite.

4.2.2.2 [AC ORG] Certificats d'Organisation

L'acceptation ou le rejet est faite manuellement.

En cas de rejet de la demande, l'Autorité d'Enregistrement en informe le point de contact identifié dans la demande en justifiant le rejet. L'AE peut alors demander des documents manquants pour compléter le dossier d'enregistrement, mais ne peut en aucun cas modifier les données signées. Une nouvelle demande doit être faite.

4.2.3 Délai d'établissement du Certificat

4.2.3.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Une fois la demande de création d'un Certificat à usage unique validée, la génération du Certificat est immédiate.

4.2.3.2 [AC ORG] Certificats d'Organisation

Une fois la demande de création d'un Certificat d'Organisation validée, la génération du Certificat est réalisée dans les meilleurs délais.

Un document technique spécifique retraçant la génération du Certificat ainsi que les intervenants techniques est créé et conservé à titre de journal d'exécution.

4.3 Délivrance du Certificat

4.3.1 Actions de l'AC concernant la délivrance du Certificat

Après avoir authentifié l'origine et vérifié l'intégrité de la demande provenant de l'Autorité d'Enregistrement, l'AC déclenche le processus de génération du Certificat. Les conditions de génération des clés et des Certificats ainsi que les mesures de sécurité à respecter sont précisées aux chapitres 5 et 6 de la présente PC-DPC. Une fois généré, l'AC transmet le Certificat produit au Dispositif Porteur de Certificats via l'AE. Le Dispositif Porteur de Certificats garantit la sécurité des Bi-clés conformément à ce qui est défini au chapitre 6.1.1.4.

4.3.1.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Dans le cas de Certificats à usage unique, le Certificat produit est accessible au Titulaire dans la signature du ou des documents pour lesquels le Certificat a été émis.

4.3.1.2 [AC ORG] Certificats d'Organisation

Dans le cas de Certificats d'Organisation, le Certificat produit est également transmis au représentant de l'Abonné pour qu'il valide les informations contenues dans le Certificat avant de pouvoir l'utiliser (cf. chapitre 4.4.1.2).

4.3.2 Notification par l'AC de la délivrance du Certificat

L'AC transmet le Certificat produit au Dispositif Porteur de Certificats via l'AE en réponse du traitement de la demande de création de Certificat (cf. chapitre 4.3.1). L'opération est tracée dans les journaux de l'AE. Cette transmission vaut notification.

4.3.2.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Sans objet.

4.3.2.2 [AC ORG] Certificats d'Organisation

Dans le cas de délivrance de Certificats d'Organisation, le Certificat est également transmis au représentant de l'Abonné (cf. chapitre 4.3.1.2), ce qui vaut convention expresse notification.

4.4 Acceptation du Certificat

4.4.1 Démarche d'acceptation du Certificat

4.4.1.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Les données d'identification du Titulaire et le résultat de leur traitement pour former les données du Certificat sont validées explicitement par le Titulaire avant l'émission du Certificat. Cette validation est alors gardée dans le dossier d'enregistrement correspondant.

En effet, compte-tenu du caractère atomique sur le plan informatique de l'opération de signature dans le cadre de l'usage d'un Certificat à usage unique, la validation des données contenues au sein du Certificat se fait en amont de l'émission de celui-ci.

En complément de cette validation, des contrôles automatiques sont effectués par le Dispositif Porteur de Certificats afin de détecter une éventuelle non-conformité avant l'émission du Certificat.

4.4.1.2 [AC ORG] Certificats d'Organisation

Le Certificat d'Organisation produit par l'AC est transmis à l'Abonné pour validation avant usage conformément à ce qui est défini au chapitre 4.3.1 du présent document.

L'acceptation explicite des informations portées dans le Certificat soit du représentant légal ou statutaire de l'Abonné qui a fait la demande, soit de l'individu habilité identifié dans le Certificat est requise par la présente PC-DPC dans les dix (10) jours ouvrés consécutifs à la génération dudit Certificat (période appelée « phase d'acceptation »). L'acceptation explicite réalisée par e-mail, dont l'adresse est communiquée lors de la constitution du dossier d'abonnement, est considérée comme suffisante. En effet, l'adresse e-mail de l'émetteur qui a été enrôlé lors de la constitution du dossier d'abonnement est réputée tenir lieu d'authentification de la provenance de l'acceptation du Certificat.

Aucune utilisation de Certificat d'Organisation par le Dispositif Porteur de Certificat n'est possible sans cette phase d'acceptation.

Une fois cette phase d'acceptation arrivée à échéance, un Certificat d'Organisation émis est réputé accepté et est désormais utilisable par le Dispositif Porteur de Certificat.

4.4.2 Publication du Certificat

Il n'y a pas de service de publication des Certificats émis par les AC. Seul les Certificats des présentes AC sont publiés (cf. chapitre 2.2).

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

Sans objet.

4.5 Usages de la Bi-clé et du Certificat

4.5.1 Utilisation de la clé privée et du Certificat par le Dispositif Porteur de Certificats

L'utilisation de la clé privée par le Dispositif Porteur de Certificats et du Certificat associé est strictement limitée au service de signature/scellement électronique comme indiqué au chapitre 1.5.1.1 du présent document. Dans le cas contraire, la responsabilité du TSP MediaCert ne pourra être engagée.

L'usage autorisé de la Bi-clé et du Certificat associé est par ailleurs indiqué dans le Certificat à travers les extensions concernant les usages des clés.

4.5.2 Utilisation de la clé publique et du Certificat par les parties prenantes

Les Abonnés doivent respecter et faire respecter par les personnes qui leur sont liées et qui sollicitent des Certificats, l'usage stipulé au sein des Certificats produits à leur demande par les AC, comme expliqué au chapitre 4.5.1 ci-dessus. Ils doivent donc refuser toute autre utilisation de Certificat. Dans le cas contraire, la responsabilité des Abonnés et des personnes qui lui sont liées qui ont sollicité un Certificat pourra être engagée.

4.6 Renouvellement d'un Certificat

Le renouvellement de Certificat (nouveau Certificat sans changement de clé) n'est pas autorisé dans le cadre de la présente PC-DPC.

4.6.1 Causses 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 de l'établissement d'un 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

La délivrance d'un nouveau Certificat lié à la génération d'une nouvelle Bi-clé est traitée comme une demande initiale de création de Certificat.

Il est interdit d'utiliser une Bi-clé existante associée à une ancienne CSR.

4.7.1 Causses possibles de changement d'une Bi-clé

Sans objet.

4.7.2 Origine d'une demande d'un nouveau Certificat

Sans objet.

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

Sans objet.

4.7.4 Notification de l'établissement d'un nouveau Certificat

Sans objet.

4.7.5 Démarche d'acceptation du nouveau Certificat

Sans objet.

4.7.6 Publication du nouveau Certificat

Sans objet.

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

Sans objet.

4.8 Modification d'un Certificat

La modification de Certificat n'est pas autorisée par la présente PC-DPC.

[AC ORG] Cependant, la modification d'un Certificat d'Organisation revient à révoquer le Certificat en question puis à procéder à une nouvelle demande de Certificat selon la procédure décrite au chapitre 4.1.1.2.

4.8.1 Causses possibles de modification d'un Certificat

Sans objet.

4.8.2 Origine d'une demande de modification

Sans objet.

4.8.3 Procédure de traitement d'une demande de modification

Sans objet.

4.8.4 Démarche d'acceptation du Certificat modifié

Sans objet.

4.8.5 Publication du Certificat modifié

Sans objet.

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

Sans objet.

4.9 Révocation et suspension d'un Certificat

La présente PC-DPC n'autorise pas la suspension de Certificat.

Par ailleurs, toute information relative à la révocation du Certificat d'une AC est disponible au sein de la Politique de Certification – Déclaration des Pratiques de Certifications régissant son AC émettrice.

4.9.1 Causes possibles de révocation d'un Certificat

4.9.1.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Les circonstances suivantes peuvent être à l'origine de la révocation du Certificat à usage unique d'un Titulaire :

- le Certificat n'est plus conforme à la PC-DPC auquel il est sujet ;
- la cryptographie employée n'assure plus la liaison entre le sujet et la clé publique ;
- en cas de changement majeur, après étude de l'impact, ayant une incidence sur la validité du Certificat ;
- un incident est survenu lorsque le Dispositif Porteur de Certificats a utilisé le Certificat du Titulaire pour une signature dans le cadre de l'usage normal défini au chapitre 1.5.1.1 ;
- les clés privées ou publiques ne correspondent pas ou le Dispositif Porteur de Certificats est dans l'incapacité de s'en servir dans le cadre de l'usage normal défini au chapitre 1.5.1.1.

Lorsqu'une des circonstances susvisées survient et que l'Autorité de Certification en a la connaissance, le Certificat en question doit être révoqué sans délai. Toutefois, compte tenu de l'utilisation des Certificats à usage unique produits dans le cadre de la présente PC-DPC et de la courte durée de vie de ces Certificats, il est important de noter que la révocation est ici un instrument permettant avant tout de fournir une LCR pour des composants techniques qui ont obligation d'en disposer.

Pour cette catégorie de Certificats, la cause de révocation n'est pas publiée.

4.9.1.2 [AC ORG] Certificats d'Organisation

Les circonstances suivantes peuvent être à l'origine de la révocation du Certificat d'Organisation :

- le Certificat n'est plus conforme à la PC-DPC auquel il est sujet ;
- la cryptographie employée n'assure plus la liaison entre le sujet et la clé publique ;
- les informations de l'Organisation figurant dans le Certificat qui a été émis à son nom ne sont pas en conformité avec l'identité de l'Organisation ou avec l'usage prévu dans le Certificat ;
- une erreur (intentionnelle ou non) est détectée dans la demande d'enregistrement de l'Organisation ;
- le contrôle sur l'utilisation de la clé privée du porteur est suspecté perdu ou la clé privée du porteur est :
    - suspectée de compromission ;
    - compromise ;
    - perdue ;
    - volée ;
    - détruite ;
    - altérée.
- le représentant habilité (cf. chapitre 3.4.2) demande la révocation du Certificat ;
- cessation d'activité de l'Autorité de Certification, de l'Organisation ou de l'Abonné ;
- fin de la relation contractuelle entre l'Abonné et l'Autorité de Certification ;
- changement de réglementation technique ou juridique, ou changement de recommandation s'appliquant à l'Autorité de Certification ou à l'Organisation, nécessitant la fin de l'utilisation du Certificat.

Lorsqu'une des circonstances susvisées survient et que l'Autorité de Certification en a la connaissance, le Certificat en question doit être révoqué sans délai.

Par ailleurs, l'Autorité de Certification peut révoquer de plein droit un Certificat d'Organisation dans les circonstances suivantes :

- non-respect de la présente PC-DPC ;
- non-observation de l'une des obligations résultant du contrat d'abonné ou de tout autre document figurant au dossier d'abonnement (comme la présente PC-DPC et son chapitre 9.6) par un Titulaire ou par un Abonné, notamment concernant l'utilisation du Certificat dans des conditions autres que celles prévues dans ce présent document (cf. chapitre 1.5.1.1).

Pour cette catégorie de Certificat, la cause de révocation est publiée. Ceci constitue notamment un moyen d'identifier le type de Certificat dans la LCR.

4.9.2 Origine d'une demande de révocation

4.9.2.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Seul le Dispositif Porteur de Certificats est habilité à faire une demande de révocation de ce type de Certificat suite à la rencontre d'une des circonstances citées au chapitre 4.9.1.1 du présent document.

4.9.2.2 [AC ORG] Certificats d'Organisation

Les personnes et entités habilitées à faire une demande de révocation de ce type de Certificat, suite à la rencontre d'une des circonstances citées au chapitre 4.9.1.2 du présent document, sont :

- le représentant de l'Abonné ou un des représentants adjoint de l'Abonné qui dispose des données d'identification et d'authentification lui permettant d'accéder à cette fonction ;
- l'Autorité de Certification.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 [AC OTU][AC OTU LCP] Certificats à usage unique

La présente PC-DPC ne formule pas d'exigence sur l'identification de la demande de révocation. En effet, seul le Dispositif Porteur de Certificat tel que décrit au chapitre 1.3.3 est à même de demander une révocation sur la base d'une des causes possibles de révocation qu'il aura détectée (cf. chapitre 4.9.1.1).

La demande est donc automatiquement autorisée. L'AC procède ensuite à la révocation. L'opération est instantanée et est enregistrée dans les journaux d'évènement (cf. chapitre 5.4.1).

Une fois le Certificat révoqué, il ne peut être rétabli. Le sujet concerné est informé du changement de statut via la publication du Certificat révoqué dans une des Listes des Certificats Révoqués publiée à l'adresse définie au chapitre 2.2 du présent document.

4.9.3.2 [AC ORG] Certificats d'Organisation

La demande de révocation de ce type de Certificat n'est quant à elle pas automatiquement autorisée. En effet, la demande de la personne ou de l'entité habilitée (cf. chapitre 4.9.1.2) doit être validée par un personnel habilité Worldline (appelé « Pilote »). Pour cela, la personne ou l'entité habilité à faire la demande contacte un numéro d'appel qui lui a été fourni lors de la création du Certificat sujet à la révocation. Ce numéro est disponible 7j/7, 24h/24. Les informations à fournir au Pilote pour l'autorisation de la révocation sont :

- éléments d'identification : nom de l'Organisation et identité du représentant habilité ;
- élément d'authentification : code secret fourni lors de la création du Certificat.

Une fois ces éléments validés par le système, la demande de révocation est alors autorisée. L'opération est réalisée en plusieurs étapes par le Pilote. Certaines étapes nécessitent par ailleurs l'intervention du demandeur, par téléphone, qui doit donner les informations que le Pilote doit saisir ou vérifier afin que le demandeur garde le contrôle sur l'opération. L'opération est enregistrée dans les journaux d'évènement (cf. chapitre 5.4.1).

Une fois le Certificat révoqué, il ne peut être rétabli. Le sujet concerné est informé du changement de statut via une notification envoyé par l'AE et via la publication du Certificat révoqué dans une des Listes des Certificats Révoqués publiée à l'adresse définie au chapitre 2.2 du présent document.

Une demande de révocation de ce type de Certificat est suivie et tracée afin de pouvoir respecter le délai de révocation établi par l'AC (cf. chapitre 4.9.5.2).

L'AC peut toutefois procéder à la révocation d'un Certificat (cf. chapitre 4.9.2.2) si les évènements le lui imposent. La [DTPC] apporte plus d'informations sur ce sujet.

4.9.4 Délai accordé pour formuler la demande de révocation

4.9.4.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Compte-tenu du caractère atomique de l'opération sur le plan informatique de signature dans le cadre de l'usage d'un Certificat à usage unique, la demande effectuée par le demandeur (cf. chapitre 4.9.2.1) est immédiate lorsque l'une des causes citées au chapitre 4.9.1.1 est rencontrée.

4.9.4.2 [AC ORG] Certificats d'Organisation

Dès que le représentant habilité a connaissance d'une des causes possibles de révocation définies au chapitre 4.9.1.2 du présent document, 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 entre la réception de la demande de révocation et la prise en compte de cette demande est de vingt-quatre (24) heures, la fonction de gestion des révocations étant disponible 7j/7 24h/24.

4.9.5.1 [AC OTU][AC OTU LCP] Certificats à usage unique

La demande de révocation d'un Certificat à usage unique est traitée immédiatement après sa réception par l'AC. La révocation est effective lorsque le Certificat en question est introduit dans la LCR générée.

L'opération est immédiatement et automatiquement réalisée après réception et validation de la demande.

4.9.5.2 [AC ORG] Certificats d'Organisation

La demande de révocation d'un Certificat d'Organisation est traitée immédiatement après sa réception par l'AC. La révocation est effective lorsque le Certificat en question est introduit dans la LCR générée.

Une demande de révocation d'un Certificat d'Organisation étant défini par son numéro suivi et par sa date de révocation, son suivi et sa traçabilité sont clairement définis et réalisables. Cela permet donc de contrôler le respect ou non-respect du délai de révocation.

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

4.9.6.1 [AC OTU][AC OTU LCP] Certificats à usage unique

Dans le cadre d'utilisation d'un Certificat à usage unique fourni par une AC en ligne, la présente PC-DPC ne formule, compte tenu du caractère atomique sur le plan informatique de l'opération de signature, aucune exigence concernant l'obligation de vérification de la révocation du Certificat.

4.9.6.2 [AC ORG] Certificats d'Organisation

Dans le cadre d'utilisation d'un Certificat d'Organisation fourni par l'AC, l'utilisateur se doit de vérifier le statut du Certificat auquel il compte se fier avant de l'utiliser. Pour cela, il peut soit consulter les LCR publiées, soit effectuer une requête auprès du répondeur OCSP (cf. chapitre 4.10).

En plus du statut, l'utilisateur se doit de vérifier la validité du Certificat en question et de la Chaîne de Certification correspondante.

4.9.7 Fréquence d'établissement des LCR

La fréquence d'établissement des LCR est de vingt-quatre (24) heures. Cependant, une nouvelle LCR peut être publiée à tout moment, à la suite d'une révocation par exemple. Elles ont une durée de validité de sept (7) jours.

4.9.8 Délai maximum de publication d'une LCR

Une LCR est publiée dans un délai maximum de soixante (60) minutes suivant sa génération.

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

Un répondeur OCSP est rendu disponible en ligne et est accessible comme décrit au chapitre 2.2, permettant ainsi à l'utilisateur de vérifier en ligne la révocation et l'état des Certificats (cf. chapitre 4.10).

L'information de révocation mise à disposition est cohérente entre les différents services d'information sur les révocations (LCR et répondeur OCSP).

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

Les exigences de vérification en ligne de la révocation des Certificats par les utilisateurs sont conformes à ce qui est détaillé au chapitre 4.9.6 de la présente PC-DPC.

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

Les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée (cf. chapitre 4.9.4).

Concernant les Certificats des AC, la révocation suite à une compromission de la clé privée fera l'objet d'une notification à l'organisme de contrôle [Notification ANSSI] dans les vingt-quatre (24) heures conformément aux exigences de [eIDAS].

4.9.13 Causes possibles d'une suspension

Dans le cadre de la présente PC-DPC, la suspension de Certificats n'est pas autorisée.

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 Fonctions d'information sur l'état des Certificats

4.10.1 Caractéristiques opérationnelles

Les AC mettent à disposition des utilisateurs deux mécanismes de consultation publique de l'état de Certificats : les LCR et le répondeur OCSP.
Les LCR sont publiées au format v2 sur un internet, accessibles en protocole HTTP(s) à l'adresse :

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

Une LCR contient la liste des Certificats émis par une des AC en ligne qui sont à la fois révoqués et non expirés (date et heure de fin de validité du Certificat non atteinte). En effet, un Certificat révoqué et expiré ne figure plus dans la LCR. Elle contient notamment la date de sa publication ainsi que la date de la prochaine publication.
Les LCR sont par ailleurs signées par l'AC cible afin d'en assurer l'origine et l'intégrité.
Le lien vers le répondeur OCSP est précisé sur internet, accessible en protocole HTTP(s) à l'adresse :

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

Les AC assurent l'origine et l'intégrité des réponses fournies par le répondeur OCSP qu'elle met à disposition des utilisateurs.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des Certificats est disponible 7j/7 24h24. L'indisponibilité maximum de la plateforme est de huit (8) heures par mois.

4.10.3 Dispositifs optionnels

Sans objet.

4.11 Fin de la relation entre l'Abonné et l'AC

La fin de la relation entre l'Abonné et le TSP MediaCert dans le cadre des services présentés au chapitre 1.5.1.1 se matérialise par la résiliation ou le non-renouvellement du Contrat d'Abonnement ou des contrats de prestations qui lui sont expressément liés.

L'Autorité d'Enregistrement ne reconnait plus les demandes transmises et signées par l'Abonné, son représentant ou encore les adjoints de son représentant.

Il est demandé alors à l'Abonné de procéder à une ou à des demandes (compte tenu du nombre de Certificats concernés) de révocation sans délai de son ou de ses Certificats d'Organisation s'ils sont toujours valides.

4.12 Séquestre de clé et recouvrement

Le séquestre des clés privées des AC et des Certificats porteurs est interdit par la présente PC-DPC.

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

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 Procédures de constitution des données d'audit

5.4.1 Type d'évènements enregistrés

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 accès physiques aux locaux hébergeant les systèmes ;
    - les changements de politique de sécurité des systèmes ;
    - changements dans le personnel intervenant pour le compte des AC ;
    - les démarrages et arrêts des systèmes ;
    - les démarrages et arrêts des paramètres de la fonction de journalisation ;
    - les pannes matérielles et logicielles ;
    - modifications (changement, correction ou évolution) des différents composants ;
    - les tentatives d'accès aux systèmes ;
    - les connexions et déconnexions aux systèmes des utilisateurs autorisés.
- 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 aux 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, les AC conservent également :

- l'identité de la personne 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.

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'évènements

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

5.4.3 Période de conservation des journaux d'évènements

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'évènements

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'évènements

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

5.4.6 Système de collecte des journaux d'évènements

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

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

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

5.4.8 Evaluation 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 des IGC.

5.5 Archivage des données

Des dispositions en matière d'archivage sont mises en place par le TSP MediaCert. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes des 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)
3 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 ; Remarque : spécificité pour les dossiers d'enregistrement liés aux Certificats à usage unique, la durée de conservation de l'archive est de huit (8) ans, ceci en raison du caractère spécial de la durée de vie de cette gamme de Certificats. • 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)

Toutefois, la durée de conservation des dossiers d'enregistrements peut être modifiée à la demande de l'Abonné qui peut requérir auprès de Worldline, de convention expresse dans le cadre de conditions particulières au Contrat d'Abonnement, une prolongation au-delà de la durée définie ci-dessus. Cette prolongation doit être justifiée par des contraintes réglementaires ou légales et assortie d'une obligation d'information à la charge de l'Abonné des personnes concernées par le traitement des données personnelles contenues dans le dossier d'enregistrement.

5.5.3 Protection des archives

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

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

- 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

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

5.5.5 Exigences d'horodatage des données

Le chapitre 6.8 du présent document précise les exigences en matière de datation, d'horodatage.

5.5.6 Système de collecte des archives

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

5.5.7 Procédure de récupération et de vérification des archives

La procédure de récupération des archives des AC est interne et est spécifiée dans la [DTPC]. L'accès aux archives est sujet à des restrictions.

Les archives seront rendues disponibles en cas de réquisition judiciaire.

5.6 Changement de Bi-clé d'AC

Les AC ne peuvent 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 expirés.

5.7 Reprise suite à 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 d'une 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 des IGC découlant de la présente PC-DPC, des engagements des AC en ligne dans la présente PC-DPC notamment en ce qui concerne les fonctions liées à la publication et/ou la révocation des certificats. Ce plan est régulièrement testé.

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 et de reprise d'activité de la composante (cf. chapitre 5.7.4) en tant que sinistre.

Dans le cas d'une compromission de la clé privée d'AC, 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.

5.7.4 Capacités de continuité suite à un sinistre

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

5.8 Fin de vie de l'IGC

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'IGC, 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'IGC 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'IGC. Ce plan est régulièrement tenu à jour et comporte notamment les actions citées ci-dessous.

L'IGC 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'IGC 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 tous les Certificats qu'elle a signés et qui seraient encore en cours de validité ;
- révoquer son Certificat ;
- 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 des Bi-clés

6.1.1 Génération des Bi-clés

6.1.1.1 Bi-clés d'AC

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

Les clés de signature des AC en ligne sont générées et mises en œuvre dans un module cryptographique ayant fait l'objet d'une évaluation sécuritaire comme défini au chapitre 6.2.11.1 du présent document.
Ces clés de signatures possèdent un identifiant unique qui est nécessairement spécifié lors de la configuration des applicatifs afin de ne pas compromettre leur utilisation.

6.1.1.2 Bi-clés d'authentification d'une composante de l'IGC

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

6.1.1.3 Bi-clés d'authentification de l'Abonné

L'authentification de l'Abonné est décrite au chapitre 3.2.5 de la présente PC-DPC.

Les AC en ligne ne produisent pas les Certificats d'authentification attachés à la clé privée d'un Abonné et n'est pas responsable de la délivrance de ces Certificats. En effet, l'Abonné est informé des règles à respecter pour s'authentifier auprès de l'Autorité d'Enregistrement (cf. chapitre 3.2.5) et il lui appartient d'obtenir le ou les Certificat(s) lui permettant de s'authentifier auprès de l'AE.

6.1.1.4 Bi-clés des Certificats porteurs générées par l'AC

Les Autorité de Certification en ligne ne génèrent pas les clés des Certificats porteurs.

6.1.1.5 Bi-clés des Certificats porteur générées pour la Partie Prenante

Les Bi-clés sont générées par le Dispositif Porteur de Certificats, qui en conserve l'usage exclusif, dans les conditions suivantes :

Certificat à usage unique	Certificat d'Organisation
Au sein d'un module cryptographique physiquement isolé répondant aux exigences définies au chapitre 6.2.11.2 du présent document	
Copiées sur les autres modules cryptographiques dédiés et prévus pour le même usage, répondants aux mêmes exigences susvisées, selon les processus de clonage préconisés par le fournisseur	
Dans les locaux sécurisés du TSP MediaCert (cf. chapitre 5.1)	

Certificat à usage unique	Certificat d'Organisation
Sous le contrôle du Dispositif Porteur de Certificat	Sous le contrôle de deux (2) personnes occupant un rôle de confiance au sein du TSP MediaCert
Suivant un script préalablement défini par le TSP MediaCert	Suivant un document Organisationnel et un document technique tous deux signés par l'ensemble des participants, notamment par le maître de cérémonie

Des moyens de contrôle et de protection sont mis en œuvre par le TSP MediaCert au niveau du Dispositif Porteur de Certificats pour protéger l'usage des clés privées.

Il est par ailleurs interdit par la présente PC-DPC d'utiliser une Bi-clé existante associée à une ancienne CSR (cf. chapitre 4.7).

6.1.2 Transmission de la clé privée au bénéficiaire

Sans objet.

6.1.3 Transmission de la clé publique à l'AC

La clé publique est transmise par le Dispositif Porteur de Certificat à l'Autorité d'Enregistrement qui la transmet à l'AC cible au sein d'un gabarit au format PKCS#10 (CSR) pour la génération du Certificat à usage unique / d'Organisation.

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

Les Certificats contenant les clés publiques des AC sont publiés sur son site web dont l'adresse est définie au chapitre 2.2 du présent document.

6.1.5 Taille des Bi-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.

Bi-clés	Algorithme	Fonction de hachage	Taille (bits)
Certificats de l'AC OTU	RSA	SHA-2	4096
Certificats de l'AC OTU LCP	RSA	SHA-2	4096
Certificats de l'AC ORG	RSA	SHA-2	4096
Certificats à usage unique « standards »	RSA	SHA-2	2048
Certificats à usage unique « renforcés »	RSA	SHA-2	2048
Certificats d'Organisation	RSA	SHA-2	2048

Bi-clés	Algorithme	Fonction de hachage	Taille (bits)
Certificats à usage unique de test « standards »	RSA	SHA-2	2048
Certificats à usage unique de test « renforcés »	RSA	SHA-2	2048
Certificats d'Organisation de test	RSA	SHA-2	2048

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

Les équipements de génération de Bi-clés utilisés pour la génération des paramètres des Bi-clés des AC sont des modules cryptographiques configurés pour répondre à ces exigences (cf. chapitre 6.1.1.1). Les Bi-clés ne peuvent être générées que sur un module conforme à cette exigence, ou d'un niveau cryptographique et sécuritaire supérieur.

Il en est de même pour les Bi-clés porteurs (cf. chapitre 6.1.1.5).

6.1.7 Objectifs d'usage de la clé

Les usages des clés sont des clés sont définis au chapitre 1.5 et plus particulièrement au sein des Certificats conformément à l'extension « *Key Usage* » (cf. chapitre 7.1).

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 Modules cryptographiques de l'AC

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

Les clés de signature des AC sont générées et mises en œuvre dans un module cryptographique ayant fait l'objet d'une évaluation sécuritaire comme défini au chapitre 6.2.11.1 du présent document.
Toutefois, les clés de signatures de ces AC sont opérées dans des composants logiciels distincts afin de garantir un contrôle lors de leur utilisation.

6.2.1.2 Dispositifs cryptographiques des bénéficiaires

Sans objet.

6.2.2 Contrôle de la clé privée

6.2.2.1 Clés privées d'AC

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

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

6.2.2.2 Clés privées des Certificats porteurs

Le contrôle des clés privées correspondantes aux différents Certificats délivrés par les AC est assuré par le Dispositif Porteur de Certificats qui en a le contrôle exclusif. Toutefois, ce contrôle exclusif reste sujet à l'activation décrite au chapitre 6.4.1.2 du présent document.

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

6.2.6.1 Clés privées d'AC

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.

6.2.6.2 Clés privées des Certificats porteurs

Sans objet.

6.2.7 Stockage de la clé privée dans un module cryptographique

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

6.2.8 Méthode de d'activation de la clé privée

6.2.8.1 Clés privées d'AC

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

6.2.8.2 Clés privées des Certificats porteurs

[AC OTU][AC OTU LCP] Certificats à usage unique

Les clefs privées des Certificats à usage unique sont activées par le Dispositif Porteur de Certificats auprès d'un des modules cryptographique prévu pour cet usage, après réception du certificat à usage unique émis par l'AC cible lors de la session de signature.

[AC ORG] Certificats d'Organisation

Les clefs privées des Certificats Organisation sont activées par le Dispositif Porteur de Certificats auprès d'un des modules cryptographique prévu pour cet usage, après réception d'une demande dûment validée et authentifiée.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

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

6.2.9.2 Clés privées des Certificats porteurs

[AC OTU][AC OTU LCP] Certificats à usage unique

La clé privée d'un Certificat à usage unique est détruite après son utilisation.

[AC ORG] Certificats d'Organisation

La désactivation de la clé privée d'un Certificat d'Organisation dans le module cryptographique est automatique dès la fin de la session de l'opération de scellement ou dès qu'il y a arrêt ou déconnexion du module.

6.2.10 Méthode de destruction de la clé privée

6.2.10.1 Clés privées d'AC

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

Par ailleurs, 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 si applicable.

6.2.10.2 Clés privées des Certificats porteurs

[AC OTU][AC OTU LCP] Certificats à usage unique

Les clés privées des Certificats à usage unique sont détruites après leur utilisation par le Dispositif Porteur de Certificats qui trace alors l'évènement.

[AC ORG] Certificats d'Organisation

Sans objet.

6.2.11 Niveau de qualification du module cryptographique

6.2.11.1 Modules cryptographique associés aux Certificats d'AC

Le module cryptographique matériel utilisé pour héberger les clés privées des AC est évalué au niveau de Certification suivant : Critères Communs EAL4+.

6.2.11.2 Modules cryptographique associés aux Certificats porteurs

Le module cryptographique matériel utilisé pour héberger les clés privées des Certificats porteurs générés par les AC est évalué au niveau de Certification suivant : FIPS 140-2 level 3.

6.3 Autres aspects de la gestion des Bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques des AC sont archivées conformément au chapitre 5.5.2 du présent document.

6.3.2 Durée de vie des Bi-clés et des Certificats

La durée de vie des Bi-clés et des Certificats diffère selon le type de Certificat. La taille des Bi-clés a été prise en compte lors de la définition de ces durées de vie, conformément aux exigences cryptographique [ETSI TS 119 312].

Les AC ne peuvent émettre des Certificats porteurs dont la durée de vie excéderait celle du Certificat de l'AC utilisé pour l'émission.

Bi-clés	Durée de vie
Certificats de l'AC OTU	10 ans
Certificats de l'AC OTU LCP	10 ans
Certificats de l'AC ORG	10 ans
Certificats à usage unique « standards »	15 minutes
Certificats à usage unique « renforcés »	15 minutes
Certificats d'Organisation	3 ans
Certificats à usage unique de test « standards »	15 minutes
Certificats à usage unique de test « renforcés »	15 minutes
Certificats d'Organisation de test	3 ans

6.3.3 Inventaire des Bi-clés

6.3.3.1 Bi-clés et Certificats d'AC

Le TSP MediaCert tiens un inventaire des secrets et Bi-clés régulièrement mis à jour.

6.3.3.2 Bi-clés et Certificats porteur

Un inventaire est réalisé de manière à vérifier que toutes les clés privées produites par les AC à destination du Dispositif Porteur de Certificat ont bien fait l'objet d'une demande correcte.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

6.4.1.1 Génération et installation des données d'activation correspondant à la clé privée d'une AC

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

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée d'un Certificat porteur

Il n'y a pas à proprement parler de données d'activation correspondant à la clé privée d'un Certificat porteur. Toutefois, le Dispositif Porteur de Certificat ne peut utiliser la clé privée d'un Certificat porteur sans avoir reçu une requête de l'Abonné.

6.4.2 Protection des données d'activation

6.4.2.1 Protection des données d'activation correspondant à la clé privée d'une AC

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

6.4.2.2 Protection des données d'activation correspondant à la clé privée d'un Certificat porteur

Une protection du mécanisme d'authentification du Dispositif Porteur de Certificats pour l'activation et l'utilisation des clés privées est mise en place.

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.

6.5.2 Niveau de qualification des systèmes informatiques

Sans objet.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

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 Mesures liées à la gestion de la sécurité

Toute évolution d'un système d'une composante des IGC est documentée et tracée. Elle apparaît dans les procédures de fonctionnement interne de la composante.

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

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

6.7 Mesures de sécurité réseau

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

6.8 Horodatage / Système de datation

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

Par ailleurs, les serveurs du TSP MediaCert synchronisent leur horloge interne toutes les 24h au plus sur des serveurs de référence afin de garantir la cohérence de l'heure (UTC) indiquée dans les différents journaux électroniques.

7 Profil des Certificats et LCR

7.1 Profils des certificats

7.1.1 Définitions

Les Certificats émis par les AC en ligne, y compris les leurs, sont conformes aux standards X.509.

Champs	Description
Version	Version du Certificat X.509
Serial number	Numéro de série unique du Certificat
Signature	OID de l'algorithme utilisé par l'AC émettrice pour signer le Certificat émis
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) du sujet
Subject Public Key Info	OID de l'algorithme et valeur de la clé publique
Extensions	Liste des extensions. Une extension peut être critique ou non-critique : • si elle est critique, l'application utilisatrice à qui le Certificat est présenté doit savoir la traiter conformément à son usage. Si l'application ne sait pas traiter l'extension ou si l'extension n'est pas conforme à l'usage attendu par celle-ci, elle doit rejeter le Certificat ; • si elle est non-critique, il n'y a pas de rejet de Certificat et l'application peut ignorer l'extension en question.

7.1.2 Certificat de l'AC OTU

Les Certificats de l'AC OTU, appelés Certificats d'AC Technique (ACT), sont différenciés par le champ *Serial Number* (SERIALNUMBER) du *Distinguished Name* (DN) du *Subject*.

Champs du DN	Obligatoire	Description
C	Oui	Pays de l'Organisation régissant l'AC : FR
O	Oui	Nom légal de l'Organisation régissant l'AC : Worldline
OU	Oui	Identifiant de l'Organisation régissant l'AC : 0002 378901946
SERIALNUMBER	Oui	Numéro de série unique du DN [1]
CN	Oui	Identité du titulaire : MediaCert OTU CA 2019

7.1.2.1 Champs de base

Champs	Valeur
Version	2 (pour version 3)
Serial number	Généré automatiquement lors de la Cérémonie de Clé
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	DN de l'AC émettrice (cf. chapitre 1.2.2)
Validity	10 ans
Subject	DN de l'AC Technique (cf. chapitre 7.1.2)
Subject Public Key Info	RSA 4096 bits

7.1.2.2 Extensions

Champs	Critique	Valeur
Authority Key Identifier	Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier	Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage	Oui	keyCertSign, CRLSign
Certificate Policies	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	Non	• CA : vrai • Maximum Path Length : 0
CRL Distribution Points	Non	• fullName : http://www.mediacert.com/trustCA2019/trustCA2019.crl [2]

[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 ;
- …

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

Champs	Critique	Valeur
		• reason : Absent • cRLIssuer : Absent
Authority Information Access	Non	• accessMethod : id-ad-caIssuers • accessLocation: http://www.mediacert.com/trustCA2019/trustCA2019.crt [2]

7.1.3 Certificat de l'AC OTU LCP

Les Certificats de l'AC OTU LCP, appelés Certificats d'AC Technique (ACT), sont différenciés par le champ *Serial Number* (SERIALNUMBER) du *Distinguished Name* (DN) du *Subject*.

Champs du DN	Obligatoire	Description
C	Oui	Pays de l'Organisation régissant l'AC : FR
O	Oui	Nom légal de l'Organisation régissant l'AC : Worldline
OU	Oui	Identifiant de l'Organisation régissant l'AC : 0002 378901946
SERIALNUMBER	Oui	Numéro de série unique du DN [3]
CN	Oui	Identité du titulaire : MediaCert OTU LCP CA 2018

7.1.3.1 Champs de base

Champs	Valeur
Version	2 (pour version 3)
Serial number	Généré automatiquement lors de la Cérémonie de Clé
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	DN de l'AC émettrice (cf. chapitre 1.2.2)
Validity	10 ans
Subject	DN de l'AC Technique (cf. chapitre 0)
Subject Public Key Info	RSA 4096 bits

7.1.3.2 Extensions

Champs	Critique	Valeur
Authority Key Identifier	Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier	Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage	Oui	keyCertSign, CRLSign
Certificate Policies	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	Non	• CA : vrai • Maximum Path Length : 0
CRL Distribution Points	Non	• fullName : http://www.mediacert.com/rootCA2018/rootCA2018.crl [4] • reason : Absent

[3] 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 ;
- …

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

Champs	Critique	Valeur
		• cRLIssuer : Absent
Authority Information Access	Non	• accessMethod : id-ad-caIssuers • accessLocation: http://www.mediacert.com/rootCA2018/rootCA2018.crt [4]

7.1.4 Certificat de l'AC ORG

Les Certificats de l'AC ORG, appelés Certificats d'AC Technique (ACT), sont différenciés par le champ *Serial Number* (SERIALNUMBER) du *Distinguished Name* (DN) du *Subject*.

Champs du DN	Obligatoire	Description
C	Oui	Pays de l'Organisation régissant l'AC : FR
O	Oui	Nom légal de l'Organisation régissant l'AC : Worldline
OU	Oui	Identifiant de l'Organisation régissant l'AC : 0002 378901946
SERIALNUMBER	Oui	Numéro de série unique du DN [5]
CN	Oui	Identité du titulaire : MediaCert ORG CA 2018

7.1.4.1 Champs de base

Champs	Valeur
Version	2 (pour version 3)
Serial number	Généré automatiquement lors de la Cérémonie de Clé
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	DN de l'AC émettrice (cf. chapitre 1.2.2)
Validity	10 ans
Subject	DN de l'AC Technique (cf. chapitre 0)
Subject Public Key Info	RSA 4096 bits

7.1.4.2 Extensions

Champs	Critique	Valeur
Authority Key Identifier	Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier	Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage	Oui	keyCertSign, CRLSign
Certificate Policies	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	Non	• CA : vrai • Maximum Path Length : 0
CRL Distribution Points	Non	• fullName : http://www.mediacert.com/trustCA2019/trustCA2019.crl [6]

[5] 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 ;
- …

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

Champs	Critique	Valeur
		• reason : Absent • cRLIssuer : Absent
Authority Information Access	Non	• accessMethod : id-ad-caIssuers • accessLocation: http://www.mediacert.com/trustCA2019/trustCA2019.crt [6]

7.1.5 Certificat à usage unique « standard »

7.1.5.1 Champs de base

Champs		Valeur
Version		2 (pour version 3)
Serial number		Défini par l'AC Technique émettrice
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de l'AC Technique émettrice
Validity		15 minutes
Subject	C	Nationalité du Titulaire
	SN	Nom du Titulaire
	GN	Prénom du Titulaire
	OU	Nom de l'Abonné
	SERIALNUMBER [7]	Numéro de série unique du DN
	CN	Identité du titulaire formée de telle manière : Prénom du Titulaire [espace] Nom du Titulaire [espace] [TraceID] [8]
Subject Public Key Info		RSA 2048 bits

7.1.5.2 Extensions

Champs		Critique	Valeur
Authority Key Identifier		Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier		Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage		Oui	nonRepudiation
Basic Constraint	Certificate Authority	Non	Faux
Certificate Policies	policyIdentifier	Non	1.2.250.1.111.20.5.3.5
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
CRL Distribution Points		Non	http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [9]
Authority Information Access	ocsp	Non	http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [9]
	caIssuers		http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [9]

[7] Conformément à la [RFC 3739], le champ SERIALNUMBER permet de lever le risque d'homonymie dans le reste des champs du DN. Il est construit comme suit :

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime :* représente l'heure de demande du Certificat ;
- *DocRef :* représente l'identification du document à signer (en cas de multi-signature, c'est le premier document qui est référencé dans la requête de signature qui apparait) ;
- *ClientId :* représente l'identification unique du client.

La valeur *ReqTime* permet de se prémunir d'un cas de co-signatures par deux (2) personnes portant le même nom. La concaténation des trois (3) informations garantit une valeur unique parmi tous les utilisateurs.

[8] Représente l'identification unique du container de trace pour la signature.

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

7.1.6 Certificat à usage unique « renforcé »

7.1.6.1 Champs de base

Champs		Valeur
Version		2 (pour version 3)
Serial number		Défini par l'AC Technique émettrice
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de l'AC Technique émettrice
Validity		15 minutes
Subject	C	Nationalité du Titulaire
	SN	Nom du Titulaire
	GN	Prénom du Titulaire
	OU	Nom de l'Abonné
	SERIALNUMBER [10]	Numéro de série unique du DN
	CN	Identité du titulaire formée de telle manière : Prénom du Titulaire [espace] Nom du Titulaire [espace] [TraceID] [11]
Subject Public Key Info		RSA 2048 bits

7.1.6.2 Extensions

Champs		Critique	Valeur
Authority Key Identifier		Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier		Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage		Oui	nonRepudiation
Basic Constraint	Certificate Authority	Non	Faux
Certificate Policies	policyIdentifier	Non	1.2.250.1.111.20.5.3.1
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
CRL Distribution Points		Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [12]
Authority Information Access	ocsp	Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [12]
	caIssuers		http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [12]

[10] Conformément à la [RFC 3739], le champ SERIALNUMBER permet de lever le risque d'homonymie dans le reste des champs du DN. Il est construit comme suit :

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime :* représente l'heure de demande du Certificat ;
- *DocRef :* représente l'identification du document à signer (en cas de multi-signature, c'est le premier document qui est référencé dans la requête de signature qui apparait) ;
- *ClientId :* représente l'identification unique du client.

La valeur *ReqTime* permet de se prémunir d'un cas de co-signatures par deux (2) personnes portant le même nom. La concaténation des trois (3) informations garantit une valeur unique parmi tous les utilisateurs.

[11] Représente l'identification unique du container de trace pour la signature.

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

7.1.7 Certificat d'Organisation

7.1.7.1 Champs de base

Champs		Valeur
Version		2 (pour version 3)
Serial number		Défini par l'AC Technique émettrice
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de l'ACT émettrice
Validity		3 ans
Subject	C	Pays de l'Organisation
	OI [13]	Identifiant de l'Organisation formé de telle manière : ICD [espace] Identifiant de l'Organisation
	SN [14]	Nom de l'individu habilité dans l'Organisation
	GN [12]	Prénom de l'individu habilité dans l'Organisation
	OU [12]	Nom de l'unité dans l'Organisation
	O	Nom de l'Abonné
	SERIALNUMBER [15]	Numéro de série unique du DN
	CN	Identité de l'Organisation
Subject Public Key Info		RSA 2048 bits

7.1.7.2 Extensions

Champs		Critique	Valeur
Authority Key Identifier		Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier		Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage		Oui	nonRepudiation
Basic Constraint	Certificate Authority	Non	Faux
Certificate Policies	policyIdentifier	Non	1.2.250.1.111.20.5.3.2
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		Non	[RFC 822] : e-mail du titulaire du Certificat
CRL Distribution Points		Non	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [16]
Authority	ocsp	Non	http://pki-org-ac[SERIALNUMBER ACT

[13] L'ICD (*International Code Designator*) est sur un code unique de 4 caractères et l'identifiant de l'Organisation est sur 35 caractères maximum.
Pour les Organisations de droit français, l'ICD est 0002 et l'identifiant de l'Organisation accepté est le n°SIREN.
[14] Au moins l'une des deux informations doit être présente dans le DN : nom de l'unité dans l'Organisation ou nom et prénom de l'individu habilité à représenter l'Organisation.
[15] Conformément à la [RFC 3739], le champ SERIALNUMBER permet de lever le risque d'homonymie dans le reste des champs du DN. Il est construit comme suit :

SERIALNUMBER = *CreationDate*

- *CreationDate :* représente la date et l'heure (arbitraire) au moment du retrait du Certificat : au format *aaaammjjhhmmss.*

La valeur *CreationDate* permet de se prémunir d'un cas de co-signatures par deux (2) personnes portant le même nom. La concaténation des deux (2) informations garantit une valeur unique parmi tous les utilisateurs.
[16] Cette URL est donnée à titre indicatif. L'URL qui fait foi est celle qui figure dans le Certificat.

Champs		Critique	Valeur
Information Access			émettrice].mediacert.com/ocsp [16]
	caIssuers		http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [16]

7.1.8 Certificat à usage unique de test « standard »

7.1.8.1 Champs de base

Champs		Valeur
Version		2 (pour version 3)
Serial number		Défini par l'AC Technique émettrice
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de l'ACT émettrice
Validity		15 minutes
Subject	C	Nationalité du Titulaire
	SN	Nom du Titulaire
	GN	Prénom du Titulaire
	OU	Nom de l'Abonné
	SERIALNUMBER [17]	Numéro de série unique du DN
	CN	Identité du titulaire de test formé de telle manière : TEST [espace] Prénom du Titulaire [espace] Nom du Titulaire [espace] [TraceID] [18]
Subject Public Key Info		RSA 2048 bits

7.1.8.2 Extensions

Champs		Critique	Valeur
Authority Key Identifier		Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier		Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage		Oui	nonRepudiation
Basic Constraint	Certificate Authority	Non	Faux
Certificate Policies	policyIdentifier	Non	1.2.250.1.111.20.5.3.6
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
CRL Distribution Points		Non	http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [19]
Authority Information Access	ocsp	Non	http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [19]
	caIssuers		https://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [19]

[17] Conformément à la [RFC 3739], le champ SERIALNUMBER permet de lever le risque d'homonymie dans le reste des champs du DN. Il est construit comme suit :

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime :* représente l'heure de demande du Certificat ;
- *DocRef :* représente l'identification du document à signer (en cas de multi-signature, c'est le premier document qui est référencé dans la requête de signature qui apparait) ;
- *ClientId :* représente l'identification unique du client.

La valeur *ReqTime* permet de se prémunir d'un cas de co-signatures par deux (2) personnes portant le même nom. La concaténation des trois (3) informations garantit une valeur unique parmi tous les utilisateurs.

[18] Représente l'identification unique du container de trace pour la signature.

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

7.1.9 Certificat à usage unique de test « renforcé »

7.1.9.1 Champs de base

Champs		Valeur
Version		2 (pour version 3)
Serial number		Défini par l'AC Technique émettrice
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de l'ACT émettrice
Validity		15 minutes
Subject	C	Nationalité du Titulaire
	SN	Nom du Titulaire
	GN	Prénom du Titulaire
	OU	Nom de l'Abonné
	SERIALNUMBER [20]	Numéro de série unique du DN
	CN	Identité du titulaire de test formé de telle manière : TEST [espace] Prénom du Titulaire [espace] Nom du Titulaire [espace] [TraceID] [21]
Subject Public Key Info		RSA 2048 bits

7.1.9.2 Extensions

Champs		Critique	Valeur
Authority Key Identifier		Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier		Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage		Oui	nonRepudiation
Basic Constraint	Certificate Authority	Non	Faux
Certificate Policies	policyIdentifier	Non	1.2.250.1.111.20.5.3.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
CRL Distribution Points		Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [22]
Authority Information Access	ocsp	Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [22]
	caIssuers		https://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [22]

[20] Conformément à la [RFC 3739], le champ SERIALNUMBER permet de lever le risque d'homonymie dans le reste des champs du DN. Il est construit comme suit :

SERIALNUMBER = *ReqTime:DocRef:ClientId*

- *ReqTime :* représente l'heure de demande du Certificat ;
- *DocRef :* représente l'identification du document à signer (en cas de multi-signature, c'est le premier document qui est référencé dans la requête de signature qui apparait) ;
- *ClientId :* représente l'identification unique du client.

La valeur *ReqTime* permet de se prémunir d'un cas de co-signatures par deux (2) personnes portant le même nom. La concaténation des trois (3) informations garantit une valeur unique parmi tous les utilisateurs.

[21] Représente l'identification unique du container de trace pour la signature.

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

7.1.10 Certificat d'Organisation de test

7.1.10.1 Champs de base

Champs		Valeur
Version		2 (pour version 3)
Serial number		Défini par l'AC Technique émettrice
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de l'ACT émettrice
Validity		3 ans
Subject	C	Pays de l'Organisation
	OI [23]	Identifiant de l'Organisation formé de telle manière : ICD [espace] Identifiant de l'Organisation
	SN [24]	Nom de l'individu habilité dans l'Organisation
	GN [22]	Prénom de l'individu habilité dans l'Organisation
	OU [22]	Nom de l'unité dans l'Organisation
	O	Identité de l'Abonné
	SERIALNUMBER [25]	Numéro de série unique du DN
	CN	TEST Identité de l'Organisation [26]
Subject Public Key Info		RSA 2048 bits

7.1.10.2 Extensions

Champs		Critique	Valeur
Authority Key Identifier		Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier		Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage		Oui	nonRepudiation
Basic Constraint	Certificate Authority	Non	Faux
Certificate Policies	policyIdentifier	Non	1.2.250.1.111.20.5.3.4
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		Non	[RFC 822] : e-mail du titulaire du Certificat
CRL Distribution Points		Non	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [27]
Authority Information	ocsp	Non	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [27]

[23] L'ICD (*International Code Designator*) est sur un code unique de 4 caractères et l'identifiant de l'Organisation est sur 35 caractères maximum.
Pour les Organisations de droit français, l'ICD est 0002 et l'identifiant de l'Organisation accepté est le n° SIREN.

[24] Au moins l'une des deux informations doit être présente dans le DN : nom de l'unité dans l'Organisation ou nom et prénom de l'individu habilité à représenter l'Organisation.

[25] Conformément à la [RFC 3739], le champ SERIALNUMBER permet de lever le risque d'homonymie dans le reste des champs du DN. Il est construit comme suit :

SERIALNUMBER = *CreationDate*

- *CreationDate :* représente la date et l'heure (arbitraire) au moment du retrait du Certificat : au format *aaaammjjhhmmss.*

La valeur *CreationDate* permet de se prémunir d'un cas de co-signatures par deux (2) personnes portant le même nom. La concaténation des deux (2) informations garantit une valeur unique parmi tous les utilisateurs.

[26] Le mot « TEST » et l'identité de l'Organisation ne sont pas séparés par un espace.

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

Champs		Critique	Valeur
Access	caIssuers		http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [27]

7.2 Profil des LCR

7.2.1 Champ de base

Champs		Valeur
Version		1 (pour version 2)
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de l'ACT émettrice
This Update		Date d'émission de la LCR
Next Update		Date d'émission de la LCR + 7 jours [28]
Revoked Certificates	userCertificate	Numéro de série unique du Certificat révoqué
	revocationDate	Date de révocation
	crlEntryExtensions	Informations supplémentaires pouvant être fournies dans les extensions d'entrée de LCR

7.2.2 Extensions

Champs	Critique	Valeur
Authority Key Identifier	Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'ACT émettrice
CRL Number	Non	Numéro de la LCR défini par l'AC Technique émettrice

7.2.3 Extensions d'entrée

Champs	Critique	Valeur
Reason Code	Non	[RFC 5280] : code correspondant à la raison de révocation correcte

[28] Dans le cas de la cessation d'activités de l'AC, la durée de validité de la dernière LCR publiée est de trois (3) ans ou plus.

7.3 Profil des OCSP

Conformément au chapitre 4.10 du présent document, le TSP MediaCert met à disposition des utilisateurs un répondeur OCSP afin que ceux-ci puissent vérifier l'état en temps réel des Certificats émis par les AC en ligne. Ce service est conforme au [RFC 6960].

7.3.1 AC OTU

Dans ce cadre, le répondeur OCSP possède un Certificat délivré par l'AC OTU et dont le profil est détaillé ci-dessous.

7.3.1.1 Champ de base

Champs		Valeur
Version		2 (pour version 3)
Serial number		Défini par l'AC Technique émettrice
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de l'ACT émettrice
Validity		3 ans
Subject	C	FR
	OI	0002 378901946
	OU	AC OTU
	O	Worldline
	SERIALNUMBER [29]	Numéro de série unique du DN
	CN	Service OCSP PKI OTU
Subject Public Key Info		RSA 2048 bits

7.3.1.2 Extensions

Champs		Critique	Valeur
Authority Key Identifier		Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier		Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage		Oui	Digital Signature
Basic Constraint	Certificate Authority	Non	Faux
Certificate Policies	policyIdentifier	Non	1.2.250.1.111.20.5.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Extended Key Usage		Non	ocspSigning (1.3.6.1.5.5.7.3.9)
CRL Distribution Points		Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [30]
Authority Information Access	ocsp	Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [30]
	caIssuers		http://pki-otu-ac[SERIALNUMBER ACT

[29] Conformément à la [RFC 3739], le champ SERIALNUMBER permet de lever le risque d'homonymie dans le reste des champs du DN. Il est construit comme suit : SERIALNUMBER = nombre incrémenté à chaque émission d'un certificat OCSP pour l'AC Technique Emettrice en question.
[30] Cette URL est donnée à titre indicatif. L'URL qui fait foi est celle qui figure dans le Certificat.

Champs		Critique	Valeur
			émettrice].mediacert.com/certificate [30]

7.3.2 AC OTU LCP

Dans ce cadre, le répondeur OCSP possède un Certificat délivré par l'AC OTU LCP et dont le profil est détaillé ci-dessous.

7.3.2.1 Champ de base

Champs		Valeur
Version		2 (pour version 3)
Serial number		Défini par l'AC Technique émettrice
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de l'ACT émettrice
Validity		3 ans
Subject	C	FR
	OI	0002 378901946
	OU	AC OTU LCP
	O	Worldline
	SERIALNUMBER [31]	Numéro de série unique du DN
	CN	Service OCSP PKI OTU LCP
Subject Public Key Info		RSA 2048 bits

7.3.2.2 Extensions

Champs		Critique	Valeur
Authority Key Identifier		Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier		Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage		Oui	Digital Signature
Basic Constraint	Certificate Authority	Non	Faux
Certificate Policies	policyIdentifier	Non	1.2.250.1.111.20.5.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Extended Key Usage		Non	ocspSigning (1.3.6.1.5.5.7.3.9)
CRL Distribution Points		Non	http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [32]
Authority Information Access	ocsp	Non	http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [32]
	caIssuers		http://pki-otu-lcp-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [32]

[31] Conformément à la [RFC 3739], le champ SERIALNUMBER permet de lever le risque d'homonymie dans le reste des champs du DN. Il est construit comme suit :
SERIALNUMBER = nombre incrémenté à chaque émission d'un certificat OCSP pour l'AC Technique Emettrice en question.
[32] Cette URL est donnée à titre indicatif. L'URL qui fait foi est celle qui figure dans le Certificat.

7.3.3 AC ORG

Dans ce cadre, le répondeur OCSP possède un Certificat délivré par l'AC ORG et dont le profil est détaillé ci-dessous.

7.3.3.1 Champ de base

Champs		Valeur
Version		2 (pour version 3)
Serial number		Défini par l'AC Technique émettrice
Signature		sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer		DN de l'ACT émettrice
Validity		3 ans
Subject	C	FR
	OI	0002 378901946
	OU	AC ORG
	O	Worldline
	SERIALNUMBER [33]	Numéro de série unique du DN
	CN	Service OCSP PKI ORG
Subject Public Key Info		RSA 2048 bits

7.3.3.2 Extensions

Champs		Critique	Valeur
Authority Key Identifier		Non	[RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice
Subject Key Identifier		Non	[RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le Certificat
Key Usage		Oui	Digital Signature
Basic Constraint	Certificate Authority	Non	Faux
Certificate Policies	policyIdentifier	Non	1.2.250.1.111.20.5.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Extended Key Usage		Non	ocspSigning (1.3.6.1.5.5.7.3.9)
CRL Distribution Points		Non	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [34]
Authority Information Access	ocsp	Non	http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [34]
	caIssuers		http://pki-org-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [34]

[33] Conformément à la [RFC 3739], le champ SERIALNUMBER permet de lever le risque d'homonymie dans le reste des champs du DN. Il est construit comme suit : SERIALNUMBER = nombre incrémenté à chaque émission d'un certificat OCSP pour l'AC Technique Emettrice en question.
[34] Cette URL est donnée à titre indicatif. L'URL qui fait foi est celle qui figure dans le Certificat.

8 Audit de conformité et autres évaluations

8.1 Fréquences et/ou circonstances des évaluations

Worldline, dans le cadre de l'évaluation du présent service de certification, procède à un audit externe de certification à la norme [ETSI 319 411-1] des IGC présentées au sein de cette PC-DPC tous les deux (2) ans par un organisme accrédité.

En complément, Worldline effectue un audit de surveillance (interne ou externe) entre deux (2) audits externe de Certification à la norme [ETSI 319 411-1].

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.

8.6 Communication des résultats

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

9 Autres problématiques métiers et légales

9.1 Tarifs

Worldline ne commercialise pas ses Certificats seuls mais uniquement au travers de services de plus haut niveau.

9.1.1 Tarifs pour la fourniture ou le renouvellement d'un Certificat

Ceci est traité dans le cadre du contrat de prestations de services de plus haut niveau conclu entre Worldline et l'Abonné.

9.1.2 Tarifs pour accéder aux Certificats

Ceci est traité dans le cadre du contrat de prestations de services de plus haut niveau conclu entre Worldline et l'Abonné.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des Certificats

Sans objet.

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

Sans objet.

9.2 Assurance

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

Sans objet.

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 rapports d'audit.

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 terme de protection des informations confidentielles

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

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

9.3.3.1 Législation applicable

La loi n° 2018-493 du 20 juin 2018, promulguée le 21 juin 2018, a modifié la loi Informatique et Libertés afin de mettre en conformité le droit national avec le cadre juridique européen.
Worldline traite les données personnelles en respectant la législation française en vigueur sur le territoire français, laquelle s'inscrit en conformité de celle prévalant sur le territoire Européen, en matière de protection des données à caractère personnel. Worldline prend toutes les mesures adaptées et nécessaires conformément à cette réglementation pour que les données personnelles qu'elle est amenée à conserver via les IGC soient protégées de toute compromission, atteinte à la sécurité ou perte d'intégrité qui pourrait avoir une incidence sur le service de confiance fourni et les données à caractère personnel qui y sont conservées.

A cet effet, le TSP MediaCert met notamment en œuvre les mesures de sécurité des locaux et des systèmes d'information pour empêcher que les fichiers détenus soient déformés, endommagés, ou que des tiers non autorisés y aient accès.

9.3.3.2 Consentement préalable du Titulaire, des représentants de l'Organisation et des représentants de l'Abonné au traitement de leurs données par l'IGC

Dans le cadre de la création des dossiers d'enregistrement, un ensemble de données personnelles sont nécessaires. Elles sont transmises à l'Autorité d'Enregistrement par les Abonnés ou leur représentant.

[AC OTU][AC OTU LCP] Certificats à usage unique

Dans le cadre des Certificats à usage unique, il est rappelé que l'Abonné veillera à obtenir l'acceptation expresse des futurs Titulaires au traitement et à la conservation de leurs données par l'IGC, avant de transmettre les données personnelles de ces derniers, pour le traitement des demandes de création de ce type de Certificats.
A cet effet, le futur Titulaire devra accepter avant toute demande initiée pour son compte par l'Abonné que les données personnelles le concernant, transmises par l'Abonné à l'Autorité d'Enregistrement fassent l'objet d'un traitement informatique aux seules fins de :

- constituer son identification et permettre son authentification afin de générer un Certificat en son nom ;
- pouvoir lui communiquer les données d'activation de sa clé privée ;
- permettre d'étayer l'identité portée dans le Certificat en apportant si besoin les preuves nécessaires via la conservation des éléments dans le dossier d'enregistrement.

Par ailleurs, lesdites pièces justificatives pourront faire le cas échéant l'objet d'un contrôle automatisé pour vérifier la cohérence des champs. En cas de contrôle infructueux ou négatif, des contrôles manuels seront réalisés par l'Organisation avec laquelle le Titulaire est en relation.

Le consentement du futur Titulaire pour ces traitements, dans le cadre de la mise en œuvre de la signature électronique, doit se manifester par le biais d'une action positive de sa part, ce dernier devant être préalablement informé des conséquences de son choix et en mesure de disposer des moyens de l'exercer.

A cet égard, il est précisé que toute opposition à la conservation de données à caractère personnel empêchera la délivrance de ce type de Certificat. En effet, en acceptant la fourniture du Certificat pour procéder à une signature électronique, le Titulaire accepte que l'AC via l'AE, conserve, à la demande de l'AE, les données à caractère personnel pendant la durée nécessaire à l'exercice des finalités des traitements opérés dans le cadre de la fourniture et la gestion du Certificat à usage unique. En effet, l'IGC doit pouvoir répondre aux obligations auxquelles il est soumis dans le cadre des audits qu'il est amené à passer, justifier du respect du ou des niveaux de certification choisis, des fonctions d'identification assignées à la signature électronique, des règles de l'art et des normes applicables.

L'Abonné veillera à donner une information complète au Titulaire et à s'assurer que le prestataire désigné respecte les dispositions légales applicables en matière de protection des données personnelles.

[AC ORG] Certificats d'Organisation

Dans le cadre de l'établissement du dossier d'enregistrement, l'Abonné via ses représentants, fournit à l'Autorité d'Enregistrement un ensemble de données personnelles nécessaires à la constitution du dossier. Cette transmission par le représentant de l'Abonné se fait en connaissance des finalités attachée à cette collecte. A cet effet, les représentants de l'Abonné et les éventuels représentants de l'Organisation devront accepter que les données personnelles les concernant fassent l'objet d'un traitement informatique aux seules fins de :

- constituer leur identification et, dans le cas où l'Abonné et l'Organisation sont la même entité, permettre leur authentification, afin de générer un Certificat contenant leurs informations ;

- permettre d'étayer l'identité éventuellement portée dans le Certificat et les pouvoirs conférés en apportant si besoin les preuves nécessaires via la conservation des éléments dans le Fichier de preuves.

En conséquence, les représentants des Abonnés, en acceptant de représenter l'Abonné, auront préalablement accepté que leurs données personnelles fassent l'objet de traitements et soient conservés aussi longtemps que l'exige l'exercice des finalités des traitements opérés dans le cadre de la fourniture et la gestion de Certificats d'Organisation.

9.3.3.3 Droits de la personne concernée sur les données

Conformément à l'article 39 de la loi informatique et libertés, modifié par la loi n°2018-493 du 20 juin 2018, et à l'article 14 du RGPD toute personne physique justifiant de son identité a le droit le de demander l'accès à ses données à caractère personnel dans les conditions visées par ces articles.

Toute personne physique justifiant de son identité peut demander la rectification, la mise à jour ou l'effacement de ses données personnelles.
Dans le cas des Certificats à usage unique, les données personnelles qui ont servi à étayer l'identification du Titulaire pour la production du Certificat avec lequel il a signé ne pourront être rectifiées, verrouillées ou effacées qu'à l'épuisement de la finalité pour laquelle lesdites données personnelles ont été collectées et les traitements opérés.
Il en est de même dans le cas des données personnelles collectées pour l'émission de Certificats d'Organisation.
Les données personnelles ayant servi à l'identification et l'authentification du futur porteur de Certificat communiquées au cours du processus de signature électronique ou de la constitution du dossier d'enregistrement restent dans l'historique des traces de la transaction et de la signature électronique opérée ceci jusqu'à l'épuisement de la finalité pour laquelle ces données personnelles ont été collectées et les traitements opérés.
Il en est de même, pour les données personnelles communiquées lors de la demande de création de Certificat d'Organisation.

En conséquence des dispositions qui précèdent, les personnes qui ont donné leur consentement préalable au traitement de leurs données personnelles par l'IGC comme exposé dans le présent document peuvent, conformément à la loi, accéder à l'ensemble des informations les concernant, détenues par l'IGC et en obtenir la copie.

Aucune des données à caractère personnel communiquées lors de l'enregistrement du Titulaire ou lors de la constitution du dossier d'enregistrement pour les Abonnés et les Organisations ne peut être utilisée par l'IGC, pour une finalité autre que celle définie dans le cadre de la PC-DPC.

Le droit d'accès peut s'exercer par écrit : courrier postal auprès du point de contact du TSP MediaCert, adresse présente au chapitre 1.6.2 de ce document ou présente sur le site web du TSP MediaCert (cf. chapitre 2.2), accompagné d'une copie d'une pièce d'identité. Idéalement, en recommandé avec accusé de réception.

9.3.3.4 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administrative

Worldline peut devoir mettre à disposition les dossiers d'enregistrement des Titulaires, des Abonnés et des Organisations à des tiers habilités dans le cadre de procédures judiciaires ou dans le cadre d'audits aux fins de vérifier la délivrance de Certificats. L'IGC dispose de procédures sécurisées pour permettre cet accès qui sont tracés nominativement et conservés.

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.

A cet effet, l'Autorité d'Enregistrement collecte et traite les données d'identification des futurs Titulaires, les contacts Abonnés ou représentants, les contacts Organisations ou représentants contenues dans les dossiers d'enregistrement (fichier de preuves).

9.4.2 Informations à caractère personnel

Les données d'enregistrement du Titulaire ou des Individus habilités telles que fournies par l'Abonné sont des informations considérées comme personnelles. Un accès aux données personnelles est mis en place conformément à la [PG].

9.4.3 Information à caractère non personnel

Sans objet.

9.4.4 Responsabilité en terme de protection des données personnelles

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

9.4.5 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'IGC ne sont pas divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

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

9.4.7 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 (cf. chapitre 1.5) ;
- 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 ;
- avoir des pratiques non-discriminatoires dans leurs politiques et leurs procédures.

9.6.1 Autorité de Certification

Les AC ont pour obligation de :

- contrôler à ce que l'Autorité d'Enregistrement agissant au nom de l'AC respecte la présente PC-DPC ;
- publier les informations publiques citées au chapitre 2.2 du présent document, notamment les Conditions Générales d'Abonnement [CGA] et les Conditions Générales des Services [CGS], de façon durable et sécurisée ;
- rendre accessible ses services à tout Abonné ayant accepté les Conditions Générales d'Abonnement [CGA] ;
- collaborer avec les auditeurs lors des contrôles de conformité et mettre en œuvre d'éventuelles mesures décidées avec les auditeurs suite aux contrôles de conformité.

9.6.2 Service d'enregistrement

L'AE a pour obligation de :

- respecter les procédures d'enregistrement décrites dans la présente PC-DPC.

9.6.3 Porteurs de Certificat

Les bénéficiaires de Certificat ont pour obligation de :

- protéger les moyens d'accès aux clés privées et aux Certificats ;
- n'utiliser leurs Certificats que pour les usages prévus et définis dans le PC-DPC associée ;
- révoquer ou demander la révocation de leur Certificat en cas de compromission ou de suspicion de compromission ;
- révoquer ou demander la révocation de leur Certificat en cas de compromission ou de suspicion de compromission des moyens d'accès susvisés ;

- vérifier et respecter les obligations qui leur incombent décrites dans le présent document et dans les Conditions Générales des Services [CGS].

9.6.3.1 Abonné

En plus des obligations définies au chapitre 9.6.3, l'Abonné a les obligations, différentes selon le type de Certificat, qui figure ci-dessous.

[AC OTU][AC OTU LCP] Certificats à usage uniques

Pour un Certificat à usage unique, l'Abonné aux AC en ligne a pour obligation de :

- collecter et vérifier ou faire collecter et faire vérifier sous sa responsabilité les informations d'identité communiquées par le futur Titulaire ;
- communiquer au titulaire ses obligations (cf. chapitre 9.6.3.2) ;
- informer le titulaire du processus de demande de Certificat et des conséquences de son utilisation dans le cadre de la présente PC-DPC ;
- transmettre, dans sa demande, les données relatives à l'identification du futur Titulaire ainsi que l'ensemble des consentements nécessaires de ce futur Titulaire comme défini au chapitre 3.2.3.1 du présent document ;
- constituer et signer la demande de Certificat du futur Titulaire ;
- garder le contrôle exclusif de ses moyens d'authentification auprès de l'Autorité d'Enregistrement;
- communiquer dans les meilleurs délais à l'Autorité d'Enregistrement tout évènement pouvant porter atteinte à la qualité de l'identification de ses futurs Titulaires ;
- communiquer dans les meilleurs délais à l'Autorité d'Enregistrement tout évènement pouvant porter atteinte à la fiabilité de ses moyens d'authentification auprès de celle-ci ;
- d'avoir des pratiques non-discriminatoires.

[AC ORG] Certificats d'Organisation

Pour un Certificat d'Organisation, l'Abonné à l'AC a pour obligation de :

- compléter le dossier de demande de création de Certificat en fournissant tous les éléments requis, les justificatifs et pouvoirs nécessaires (cf. chapitre 4.1.2.2). Les informations et les justificatifs communiqués à l'Autorité d'Enregistrement se doivent d'être exacts, sincères et à jour lors de la demande de création de Certificat ;
- informer l'Autorité d'Enregistrement dans le cas où les données du Certificat ne seraient plus valables du fait d'un changement au sein de l'Organisation. A cet égard, l'Abonné doit notifier sans délai à l'AE, par lettre recommandée avec accusé de réception :
    - tout changement dans l'identité de la personne assurant la fonction de représentant d'Abonné ou de représentant adjoint d'Abonné, ainsi que la date d'effet de ce changement, accompagné des pièces justificatives ;

- tout changement dans les informations communiquées à l'AE, ainsi que la date d'effet de ces changements.

- demander la révocation du Certificat dans les cas listés par le présent document. A cet égard, la modification d'informations figurant dans le Certificat d'Organisation entraîne la révocation du Certificat et son remplacement aux frais de l'Organisation ;

- communiquer dans les meilleurs délais à l'Autorité d'Enregistrement tout évènement pouvant porter atteinte à la fiabilité des moyens d'authentification auprès de celle-ci. A cet égard, les changements (prénom, nom, adresse e-mail) doivent être notifiés à l'AE ;

- informer l'Autorité d'Enregistrement dans le cas où l'Organisation n'existerait plus. A cet égard, l'Abonné doit notifier sans délai à l'AE, par lettre recommandée avec accusé de réception, les changements (prénom, nom, adresse e-mail, identifiant de l'Organisation) affectant l'ensemble des Certificats de l'Organisation, accompagnés des pièces justificatives ;

- informer l'Autorité d'Enregistrement dans le cas où des informations concernant l'Organisation, ne figurant pas dans le Certificat d'Organisation et n'ayant pas d'impact sur sa validité, sont amenées à être modifiées. A cet égard, l'Abonné doit notifier dans les meilleurs délais l'AE, par lettre simple, les changements d'informations ;

- d'avoir des pratiques non-discriminatoires.

Dans le cas où l'Abonné fait appel à un prestataire technique, il lui appartient de faire respecter ces obligations par ce dernier d'autant que ce prestataire pourra être détenteur de secrets propres à l'Abonné : clés privées correspondants à des Certificats d'authentification et de signature de message. Il appartient donc à l'Abonné de s'assurer que des mesures de protection d'accès à ces secrets sont bien mis en œuvre.

9.6.3.2 Titulaires

En plus des obligations définies au chapitre 9.6.3, le futur titulaire a le devoir de communiquer des informations et des justificatifs, demandés par l'Abonné, qu'il certifie exacts et à jour lors de la demande de Certificat.

Les obligations qui incombent au futur Titulaire sont par ailleurs définies dans le contrat conclu avec son mandataire, ici désigné comme étant l'Abonné.

9.6.4 Utilisateurs de Certificat

Les utilisateurs des Certificats doivent :

- vérifier et respecter les obligations qui leur incombent dans le présent document et dans les Conditions Générales des Services [CGS]. Ces obligations seront pour les Certificats à usage unique décrites par l'Abonné dans le contrat qui le lie au futur Titulaire (cf. chapitre 9.6.3.1). Ce contrat expose le fonctionnement d'une signature sous forme électronique, les implications de ce choix, les modalités pour y procéder avec les recueils des consentements nécessaires en conformité avec celles figurant dans son Contrat d'Abonnement ;

- 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

Les AC en ligne s'engagent à émettre des Certificats en conformité avec le présent document, ainsi qu'avec l'état de l'art et de la technique.

Le TSP MediaCert garantit via ses services :

- l'authentification de l'Abonné avec son Certificat par l'Autorité d'Enregistrement ;
- la génération de Certificat(s) conformément à la demande de l'Abonné, préalablement authentifié et vérifiée ;
- la mise à disposition de fonctions d'informations sur l'état des Certificats émis, suite à la demande de l'Abonné, par les AC conformément au présent document ;
- le contrôle exclusif de la clé privée du Certificat par le Dispositif Porteur de Certificats et la destruction de cette même clé à l'issue d'une session unique d'utilisation dans le cas d'un Certificat à usage unique.

Aucune autre garantie n'est assurée.

9.8 Limite de responsabilité

La responsabilité du TSP MediaCert ne peut être engagée qu'en cas de non-respect prouvé de ses obligations.

Le TSP MediaCert ne pourra être tenue responsable dans le cas d'une faute sur le périmètre d'une entité Abonnée, notamment en cas :

- d'utilisation d'un Certificat expiré ;
- d'utilisation d'un Certificat révoqué ;
- d'utilisation d'un Certificat dans le cadre d'une application autre que celles décrites au chapitre 4.5 de la présente PC-DPC.

Le TSP MediaCert n'est d'une façon générale pas responsable des documents et informations transmises par l'Abonné et ne garantit pas leur exactitude ni les conséquences de faits, actions, négligences ou omissions dommageables de l'Abonné, de son représentant ou du Titulaire.

L'Abonné s'interdit de prendre un engagement au nom et pour le compte du TSP MediaCert auquel il ne saurait en aucun cas se substituer.

9.9 Indemnités

La délivrance de Certificats par les AC concernées par le présent document est opérée dans le cadre de services de plus haut niveau tels que notamment de souscription électronique.

Le contrat cadre signé entre le client et Worldline, ou son mandataire dument habilité, précise les conditions d'indemnisation en cas de dommage. En l'absence de contrat cadre, les Conditions Générales de Ventes de Worldline s'appliqueront.

9.10 Durée et fin anticipé de validité de la PC

9.10.1 Durée de validité

La PC-DPC est rendue effective une fois validée par l'entité responsable de ce document (cf. chapitre 1.6.1). Elle 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

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

En dépit du remplacement de la présente PC-DPC par une nouvelle version, les derniers Certificats émis lorsqu'elle était encore valide entraînent l'application du présent document auxdits Certificats et aux différents acteurs et ce jusqu'à l'expiration des Certificats en question.

9.11 Notifications individuelles et communications entre les participants

Le TSP MediaCert informera, via un communiqué par e-mail, ses Abonnés au plus tard un (1) mois avant la publication de la nouvelle version du présent document, en cas de changement impactant la présente PC-DPC.

L'Abonné sera également informé de la mise en place effective de la nouvelle version de la PC-DPC au plus tard un (1) mois suivant sa publication via un communiqué par e-mail signé.
Par ailleurs, l'Abonné sera informé de toute modification des CGS, des CGA ou des CGV via un communiqué par e-mail.

Toutes les composantes et tous les acteurs des AC sont tenus informés, à travers un communiqué interne, des amendements effectués sur le présent document et des impacts éventuels qui en découlent les concernant.

Aucune exigence concernant la validation des changements de la part des Abonnés n'est formulée par le présent document. En effet, l'utilisation des services après notification des modifications opérées vaut acceptation de plein droit de ces modifications.

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

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

9.12.2 Mécanisme et période d'information sur les amendements

En cas de changement nécessitant la modification de la présente PC-DPC, les informations concernant le mécanisme et la période d'information sur les amendements sont fournies au chapitre 9.11.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

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

9.13 Dispositions concernant la résolution de conflits

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

Le contrat cadre signé entre l'Abonné et Worldline, ou son mandataire dument habilité, précise les dispositions concernant la résolution de conflits. En l'absence de contrat cadre, les Conditions Générales de Ventes de Worldline s'appliqueront.

Le contact habilité pour toute remarque, demande d'informations complémentaires, réclamation ou remise de dossier de litige concernant la présente PC-DPC est défini au chapitre 1.6.2. Toute demande doit être établie par e-mail avec accusé de réception ou par courrier postal recommandé avec accusé de réception.

9.14 Juridictions compétentes

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

Le contrat cadre signé entre le client et Worldline, ou son mandataire dument habilité, précise cette disposition. En l'absence de contrat cadre, les Conditions Générales de Ventes de Worldline s'appliqueront.

9.15 Conformité aux législations et réglementations

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

9.16 Dispositions diverses

9.16.1 Accord global

Sans objet.

9.16.2 Transfert d'activités

Sans objet.

9.16.3 Conséquences d'une clause non valide

Sans objet.

9.16.4 Application et renonciation

Sans objet.

9.16.5 Force majeure

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

Le contrat cadre signé entre le client et Worldline, ou son mandataire dument habilité, précise cette disposition. En l'absence de contrat cadre, les Conditions Générales de Ventes de Worldline s'appliqueront.

9.17 Autres dispositions

9.17.1 Indépendance des parties et non-discrimination

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

9.17.2 Analyse de risques

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

9.17.3 Documents contractuels

En cas de contradiction entre les articles des Conditions Générales d'Abonnement [CGA] et ceux des dispositions du Contrat de Service de plus haut niveau (contrat cadre), les clauses des Conditions Générales d'Abonnement [CGA] qui procèdent de la Politique de Certification – Déclaration des Pratiques de Certification applicable prévaudront.