Référence du document :	OTU.PC-DPC.0002
Révision du document :	3.1
Date du document :	21/07/2017
Classification :	Publique

Autorité de Certification OTU

Politique Certification
Déclaration des Pratiques de Certification

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

Historique des révisions de document

Version	Date	Auteur	Motif
1.0	24/12/2012	C.BRUNET	Version publique initiale
1.1	08/04/2013	C.BRUNET	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
1.2	22/11/2013	C.BRUNET	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
1.3	01/02/2015	C.BRUNET	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 •
2.0	07/11/2016	V. DUMOND C. LOOTVOET A. BRUGNOT J.J. MILHEM	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 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	C. LOOTVOET	• 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)
3.0	09/06/2017	F. LESECQ V. DUMOND	Réécriture pour prise en compte des contraintes réglementaires eIDAS.
3.1	21/07/2017	F.LESECQ, F. DA SILVA	Prise en compte des remarques de l'audit eIDAS.

Table des matières

1 Introduction

1.1 Présentation Générale

Ce document décrit la Politique de Certification de l'Autorité de Certification OTU établie par Worldline pour régir l'ensemble du cycle de vie (création, émission, utilisation, …) des Certificats de signature One Time Usage (OTU) mis en œuvre dans le cadre de souscription en ligne OTU, mais également celui des Certificats cachets électroniques utilisés pour sceller des données électroniques afin de garantir leur origine et leur intégrité.

Ce document présente dans ce cadre :

- les exigences auxquelles se conforme l'Autorité de Certification OTU dans les étapes d'enregistrement et de contrôle des demandes de Certificats ;
- 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 l'Autorité de Certification OTU a recours dans la gestion des Certificats qu'elle émet.

Ce document concerne les Certificats à destination d'un Dispositif Porteur de Certificats géré par Worldline. Il considère par ailleurs quatre (4) types de Certificats conformément aux chapitres 1.2.2 et 7.1 :

- les Certificats à usage unique, en conformité avec [ETSI EN 319 411-1] niveau LCP ;
- les Certificats d'Organisation, en conformité avec [ETSI EN 319 411-1] niveau LCP ;
- les Certificats à usage unique de test, en conformité avec [ETSI EN 319 411-1] niveau LCP ;
- les Certificats d'Organisation de test, en conformité avec [ETSI EN 319 411-1] niveau LCP.

1.2 Identification

1.2.1 Identification du document

Eléments	Valeur
Titre	**Autorité de Certification OTU : Politique de Certification / Déclaration des Pratiques de Certification**
Référence document	**OTU PC-DPC 0002**
Version	**3.1**
Auteur	**Worldline**
Référence produit	**Autorité de Certification OTU**

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

1.2.2 Identification de l'Autorité de Certification

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

L'OID de cette PC/DPC est le suivant : **1.2.250.1.111.17.0.3**

Cet OID est basé sur l'OID attribué par l'AFNOR à Worldline (1.2.250.1.111) et est construit de la façon suivante : 1.2.250.1.111.x.y.z.w où :

- x : année de création de la Politique de Certification/Déclaration des Pratiques de Certification : 2017 → 17 ;
- y : numéro attribué à l'Autorité de Certification par Worldline d'après l'année de création ;
- z : version de la Politique de Certification/Déclaration des Pratiques de Certification ;
- w : type du Certificat utilisé par l'AC OTU.

Comme le sous-entend la description ci-dessus, l'AC OTU a défini un OID pour chacun des types de Certificats qu'elle délivre comme suit :

- OID des Certificats à usage unique [LCP] : 1.2.250.1.111.17.0.3.1 ;
- OID des Certificats d'Organisation [LCP] : 1.2.250.1.111.17.0.3.2 ;
- OID des Certificats à usage unique de test [LCP] : 1.2.250.1.111.17.0.3.3 ;
- OID des Certificats d'Organisation de test [LCP] : 1.2.250.1.111.17.0.3.4.

L'AC OTU est rattachée à une Autorité de Certification Racine Atos Worldline dont les informations nécessaires sont les suivantes :

Eléments	Valeur
***OID* de la PC/DPC Racine**	**1.2.250.1.111.12.0.2**
***Distinguish Name* (DN)**	**C = FR** **O = Atos Worldline** **OU = 0002 378901946** **CN = AC Racine – Root CA – 2012**

La Chaîne de Certification de l'IGC OTU possède la structure suivante :

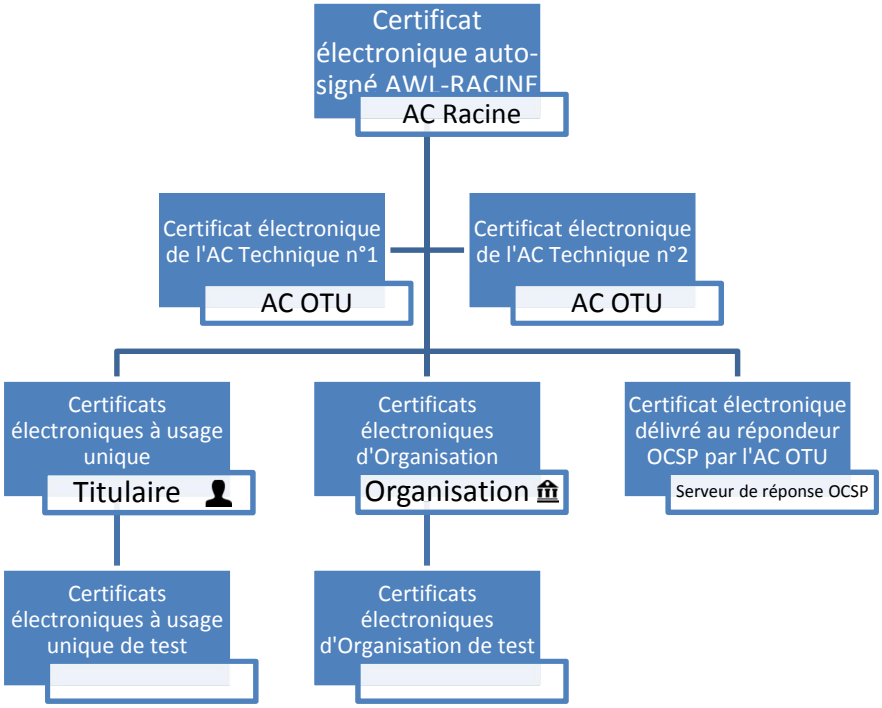

Figure 1 - Chaîne de Certification de l'IGC OTU

1.3 Entités intervenant dans l'IGC

L'Infrastructure à Gestion de Clés (IGC) 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.

L'AC OTU s'appuie 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, l'IGC OTU est constituée d'un certain nombre d'entités comme présenté par le schéma fonctionnel en figure 2.

La décomposition fonctionnelle de l'IGC OTU 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.

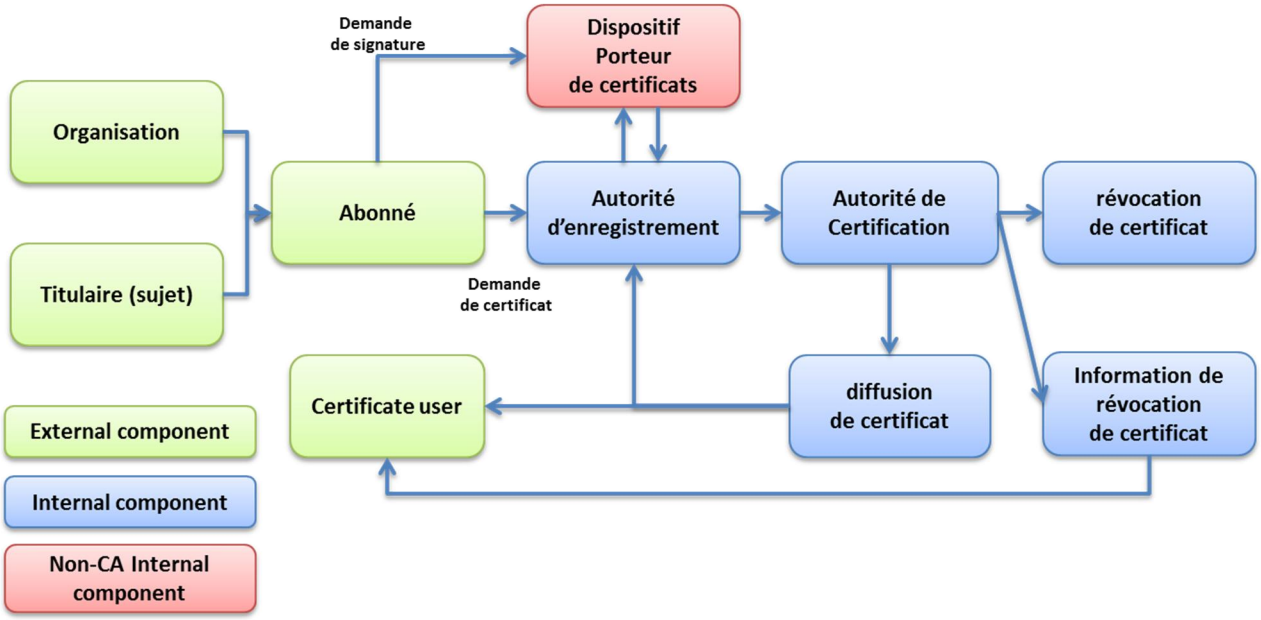

Figure 2 – Schéma fonctionnel de l'IGC OTU

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, …).

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 OTU et ne peuvent être utilisés que pour les usages décrits au chapitre 1.5.1.1 de cette PC/DPC.

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.

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.

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.

L'Autorité de Certification OTU est représentée 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.

1.3.2 Autorité d'Enregistrement

L'Autorité d'Enregistrement (AE) est l'entité interlocutrice des unités clientes (Abonnés) qui lui transmettent des demandes de création ou de révocation de Certificats. Elle prend donc en charges 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 ;
- enregistrement des demandes de création et de révocation de Certificat ;
- acceptation ou refus des demandes de création et de révocation de Certificat ;
- livraison des Certificats au Dispositif Porteur de Certificats ;
- archivage des demandes de création et de révocation de Certificat.

Pour rendre ces services, l'AC OTU opère sa propre Autorité d'Enregistrement 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 pour l'AC OTU et qui constituent à ce titre un point d'accès unique à cette Autorité de Certification (serveurs permettant la transmission des demandes et la livraison des Certificats).

1.3.3 Dispositif Porteurs 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 l'AC OTU, 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.

1.3.4 Bénéficiaires de Certificats

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

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

Certificat de signature OTU

Il est aussi précisé que dans le cadre des Certificats de signature OTU, la demande de Certificat à l'Autorité d'Enregistrement OTU est faite par l'Abonné un moyen d'un message signé électroniquement par celui-ci. L'Abonné, dans ce cas :

- doit préalablement à la demande 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 OTU (cf. chapitre 3.2.3.1).

- l'Autorité de Certification produira alors un Certificat à usage unique (cf. chapitre 1.4.1).

Cachet électronique
S'il s'agit de sceller des données électroniques au nom d'Organisations rattachées à l'Abonné, légalement ou par convention, l'AC OTU 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 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. Cette signature ou ce scellement est associé à un Document.

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.

Il appartient aux utilisateurs de vérifier, à minima avant utilisation, les informations sur le statut de révocation du Certificat à travers les différents moyens mis à sa disposition comme décrit au chapitre 4.9.10.

1.3.6 Autres 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

L'AC OTU produit quatre (4) types de Certificats qui se distinguent notamment par leur OID (cf. chapitre 1.2.2).

1.4.1 Certificat à usage unique

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

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 OTU 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 OTU 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 Certificat 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 Certificat 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 l'AC OTU 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 l'AC OTU 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 7.1.5 et 7.1.6). 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

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 :

- signer électroniquement un Document avec un Certificat à usage unique ;
- sceller électroniquement un Document avec un Certificat Organisation.

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

La Bi-clé de l'AC OTU sert exclusivement à signer des Certificats et des LCR dont les gabarits sont définis au chapitre 7 du présent document.
Son 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

Toute utilisation de Certificat émis par l'AC OTU en violation avec les usages décrits dans la présente PC/DPC au chapitre précédent (chapitre 1.5.1) est strictement interdit. L'AC OTU ne pourra être tenue pour responsable de tout détournement d'usage tel que spécifiés.

1.6 Gestion de la PC

1.6.1 Entité gérant la PC

Worldline est responsable de l'élaboration, du suivi et de la révision, dès que nécessaire, de la présente PC/DPC. A cette fin, un Comité Sécurité est en place au sein de l'IGC OTU. Il est constitué :

- d'au moins un représentant de l'AC OTU ;
- du responsable sécurité de l'AC OTU ;
- d'au moins un membre de l'équipe de suivi de conformité des plateformes, selon les nécessités de validation documentaire.

Il statue au moins une fois par an sur la nécessité d'apporter des modifications à ce document et procède ainsi à la vérification de sa conformité à l'état de l'art, aux textes législatifs et réglementaires en vigueur auxquels il est sujet.

1.6.2 Point de contact

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

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

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

La cohérence de la DPC est garantie par l'unicité du présent document et par sa relecture et validation par le Comité Sécurité lors de toute modification majeure (cf. chapitre 9.12.1).

1.6.4 Procédure d'approbation de la conformité de la DPC

Worldline est responsable de la conformité des pratiques qui sont documentées dans la présente PC/DPC. A cette fin, Worldline s'appuie sur le Comité Sécurité (cf. chapitre 1.6.1) qui a notamment le rôle de procéder à la validation de ces pratiques suite à un suivi régulier de l'état de l'art ou aux résultats d'audits externes effectués.

Le processus de vérification de conformité de la PC/DPC est spécifié dans le chapitre ci-dessus (cf. chapitre 1.6.3).

Les modifications effectuées dans la PC/DPC sont notifiées aux acteurs concernés et la PC/DPC leur est rendue disponible sans délai.

1.7 Définitions et abréviations

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 de l'AC OTU pour la délivrance par l'AC OTU :

- de Certificats d'Organisation à la demande de personnes dûment habilitées au sein de l'Abonné qui lui sont rattachées légalement et/ou conventionnellement ;
- de Certificats à usage unique au nom des Titulaires tels que définis dans la présente PC/DPC qu'il 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 OTU, 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.

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.

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

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.entité représentant une entreprise ou pouvant faire référence à un nom de marque pour laquelle un Certificat de scellement 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.

Service d'information sur l'état des Certificats : cf. chapitre 1.3.1.

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 e-IDAS, 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 e-IDAS, 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 Abréviations

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 ;
- **PSO :** Politique de Sécurité Opérationnelle ;
- **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*) ;

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

2.1 Entités chargées de la mise à disposition des informations

L'AC OTU est l'entité qui se charge de mettre à disposition les informations devant être publiées.

En effet, pour la mise à disposition des informations devant être publiées à destination des utilisateurs de Certificats générés par l'AC OTU, celle-ci met en œuvre une fonction de publication et une fonction d'information sur l'état des Certificats par le biais d'un répondeur OCSP et de la publication de LCR sur son site web.

L'AC OTU se charge notamment de publier cette PC/DPC sur son site web.

2.2 Informations devant être publiées

Les informations publiées par l'AC OTU sur son site web sont les suivantes :

- les listes des Certificats révoqués (LCR) ;
- la présente PC/DPC écrite en français et en anglais ;
- les anciennes versions de PC écrites en français et en anglais ;
- 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 ;
- l'adresse pour accéder au répondeur OCSP de l'AC OTU ;
- le Certificat de l'AC OTU en cours de validité ;
- les Certificats de la gamme de test.

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 l'AC OTU conformément au chapitre 7.1 du présent document.

La politique de gestion de preuve (PGP) est rendue disponible à l'Abonné sur demande électronique (e-mail).

Le site web de l'AC OTU est disponible 7j/7 et 24h/24. Il est surveillé par les services du groupe Atos. Son adresse est la suivante : https://www.mediacert.com
Cette page contenant les informations publiées dispose d'un haut niveau de disponibilité avec une exigence de 99,8% de disponibilité.

2.3 Délais et fréquences de publication

Le délai et la fréquence de publication ainsi que les exigences de disponibilité pour les informations sur l'état des Certificats sont indiqués aux chapitres 4.9.7, 4.9.8 et 4.10.2.

Il est précisé que les versions antérieures des documents contractuels (CGA, …) régissent exclusivement les périodes de temps couvertes par ces versions, soit jusqu'à leur remplacement notifié aux Abonnés. Dès lors qu'une nouvelle version est publiée et notifiée aux Abonnés, elle aura vocation à s'appliquer immédiatement pour l'avenir, les

changements intervenus ne concernant que des précisions rédactionnelles, des modifications liées à l'état de l'art et de la réglementation, sans incidence sur les clauses du contrat de plus haut niveau rattaché aux conditions générales d'Abonnement mais nécessaires pour le suivi qualitatif des prestations de confiance. Si toutefois, elles devaient avoir une incidence sur l'économie du contrat de plus haut niveau rattaché aux conditions générales d'Abonnement, les parties se reporteront aux modalités prévues dans les conditions générales d'abonnement.
L'AC OTU prévient, dans des délais raisonnables, les Abonnés disposant de Certificat(s) d'Organisation lors de toute modification des CGS, des CGA, des CGV et de la présente PC/DPC (cf. chapitre 9.11) afin qu'ils prennent connaissance des changements susceptibles ou non de les affecter. Ces documents sont régulièrement revus conformément à ce qui est écrit au chapitre 9.12. De plus, ils sont publiés à la fin de ce délai de préavis sur le site web de l'AC OTU.

Le Certificat de l'AC OTU est publié suite à sa génération et avant toute Certification.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées sur le site web de l'AC OTU est accessible aux utilisateurs uniquement en lecture. De plus, ces documents déposés sur ce site web sont certifiés authentiques par la présence d'une signature électronique.

L'accès en modification aux systèmes de publication des informations sur l'état des Certificats (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions habilitées de l'IGC OTU et se fait à travers une authentification forte sur des serveurs dédiés au contrôle d'accès.

L'accès en modification des autres informations est strictement limité aux fonctions d'administration internes habilitées de l'IGC OTU. Le contrôle d'accès est effectué par des serveurs dédiés à cette fonction.

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 Certificat à usage unique

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

3.1.2.2 Certificat 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 notions d'anonymisation ou de pseudonymisation ne sont pas utilisées.

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 de l'AC OTU et après sa cessation d'activité, un « *Distinguished Name* » (DN) attribué à un Titulaire ou à une Organisation par l'AC OTU 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 :

- pour les Certificats à usage unique, l'unicité est garantie par le champ « SERIALNUMBER » du DN ;

- pour les Certificats d'Organisation, l'unicité est garantie par le champ « SERIALNUMBER » du DN mais aussi par le champ « *Organisation ID* » du DN qui doit être unique pour chaque Organisation. Cette deuxième partie de la règle est notamment vérifiée par l'AE.

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 Certificat 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 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 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.

3.2.2.1.1 La signature préalable d'un Contrat d'Abonnement

Le statut d'Abonné est conditionné par la mise en place préalable d'une relation contractuelle entre l'Abonné et l'AC OTU. 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 ainsi que dans les Conditions Générales d'Abonnement (documents joints au Contrat d'Abonnement).

3.2.2.1.2 La désignation ou la nomination de représentants au sein de l'Abonné pour les demandes de création de Certificats à usage unique et/ou d'Organisation

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 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 à l'AC OTU 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.

3.2.2.1.3 Les documents à fournir lors de la souscription du Contrat d'Abonnement

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

- la fiche d'information du représentant de l'Abonné à l'AC OTU, 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 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 comportant une photographie d'identité parmi les documents définis ci-après : carte nationale d'identité d'un pays de l'union européenne ou passeport et
- un extrait KBIS datant de moins de trois (3) mois, 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 ; ou
- 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 Validation d'une Organisation

Comme décrit au chapitre 1.3.4, une Organisation est représentée par un individu habilité : le représentant de l'Organisation. Les informations concernant l'Organisation à fournir à l'Autorité d'Enregistrement par l'Abonné sont les suivantes :

Concernant l'Organisation

- 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, …).

Concernant le droit de l'Abonné à faire figurer le nom de l'Organisation dans le Certificat

- 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.

- si le Certificat est destiné à l'Abonné lui-même, c'est-à-dire que le nom de l'Abonné est alors le même que celui de l'Organisation, ce document n'est pas requis.

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

- une demande signée et datée de moins de trois (3) mois par un représentant habilité de l'Abonné si le Certificat est destiné à l'Abonné, spécifiant :
    - le nom de l'Organisation à faire figurer sur le Certificat électronique ;
    - le nom et prénom de l'individu habilité à représenter l'Organisation et identifié dans le Certificat.
- une demande signée et datée de moins de trois (3) mois par un représentant habilité de l'Organisation fournie à l'Abonné si le Certificat n'est destiné à l'Abonné, spécifiant :
    - le nom de l'Organisation à faire figurer sur le Certificat électronique ;
    - le nom et prénom de l'individu habilité à représenter l'Organisation et identifié dans le Certificat.
- 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 ;
    - Carte 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 par téléphone.

3.2.3 Validation de l'identité d'un individu

3.2.3.1 Validation de l'identité d'un titulaire de 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. 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 le Certificat produit par l'AC OTU. 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.

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 l'AC OTU, la politique d'identification qu'il a mis en place (cf. chapitre 3.2.2.1.3) 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 carte 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.
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 de cette politique, au moins une (1) fois par an, en réalisant des échantillonnages conformément à la procédure d'échantillonnage de l'AE.

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.

La politique d'identification mentionnée plus haut 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 ;

- 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 d'expression et de recueil du consentement du Titulaire 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 du Titulaire ;

- un enregistrement vocal 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 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 lors de la mise en œuvre du procédé choisi.

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 Validation de l'identité d'un titulaire de Certificat d'Organisation

Les informations sont disponibles au chapitre 3.2.2.2 – *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 l'Autorité de Certification OTU 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

La validation d'un Abonné est décrite au chapitre 3.2.2.1. Lors des demandes 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 Certificat 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 l'AC OTU comme décrit dans le document DTPC.

3.2.5.2 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 des clés

3.3.1 Certificat 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 Certificat 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 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 OTU. 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 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 Certificat

4.1.1 Origine d'une demande de Certificat

4.1.1.1 Certificat 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 service de signature fourni par l'AC OTU.

4.1.1.2 Certificat 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 de Certificat

4.1.2.1 Certificat 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 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 ;
- informer le futur Titulaire des traitements réalisés de ses informations personnelles par l'Autorité d'Enregistrement 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 par elle-même, celle-ci la transmet à l'Autorité de Certification pour la génération du Certificat à usage unique au nom du Titulaire.

L'AC OTU ne peut être tenue responsable si l'Abonné et/ou le Titulaire ne respectent pas les engagements qu'ils ont acceptés pour bénéficier du service de signature fourni par l'AC OTU.

L'AC OTU 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 Certificat 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.

L'AC OTU ne peut être tenue responsable si l'Abonné ne respecte pas les engagements qu'il a acceptés dans le cadre du Contrat d'Abonnement conclu avec l'AC OTU.

L'AC OTU 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 Certificat

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

4.2.1.1 Certificat 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 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 OTU et conserve une trace de la demande de l'Abonné archivée au format numérique.

L'AC OTU génèrera un Certificat contenant les données d'identité du titulaire comme défini au chapitre 7.1.30 du présent document.

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

4.2.1.2 Certificat 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 : 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 OTU 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 Certificat 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 Certificat 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 Certificat à usage unique

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

3.1.1.1 Certificat 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 OTU 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 OTU transmet le Certificat produit au Dispositif Porteur de Certificats via l'AE. Le Dispositif Porteur de Certificat garantit la sécurité des Bi-clés conformément à ce qui est défini au chapitre 6.1.1.4.

4.3.1.1 Certificat 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 Certificat d'Organisation

Dans le cas de Certificats d'Organisation, le Certificat produit est également transmis par e-mail au représentant de l'Abonné.

4.3.2 Notification par l'AC de la délivrance du Certificat

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

4.3.2.1 Certificat à usage unique

Sans objet.

4.3.2.2 Certificat d'Organisation

Dans le cas de délivrance de Certificats d'Organisation, le Certificat 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), ce qui vaut convention expresse notification.

4.4 Acceptation du Certificat

4.4.1 Démarche d'acceptation du Certificat

4.4.1.1 Certificat 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 Certificat d'Organisation

Le Certificat d'Organisation produit par l'AC OTU 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. 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.

4.4.2 Publication du Certificat

Il n'y a pas de service de publication des Certificats émis par l'AC OTU. Seul le Certificat de l'AC OTU est publié (cf. chapitre 2.2).

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

Sans objet.

4.5 Usage de la Bi-clé et du Certificat

4.5.1 Utilisation de la clé privée et du Certificat 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 indiqué au chapitre 1.5.1.1 du présent document. Dans le cas contraire, la responsabilité de l'AC OTU 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 l'AC OTU, 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 Causes possibles de renouvellement d'un Certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification de l'établissement du nouveau Certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau Certificat

Sans objet.

4.6.6 Publication du nouveau Certificat

Sans objet.

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

Sans objet.

4.7 Délivrance d'un nouveau Certificat suite à changement de la Bi-clé

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 Causes 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 Démarche d'acceptation du nouveau Certificat

Sans objet.

4.7.5 Publication du nouveau Certificat

Sans objet.

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

Sans objet.

4.8 Modification du Certificat

La modification de Certificat n'est pas autorisée par la présente PC/DPC.
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 Causes possibles de modification d'un Certificat

Sans objet.

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

Sans objet.

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

Sans objet.

4.8.4 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 des Certificats

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

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificat à usage unique

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

- les informations du Titulaire figurant dans le Certificat qui a été émis à son nom ne sont pas en conformité avec l'identité de celui-ci telles que reçues de l'Abonné ;
- la ou les informations concernant l'utilisation du Certificat figurant dans le Certificat ne sont pas en conformité avec celle(s) prévue(s) dans le cadre défini au chapitre 1.5.1.1 ;
- une erreur (intentionnelle ou non) est détectée dans la demande d'enregistrement du Titulaire ;
- 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 ;
- 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.

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 Certificat d'Organisation

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

- 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 présence 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).

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.

4.9.1.3 Certificat d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un Certificat d'une composante de l'IGC OTU (y compris le Certificat de l'AC OTU) :

- suspicion de compromission, compromission, perte ou vol de la clé privée ;

- changement de contenu nécessaire suite à une évolution (correction de non-conformité, évolution du gabarit de Certificat, …) ;
- cessation d'activité ;
- évolutions réglementaires sur les algorithmes utilisés.

Lorsqu'une des circonstances énoncée ci-dessus survient et que Worldline en a la connaissance, Worldline décide de la révocation du Certificat en question de la composante concernée de l'IGC OTU.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat 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 Certificat 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 OTU.

4.9.2.3 Certificat d'une composante de l'IGC

La révocation du Certificat de l'AC OTU ou des autres Certificats de composantes de l'IGC OTU ne peut être décidée que par Worldline ou par les autorités judiciaires suite à une décision de justice.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat 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 OTU 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 Certificat 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 OTU (cf. chapitre 4.9.5.2)

4.9.3.3 Certificat d'une composante de l'IGC

La demande de révocation de ce type de Certificat est automatiquement validée en raison de son origine. La procédure de traitement en cas de révocation d'un des Certificats d'une composante de l'IGC OTU est interne et dépend de la raison de la demande et de la nature du Certificat à révoquer.

4.9.4 Délai accordé pour formuler la demande de révocation

4.9.4.1 Certificat 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 Certificat 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.

4.9.4.3 Certificat d'une composante de l'IGC

Dès que le représentant habilité a connaissance d'une des causes possibles de révocation définies au chapitre 4.9.1.3 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 Certificat à usage unique

La demande de révocation d'un Certificat à usage unique est traitée immédiatement après sa réception par l'AC OTU. 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.

L'indisponibilité maximum de la plateforme est de huit (8) heures par mois.

4.9.5.2 Certificat d'Organisation

La demande de révocation d'un Certificat d'Organisation est traitée immédiatement après sa réception par l'AC OTU. 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.

L'indisponibilité maximum de la plateforme est de huit (8) heures par mois.

4.9.5.3 Certificat d'une composante de l'IGC

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

Une demande de révocation d'un Certificat d'une composante de l'IGC 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 Certificat à usage unique

Dans le cadre d'utilisation d'un Certificat à usage unique fourni par l'AC OTU, 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 Certificat d'Organisation

Dans le cadre d'utilisation d'un Certificat d'Organisation fourni par l'AC OTU, 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 conformément à ce qui est défini au chapitre 2.2 du présent document, soit effectuer une requête auprès du répondeur OCSP à l'adresse définie au chapitre susvisé.

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.

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 le Certificat de l'AC OTU, sa révocation suite à une compromission de la clé privée fait l'objet d'une information clairement diffusée sur le site web de l'AC OTU.

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 Fonction d'information sur l'état des Certificats

4.10.1 Caractéristiques opérationnelles

L'AC OTU met 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 OTU comme spécifié au chapitre 7.1 de la présente PC/DPC.

Une LCR contient la liste des Certificats émis par l'AC OTU 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 OTU 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 OTU comme spécifié au chapitre 7.1 de la présente PC/DPC.

L'AC OTU assure 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 l'AC OTU 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.

L'AC OTU demande 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.

4.12 Séquestre de clé et recouvrement

Le séquestre des clés privées de l'AC OTU 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

L'IGC OTU respecte une politique de sécurité de l'information et possède une politique de sécurité opérationnelle.

Ce dernier document, qui fixe notamment le cadre des règles de sécurité applicables aux systèmes de l'IGC, tient compte de l'état de l'art en la matière et fait l'objet d'une révision régulière en conformité avec l'Analyse de Risques effectuée par le responsable sécurité de l'IGC OTU. Elle est validée par le Comité Sécurité suite à sa révision qui intervient au maximum tous les vingt-quatre (24) mois.

5.1 Mesures de sécurité physique

Un ensemble de mesures de sécurité physique est mis en place par l'IGC OTU afin de garantir que :

- les moyens, systèmes d'informations et données utilisés dans le cadre de la mise en œuvre opérationnelle de l'IGC OTU sont installés dans des locaux sécurisés dont les accès sont contrôlés et réservés aux personnels strictement habilités ;
- le système de contrôle des accès permet de garantir la traçabilité des accès aux locaux hébergeant les moyens et informations de l'IGC OTU ;
- la mise en œuvre de ces contrôles permet de respecter la séparation des rôles de confiance telle que prévue dans la présente PC/DPC.

Ci-dessous figure un panel de mesures de sécurité physique mises en place selon différentes catégories. Des précisions sont apportées dans le document DTPC.

5.1.1 Situation géographique et construction des sites

L'IGC OTU est installée sur les sites Worldline de production informatique de Vendôme et de Bruxelles. Ces sites sont conçus pour héberger des systèmes informatiques et télécom. Ils respectent les exigences (règlements et normes) de construction en vigueur. Les équipes administratives et opérationnelles sont amenées à administrer et opérer sur les sites de Blois et de Seclin.

5.1.2 Accès physique

Les sites et locaux qui accueillent l'IGC OTU garantissent la sécurité des moyens de Certification.

Les sites de production informatique concernés disposent d'un contrôle d'accès au site et aux salles informatiques avec des définitions de groupes et de droits d'accès pour ces groupes par zone et par plage horaire.
Ces sites fonctionnent 7j/7 24h/24.

Les personnels sur site disposent de cartes avec pin-code pour l'accès aux zones qui leur ont été autorisées. En effet, il est obligatoire de posséder une carte d'accès pour pouvoir accéder aux locaux. Certaines zones plus sensibles font l'objet de mesures complémentaires comme un anti-passback et/ou la nécessité de faire intervenir deux (2) personnes pour l'ouverture du local.

Les serveurs de l'IGC OTU, avec leur carte HSM intégrée, sont installés dans des zones de haute sécurité nécessitant notamment l'authentification obligatoire de deux (2) personnes autorisées (dual control). Les sites de Vendôme et Bruxelles utilisent un dispositif d'authentification avec carte et données biométriques. La protection de ces zones est renforcé par d'autres mesures de sécurité physique telles que la présence de barrières infrarouges, de détecteurs de présences, d'un système de vidéosurveillance complémentaire et autonome et autres.

Le contrôle d'accès bâtiment est géré par des administrateurs locaux sur un serveur dédié. Celui-ci conserve également les journaux d'accès sur les différents lecteurs ainsi que les messages de service du contrôle d'accès.

Des mesures sont mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services de l'IGC OTU soient sortis du site sans autorisation.

5.1.3 Alimentation électrique et climatisation

Un certain nombre de mesures sont mis en place afin de parer aux pannes électriques et simplifier les interventions de maintenance. De même, des mesures sont mises en place pour parer à des défaillances au niveau du système de climatisation. L'ensemble de ces mesures permet d'assurer la continuité des services fournis par l'IGC OTU.

5.1.4 Vulnérabilité aux dégâts des eaux

Des moyens de surveillances (capteurs, monitoring, …) sont en place pour parer aux dégâts des eaux, permettant ainsi d'assurer la continuité des services fournis par l'IGC OTU.

5.1.5 Prévention et protection incendie

Des mesures de prévention et de lutte contre les incendies (détecteurs, portes coupe-feu, …) sont en place afin d'assurer la continuité des services fournis par l'IGC OTU.

5.1.6 Conservation des supports

Dans le cadre des activités de l'IGC OTU, une analyse de risque est réalisée sur son périmètre (cf. chapitre 9.17.2). Cette analyse de risque permet d'identifier les actifs et leurs besoins en termes de sécurité. Parmi ces actifs, sont identifiés différents supports (documents papiers, disques durs, …) qui sont alors conservés conformément aux besoins de sécurité définis. Les informations concernant les mesures mises en place sont détaillées dans la DTPC.

5.1.7 Mise hors service des supports

Tous les documents papier contenant des données confidentielles (PIN code, mot de passe, …) devenus inutiles ou obsolètes sont détruits à l'aide d'un broyeur.

Pour les supports physiques (disque, HSM, …) une procédure spéciale de stockage tampon en vue d'un broyage devant huissier est mise en place. Cette destruction donne lieu à la production d'un Procès-Verbal.

5.1.8 Sauvegardes hors site

Dans le cadre de la présente PC/DPC, l'IGC OTU met en place des sauvegardes hors site conformément aux procédures définies (cf. document [PESC]).

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

L'IGC OTU définit explicitement les rôles de confiance requis pour assurer le fonctionnement et la sécurité de celle-ci.
Les fonctions opérées sur toutes les composantes de l'IGC OTU sont réparties sur plusieurs types d'intervenants afin de veiller à la séparation des connaissances pour les tâches ou rôles sensibles. Les rôles de confiance intervenants dans l'Organisation de l'IGC OTU sont les suivants :

- Administrateur HSM : il est en charge des installations et configurations des boîtiers cryptographiques (HSM) de l'IGC OTU ;

- Administrateur système : il est en charge des installations, configurations et maintenances des systèmes de confiance de l'IGC OTU pour la gestion des services. Il est notamment responsable de l'exploitation quotidienne des systèmes de confiance de l'IGC OTU. Il est autorisé à effectuer les sauvegardes de ces systèmes ;

- Auditeur système : il est autorisé à consulter les archives et l'ensemble des données d'audit des systèmes de confiance de l'IGC ;

- Maître de cérémonie : il est en charge de gérer les opérations d'entrées, sorties ou destruction de clés (cérémonies de clés) dont il est le seul et unique point d'entrée ;

- Officier de sécurité : il est en charge d'administrer l'implémentation des pratiques de sécurité et d'appliquer les contraintes techniques définies dans l'analyse de risque ;

- Opérateur d'enregistrement : il est chargé d'intervenir dans le processus de création de Certificats ;

- Porteur de secrets : il assure la confidentialité, l'intégrité et la disponibilité des secrets. Il est dépositaire des secrets et des clés physiques d'accès à leurs coffres. Il est membre d'une équipe dont l'ensemble des membres dispose des mêmes droits sur les accès aux coffres ;

- Responsable d'application : il est en charge d'assurer le suivi du service et de ses performances. Il coordonne et/ou réalise la maintenance corrective et évolutive de l'application.

- Responsable de l'AC : il est en charge de la mise en œuvre de la présente PC/DPC ainsi que de la vérification de son application. Il est notamment en charge de la révocation d'un certificat émis par l'AC OTU. Membre du Comité Sécurité, il est aussi en charge de l'approbation du présent document, du document DTPC, de l'analyse de risque et de la politique de sécurité opérationnelle de l'IGC OTU ;

- Responsable adjoint de l'AC : il est en charge de la mise en œuvre de la présente PC/DPC ainsi que de la vérification de son application. Il est notamment en charge de la révocation d'un certificat émis par l'AC OTU. Membre du Comité Sécurité, il est aussi en charge de l'approbation du présent document, du document DTPC, de l'analyse de risque et de la politique de sécurité opérationnelle de l'IGC OTU ;

- Responsable de centre : il est responsable de l'application des procédures qui concerne le centre informatique accueillant les systèmes de l'IGC OTU. Il est notamment chargé d'intervenir pour permettre l'accès aux moyens de l'IGC OTU ;

- Responsable sécurité : il est en charge de la définition des règles et procédures de sécurité autour de l'IGC OTU en liaison avec l'AC OTU.

Lors de l'enrôlement d'un nouveau membre dans un rôle de confiance au sein de l'IGC OTU, un document actant de sa désignation doit être signé par la personne concernée. Ce document fait référence à la DTPC afin que le futur membre du personnel de confiance ait connaissance de la description de son rôle et des responsabilités qui lui sont affectées. Il spécifie notamment :

- les engagements du signataire et leur bonne compréhension ;

- en cas de modification du document DTPC, le signataire en sera informé.

De même, lors de la cessation d'un rôle de confiance au sein de l'IGC OTU, un document actant de la cessation doit être signé par la personne concernée.

Il est vérifié au moins une (1) fois par an que l'ensemble des rôles de confiance définis ci-dessus sont pourvus.

5.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et les rôles des personnes devant être présentes, en tant qu'acteurs ou témoins, peuvent être différents. En effet, certaines tâches sensibles, telles que la génération de Certificat initiale de l'AC OTU, nécessite plus d'une personne occupant un rôle de confiance au sein de l'IGC OTU pour des raisons de sécurité.

Certains rôles de confiances sont occupés par plusieurs personnes pour que l'IGC OTU puisse assurer la continuité de ses services sans dégrader la sécurité des services offerts.

5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC OTU vérifie, pour chacun de ses composants, l'identité et les autorisations de tout membre du personnel ainsi que d'éventuelles personnes extérieures intervenant sur les tâches sensibles. Ces contrôles sont conformes à la Politique de Sécurité Opérationnelle [PSO] appliquée par l'IGC OTU.

Chaque attribution d'un rôle de confiance à un membre du personnel de l'IGC OTU est notifiée et documentée par écrit.

5.2.4 Rôles exigeant une séparation des attributions

Dans le cadre du présent document, les rôles de confiance peuvent être assurés par plusieurs personnes physiques.
De plus, certains rôles peuvent être attribués à une même personne. Ces rôles sont définis dans la matrice qui figure ci-dessous :

	Administrateur HSM	Administrateur Système	Auditeur Système	Maître de cérémonie	Officier de sécurité	Opérateur d'enregistrement	Porteur de secrets	Responsable d'application	Responsable d'AC	Responsable Adjoint d'AC	Responsable de centre	Responsable sécurité
Administrateur HSM		✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗
Administrateur Système	✗		✗	✓	✓	✗	✓	✓	✓	✓	✓	✗
Auditeur Système	✗	✗		✗	✗	✗	✗	✗	✗	✗	✗	✗
Maître de cérémonie	✓	✓	✗		✓	✗	✓	✓	✓	✓	✓	✗
Officier de sécurité	✓	✓	✗	✓		✗	✓	✓	✓	✓	✓	✗
Opérateur d'enregistrement	✓	✗	✗	✗	✗		✗	✓	✓	✓	✓	✗
Porteur de secret	✓	✓	✗	✓	✓	✗		✓	✓	✓	✓	✗
Responsable d'application	✓	✓	✗	✓	✓	✓	✓		✓	✓	✓	✗
Responsable d'AC	✓	✓	✗	✓	✓	✓	✓	✓		✓	✓	✗
Responsable adjoint d'AC	✓	✓	✗	✓	✓	✓	✓	✓	✓		✓	✗
Responsable de centre	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓		✗
Responsable sécurité	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

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

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

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

5.3.2 Procédures de vérification des antécédents

Des procédures de vérification des antécédents judiciaires sont mises en place pour les personnes qui sont appelées à endosser un rôle de confiance au sein de l'IGC OTU. Ces personnes ne doivent notamment pas avoir fait l'objet de condamnation judiciaire susceptible de compromettre leur participation aux activités de l'IGC OTU, ni être en situation de conflit d'intérêt avec leurs attributions. Pour cela, les personnes concernées doivent remettre une copie du bulletin n°3 de leur casier judiciaire aux Ressources Humaines de Worldline lors de la signature du document (cf. chapitre 5.2.1) par lequel ils acceptent leur rôle, leurs obligations et leurs responsabilités dans le cadre de leur participation à ces activités.

Le dossier de candidature du postulant est soumis à la validation du service Ressources Humaines et à celle du responsable de l'Autorité de Certification OTU.

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

Les personnels chargés d'opérer les services de Certification ne sont pas chargés des aspects commerciaux liés à ces services et sont dégagés de tout conflit d'intérêts qui pourraient influencer la manière de mener les opérations dont ils sont chargés et obérer la confiance (cf. chapitre 9.17.1). A cet égard, ils s'engagent à confirmer par écrit, lors de leur acceptation du rôle de confiance au sein de l'IGC OTU, l'absence de tout conflit d'intérêt lié à l'exercice de cette nouvelle activité.

5.3.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures de fonctionnement de l'IGC OTU. Ce même personnel a pris la mesure et la connaissance de ce qui implique les opérations dont il a la responsabilité.

5.3.4 Exigences et fréquences en matière de formation continue

Le personnel reçoit la formation nécessaire préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation ou autres en fonction de la nature de ces évolutions. Il est notamment formé sur les enjeux en matière de sécurité des systèmes d'information et sensibilisé au traitement des incidents.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Le règlement intérieur de Worldline indique que des sanctions disciplinaires administratives appropriées sont applicables en cas de faute (non-respect de la présente PC/DPC, …). Ceci est notamment rappelé au personnel dans l'engagement de responsabilités qu'il accepte lors de l'acceptation de son rôle au sein de l'IGC OTU.

Les entités externes à Worldline et participantes aux activités de l'IGC OTU s'exposent à des sanctions définies lors de la contractualisation en cas de faute (non-respect de la présente PC/DPC, …).

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

Le personnel des éventuels prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC OTU doit respecter les exigences énoncées dans les chapitres 5.3.1 à 5.3.4 du présent document.

5.3.8 Documentation fournie au personnel

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

5.4 Procédures de constitution des données d'audit

Les évènements intervenant dans la vie de l'IGC OTU sont journalisés sous forme de fichiers à partir de générations automatisées par logiciel et complétées s'il y a lieu de saisies manuelles. Ces fichiers ont pour but d'assurer la traçabilité et l'imputabilité des opérations effectuées (auteurs, horodatages, …).

Le processus de journalisation est réalisé au fil de l'eau pour les systèmes automatiques et au plus tôt, dès l'initialisation de l'opération, pour les interventions manuelles.

Aucune opération manuelle ne peut être déclenchée sans l'initialisation d'un ticket de traçabilité.

Les journaux d'évènement comprennent explicitement l'identifiant de l'exécutant, logiciel ou humain, de l'opération.

Ils peuvent être mis à disposition de la justice lors d'une requête légale les requérants.

5.4.1 Type d'évènements enregistrés

Les évènements enregistrés dans les journaux d'évènements de l'IGC OTU sont les suivants :

- démarrages et arrêts des systèmes informatiques et des applications ;
- démarrages et arrêts des paramètres de la fonction de journalisation ;
- modifications des paramètres de la fonction de journalisation ;
- générations des clés pour les différents composants ;
- modifications (changement, correction ou évolution) des différents composants ;
- réceptions de demande de création de Certificat et de demande de révocation de Certificat ;
- traitements (validation ou rejet) de demande création de Certificat et de demande de révocation de Certificat ;
- générations et révocations des Certificats ;

- transmissions des Certificats à usage unique et des Certificats d'Organisation au Dispositif Porteur de Certificats ;
- générations et publications des Listes de Certificats Révoqués ;
- modifications (changement, correction ou évolution) de la présente PC/DPC, du document DTPC, de l'Analyse de Risque et de la Politique de Sécurité Opérationnelle.

De plus, des évènements propres à la sécurité sont aussi enregistrés dans les journaux d'évènements de l'IGC OTU. En voici une liste non-exhaustive :

- accès physiques dans les locaux hébergeant l'IGC OTU ;
- actions de changements sur la plate-forme technique (maintenance, évolution des logiciels) ;
- changements dans le personnel intervenant au sein de l'IGC OTU ;
- épurations ou destructions de Certificats expirés ;
- actions des Pilotes dans le cadre de la surveillance et du pilotage ;
- créations, modifications et suppressions de comptes utilisateurs et de données d'authentification correspondantes ;
- connexions et déconnexions des utilisateurs ayant un rôle de confiance au sein de l'IGC OTU (incluant les tentatives correspondantes soldées par un échec) ;
- évènements liés aux clés de signature et aux Certificats d'AC (générations lors d'une cérémonie de clés, sauvegardes, récupérations, révocations, renouvellements, destructions, …).

Les évènements journalisés reprennent l'ensemble des informations qui permettent de les identifier et de les analyser. Ces informations sont les suivantes :

- type d'évènements ;
- date et heure de l'évènement ;
- intervenants – composant logiciel ou intervention humaine ;
- contexte – opération planifiée avec demander, intervention opérationnelle effectuée suite à un dysfonctionnement, … ;
- résultat – échec ou réussite ;
- lien éventuels avec d'autres évènements.

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant opérée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements, comme définit ci-dessus.

5.4.2 Fréquence de traitement des journaux d'évènement

Les journaux d'évènements sont collectés au fil de l'eau et sont inspectés en temps réel.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements électroniques sont sauvegardés tous les jours pour une durée de trois (3) mois et sont archivés périodiquement (cf. chapitre 5.5.6) pour une durée définie au chapitre 5.5.2 du présent document.

Les journaux d'évènements manuscrits sont stockés et conservés comme défini au chapitre 5.5.2 de ce document.

5.4.4 Protection des journaux d'évènements

Les journaux d'évènements électroniques sont collectés puis externalisés vers deux types d'environnement dont les administrations sont différentes. L'accès à ces éléments sont donc rendus possible uniquement au personnel autorisé par l'IGC OTU comme défini dans le document DTPC et ne sont pas modifiables sans autorisation.

Les journaux d'évènements manuscrits sont protégés grâce à des systèmes physiques sécurisés (coffre-fort ou armoire forte).

5.4.5 Procédure de sauvegarde des journaux d'évènements

La procédure de sauvegarde des journaux d'évènements de l'IGC OTU est interne et est spécifiée dans le document DTPC.

5.4.6 Système de collecte des journaux d'évènements

La système de collecte des journaux d'évènements de l'IGC OTU est interne et est spécifiée dans le document DTPC.

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

Il n'y a pas systématiquement de notification de l'enregistrement d'un évènement au responsable de l'évènement.

5.4.8 Evaluation des vulnérabilités

L'analyse des journaux d'évènements est effectuée par un outil spécifié dans le document DTPC qui produit également un compte-rendu accessible à l'entité contrôleur pour analyse et suivi à intervalle régulier ou suite à une alerte lancée par ce même outil.

5.5 Archivage des données

Les données à archiver le sont conformément aux pratiques énoncées ci-dessous.

5.5.1 Types de données à archiver

L'archivage est réalisé par l'IGC OTU afin d'assurer la traçabilité et l'imputabilité des opérations. Les données à archiver sont différentes selon les entités.

5.5.1.1 Autorité de Certification et Autorité d'Enregistrement

Pour l'AC et l'AE de l'IGC OTU, les données archivées sont :

- les informations d'enregistrement ;
- les demandes de génération de Certificat ;
- les demandes de révocation de Certificat ;

- les Certificats et les Listes de Certificats Révoqués.

5.5.1.2 Plate-forme technique

Pour la plate-forme technique de l'IGC OTU, les données archivées sont :

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

5.5.1.3 Documentation

Pour la documentation de l'IGC OTU, les données archivées sont :

- les manuels de cérémonie de clés ;
- les versions et les révisions de la présente PC/DPC ;
- les versions et les révisions du document DTPC ;
- les versions et les révisions de l'Analyse de Risque ;
- les versions et les révisions de la Politique de Sécurité Opérationnelle.

5.5.2 Période de conservation des archives

5.5.2.1 Autorité de Certification et Autorité d'Enregistrement

Les archives des LCR sont conservées jusqu'à la fin de la vie de l'Autorité de Certification.

5.5.2.1.1 Certificat à usage unique

La durée de conservation des archives des dossiers d'enregistrement est de huit (8) ans à compter du moment où la validation du dossier par l'Autorité d'Enregistrement et la clôture de traitement du dossier par l'Abonné ont été acquises.

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 huit (8) ans. 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.

Les demandes de création et de révocation de Certificats sont conservées huit (8) ans à compter de leur réception.

5.5.2.1.2 Certificat d'Organisation

La durée de conservation des archives des dossiers d'enregistrement est de dix (10) ans à compter du moment où la validation du dossier par l'Autorité d'Enregistrement et la clôture de traitement du dossier par l'Abonné ont été acquises.

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 dix (10) ans. 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.

Les demandes de création et de révocation de Certificats sont conservées dix (10) ans à compter de leur réception.

5.5.2.2 Plate-forme technique

La durée de conservation des journaux d'évènements est de dix (10) ans à partir de leur création.

5.5.2.3 Documentation

La durée de conservation des archives documentaires est de dix (10) ans après la dernière émission d'un Certificat par l'AC OTU avant sa cessation d'activité.

5.5.3 Protection des archives

Durant leur période de rétention au sein des locaux sécurisés de l'IGC OTU, les archives sont protégées en intégrité et ne sont accessibles qu'aux personnes habilitées. En effet, la demande d'accès à une archive ne peut être uniquement faite que par le responsable de l'Autorité de Certification, un responsable adjoint de l'Autorité de Certification ou l'officier sécurité de l'IGC OTU afin d'assurer la confidentialité des informations.

Des procédures sont en place afin de parer à l'obsolescence et à la détérioration des archives. Celles-ci sont notamment stockées dans des locaux sujets à des mesures de protection contre les dangers naturels.

5.5.4 Procédure de sauvegarde des archives

Le niveau de protection des archives est équivalent au niveau de protection des sauvegardes. Les procédures de sauvegarde des archives sont internes et sont spécifiées dans le document DTPC.

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

Les archives sont produites une (1) fois par mois. Le procédé mis en œuvre pour collecter les archives est interne et est spécifié dans le document DTPC.

5.5.7 Procédure de récupération et de vérification des archives

Les archives peuvent être récupérées dans un délai inférieur à deux (2) jours ouvrés à compter de l'enregistrement de la demande. L'accès aux archives est sujet à des restrictions (cf. chapitre 5.5.3).

5.6 Changement de clé d'AC

L'Autorité de Certification OTU ne peut émettre de Certificats dont les dates de validité (début ou fin) dépassent la date d'expiration du Certificat avec lequel elle souhaiterait émettre le Certificat.

Dans le cas où l'un des Certificats de l'AC OTU arriverait à expiration, il sera renouvelé dans l'année précédant sa date d'expiration afin d'assurer la continuité des opérations des entités utilisant le Certificat en question.

Dès qu'une nouvelle Bi-clé de l'AC OTU est générée et opérationnelle, seule la nouvelle clé privée est utilisée pour signer des Certificats.

Le Certificat précédent n'est alors plus utilisable dans le cadre qui lui a été défini : signature de Certificats et de LCR (cf. chapitre 0). Cependant, il reste accessible pour valider les Certificats signés avec la clé-privée correspondante jusqu'à ce que le dernier de ces Certificats soit expiré.

L'AC OTU ne peut réutiliser la Bi-clé précédemment en vigueur qu'elle aurait fait re-certifié auprès de l'Autorité de Certification Racine pour une nouvelle période de validité.

5.7 Reprise suite à compromission et sinistre

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

L'AC OTU prend les mesures techniques et Organisationnelles adéquates (formation du personnel, guide de procédures opérationnelles, …) pour gérer les risques liés à la sécurité des services de confiance fournis. Ces mesures garantissent un niveau de sécurité proportionnel au degré de risque.

Ces mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents.

En cas d'incident, l'IGC OTU se réfère à la DTPC et à la Politique de Gestion des Incidents de Worldline [PGI] permettant la remontée et le traitement de ceux-ci. De plus, l'IGC OTU prend les mesures nécessaires, dans la mesure du possible, pour éviter une récidive comme indiqué dans la Politique de Sécurité Opérationnelle [PSO].

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

Si le matériel de l'IGC OTU est endommagé ou hors service alors que les clés de signatures ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant priorité à la capacité de fourniture des services de révocation et de publication d'état de validité des Certificats. En effet, afin d'assurer la continuité dans la fourniture de ses services, l'IGC OTU met en place un plan de continuité et de reprise d'activité [PCRA].

Un test de simulation d'incident avec arrêt de service d'une composante de l'IGC OTU est régulièrement réalisé.

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

Le cas de compromission d'une clé d'infrastructure ou d'un algorithme est traité via les procédures de gestions des incidents et via le plan de continuité et de reprise d'activité de l'IGC OTU [PCRA]. Ce plan est appliqué dès lors où l'IGC OTU a connaissance du cas.

Ce plan adresse entre autre les points qui suivent, si la clé privée de l'AC OTU est compromise ou est soupçonnée de l'être, si elle est détruite ou encore si l'algorithme utilisé est compromis :

- après enquête sur l'évènement, Worldline décide de la révocation ou non du Certificat concerné de l'AC OTU ;
- s'il est décidé de révoquer le Certificat concerné de l'AC OTU :

- l'AC OTU assure la continuité de ses services comme décrit dans le plan de continuité et de reprise d'activité [PCRA] ;
- tous les Certificats délivrés par l'AC OTU et signés avec la clé privée concernée sont révoqués.

- si un algorithme est compromis, il est alors remplacé ;
- une nouvelle Bi-clé est générée et un nouveau Certificat d'AC correspondant est émis ;
- Worldline statue sur le plan de communication à destination :
  - des Autorités qui accréditent le Certificat en question (Adobe, …) ;
  - des Abonnés et des utilisateurs de Certificats de l'AC OTU.

5.7.4 Capacités de continuité suite à un sinistre

En cas de sinistre, l'IGC OTU possède les capacités nécessaires et suffisantes afin d'assurer la continuité de ses services comme défini dans le plan de continuité et de reprise d'activité [PCRA]. Suite à un sinistre, ce plan est mis en place afin de restaurer les services impactés.

5.8 Fin de vie de l'IGC

L'IGC OTU ne transfère pas les activités de l'AC OTU vers un tiers.

Dans le cas où l'IGC OTU déciderait d'interrompre définitivement ses activités, un plan de cessation d'activité serait alors appliqué. Ce plan comprend entre autre les points suivants :

- information de la décision de l'IGC OTU aux personnes concernées (organes de contrôle tels que l'ANSSI, partenaires, Abonnés) avant la cessation de ses activités en respectant un préavis ;
- informations aux représentants d'Abonnés et aux entités concernées de la prochaine révocation de leur(s) Certificat(s) préalablement fournis par l'AC OTU ;
- révocation et gestion du statut de révocation pour les Certificats non-expirés émis par l'AC OTU ;
- destruction des bi-clés (nominales et sauvegardes) et des secrets associés ;
- cessation de la contractualisation avec les Abonnés ;
- transfert de ses obligations à Worldline.

Le plan de cessation d'activité de l'IGC OTU est régulièrement revu et maintenu à jour.

Dans le cas où l'IGC OTU ferait faillite, celle-ci se raccroche à Worldline afin de couvrir ses obligations de fin de vie.

6 Mesures de sécurité techniques

6.1 Génération et installation de Bi-clés

6.1.1 Génération des Bi-clés

Dans l'ensemble des cas explicités ci-dessous, la clé privée d'une entité est toujours produite par l'entité elle-même. Par ailleurs, aucune transmission de clé privée n'est autorisée.

6.1.1.1 Clés d'AC

La génération des Bi-clés de l'AC OTU est réalisée au cours d'une cérémonie de clés. Ces cérémonies de clés se déroulent :

- au sein d'un module cryptographique physiquement isolé répondant aux exigences définies au chapitre 6.2.1.1 du présent document ;
- dans les locaux sécurisés de l'IGC OTU (cf. chapitre 5.1) ;
- sous le contrôle permanent d'au moins deux (2) personnes occupant un rôle de confiance au sein de l'IGC OTU parmi : le porteur de secrets, le maître de cérémonie, l'administrateur HSM et le responsable d'application (cf. chapitre 5.2.1) ;
- suivant un document Organisationnel et un document technique tous deux signés par l'ensemble des participants, notamment par le maître de cérémonie.

La clé privée de l'AC OTU est mise en œuvre et reste dans les locaux sécurisés de l'IGC OTU définis au chapitre 5 du présent document.

6.1.1.2 Clés d'authentification d'une composante de l'IGC

Les clés d'authentification d'une composante de l'IGC OTU sont générées lors d'une cérémonie de clés. Cela peut être effectué en même temps que pour les clés d'AC. Cette cérémonie se déroule dans les mêmes conditions que celles décrites au chapitre 6.1.1.1 ci-dessus.

6.1.1.3 Clés d'authentification de l'Abonné

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

L'IGC OTU ne produit pas les Certificats 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 Clés des Certificats porteur générées par l'AC

L'Autorité de Certification OTU ne génère pas les clés des Certificats porteurs.

6.1.1.5 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 6.2.1.1 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 de l'IGC OTU (cf. chapitre 5.1)	
Sous le contrôle du Dispositif Porteur de Certificat	Sous le contrôle de deux (2) personnes occupant un rôle de confiance au sein de l'IGC OTU
Suivant un script préalablement défini par l'AC OTU	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 l'IGC OTU 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.

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 OTU 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 de l'AC OTU sont publiés sur son site web dont l'adresse est définie au chapitre 2.2 du présent document.

6.1.5 Taille des clés

La taille des clés et les algorithmes utilisés sont conformes aux exigences [ETSI TS 119 312].

Bi-clés	Algorithme	Fonction de hachage	Taille (bits)
Certificats de l'AC OTU	RSA	SHA-2	2048
Certificats à usage unique	RSA	SHA-2	2048
Certificats d'Organisation	RSA	SHA-2	2048
Certificats à usage unique de test	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

La génération des Bi-clés de l'AC OTU est réalisée conformément à ce qui est détaillé au chapitre 6.1.1.1 du présent document. Les paramètres de l'équipement de génération de Bi-clés (module cryptographique) sont décrits dans le document Organisationnel de cérémonie de clés.

Dans le cas d'un Certificat à usage unique ou d'un Certificat d'Organisation, les caractéristiques de la Bi-clé sont vérifiées par l'AC OTU avant toute émission dudit Certificat.

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

Les modules cryptographiques (HSM) utilisés par l'IGC OTU, pour la génération des Bi-clés de l'AC OTU et des Bi-clés correspondantes aux différents Certificats délivrés par l'AC OTU, sont des modules cryptographiques (HSM) certifiés répondant aux exigences de qualification définies au chapitre 6.2.11 du présent document.

L'IGC OTU s'assure de la sécurité des HSM qu'elle utilise tout au long de leur cycle de vie. Des procédures sont notamment mises en place pour :

- s'assurer de l'intégrité de ces HSM durant leur transport ;
- s'assurer de l'intégrité de ces HSM durant leur stockage ;
- s'assurer du bon fonctionnement de ces HSM.

6.2.1.2 Dispositifs cryptographiques des bénéficiaires

Sans objet.

6.2.2 Contrôle de la clé privé

6.2.2.1 Clés d'AC

Le contrôle des clés privées de l'AC OTU et des copies de sauvegarde correspondantes est assuré par du personnel de confiance : porteur de secrets et administrateur système (cf. chapitre 5.2.1) ; dans un environnement protégé. Ce contrôle est assuré à l'aide de données d'activations, appelées « secrets », réparties entre plusieurs personnes ayant différents rôles de confiance.

6.2.2.2 Clés des Certificats porteurs

Le contrôle des clés privées correspondantes aux différents Certificats délivrés par l'AC OTU est assuré par le Dispositif Porteur de Certificats qui en a le contrôle exclusif.

6.2.3 Séquestre de la clé privée

Sans objet.

6.2.4 Copie de secours de la clé privée

6.2.4.1 Clés d'AC

Les Bi-clés de l'AC OTU sont sauvegardées sous le contrôle de plusieurs personnes au cours d'une cérémonie de clés. Les sauvegardes des clés privées sont réalisées :

- dans les locaux sécurisés de l'IGC OTU ;
- sous le contrôle permanent d'au moins deux (2) personnes occupant un rôle de confiance au sein de l'IGC OTU parmi : le porteur de secrets, le maître de cérémonie, l'administrateur HSM et le responsable d'application (cf. chapitre 5.2.1) ;
- à l'aide de ressources cryptographiques matérielles (HSM) physiquement isolés répondant aux exigences définies au chapitre 6.2.1.1 du présent document ;
- conformément à la procédure de sauvegarde figurant dans le document technique de cérémonie de clés.

Les procédures de sauvegardes sont opérées selon les spécifications du fournisseur des matériels cryptographiques (HSM) de l'AC OTU.

Le nombre de copies est limité au minimum requis pour assurer la continuité des services de l'IGC OTU.

6.2.4.2 Clés des Certificats porteurs

Seule la clé privée des Certificats d'Organisation fait l'objet d'une copie de secours au cours de la cérémonie de création du Certificat. La sauvegarde est réalisée :

- dans les locaux sécurisés de l'IGC OTU ;
- sous le contrôle de deux (2) personnes occupant un rôle de confiance au sein de l'IGC OTU : porteur de secrets et opérateur d'enregistrement (cf. chapitre 5.2.1) ;
- à l'aide de ressources cryptographiques matérielles (HSM) physiquement isolés répondant aux exigences définies au chapitre 6.2.1.1 du présent document ;
- conformément à la procédure de sauvegarde figurant dans le document technique de cérémonie de clés.

Le nombre de copies est limité au minimum requis (2) pour assurer la continuité des services de l'IGC OTU.

6.2.5 Archivage de la clé privée

Sans objet.

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

6.2.6.1 Clés d'AC

Les clés privées de l'AC OTU sont générées dans son HSM et ne sont transférées vers un autre module cryptographique qu'uniquement dans le cas des copies de sauvegarde (cf. chapitre 6.2.4.1).

Lors d'un transfert, la clé privée est chiffrée avec un algorithme préconisé par le constructeur de HSM permettant d'assurer la sécurité de l'information. La clé privée de l'AC chiffrée ne peut alors pas être déchiffrée sans l'utilisation de composants cryptographiques matériels et sans l'action des personnes identifiées dans les rôles de confiances nécessaires.

6.2.6.2 Clés des Certificats porteurs

Sans objet.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées de l'AC OTU sont stockés au sein d'un module cryptographique physiquement isolé répondant aux exigences définies au chapitre 6.2.1.1 du présent document. Il en est de même pour le stockage des copies de sauvegarde des clés privées de l'AC OTU.

6.2.8 Méthodes d'activation de la clé privée

6.2.8.1 Clés privées d'AC

Les clés privées de l'AC OTU ne peuvent être activées qu'avec des données d'activation détenues par deux (2) personnes occupant un rôle de confiance au sein de l'IGC OTU.

L'activation d'une clé privée de l'AC OTU ne peut se faire qu'au cours d'une cérémonie de clé, documentée et tracée.

6.2.8.1 Clés privées des 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 OTU lors de la session de signature.

6.2.8.2 Clés privées des 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

La désactivation des clés privées de l'AC OTU dans le module cryptographique est automatique dès qu'il y a arrêt ou déconnexion du module.

6.2.9.2 Clés privées des Certificats à usage unique

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

6.2.9.3 Clés privées des 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 signature ou dès qu'il y a arrêt ou déconnexion du module.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'AC

Les clés privées de l'AC OTU et les copies de sauvegarde correspondantes sont détruites par effacement sur la ressource cryptographique matérielle. Les opérations de destruction sont effectuées au cours d'une procédure auditée de type cérémonie de clés.
Détruire les clés privées de l'AC OTU ou les copies de sauvegarde correspondantes dans le HSM requiert de détruire les clés présentes à l'intérieur du module cryptographique matériel. Les fonctions de remise à zéro qui lui sont spécifiques sont alors utilisées, de telle manière qu'aucune information ne peut être utilisée pour restaurer ne serait-ce qu'une partie des clés privées. Si les fonctions nécessaires à la destruction des clés de l'AC OTU ne sont pas ou plus accessibles sur le HSM, alors celui-ci est physiquement détruit.

En fin de vie normale ou anticipée (pour cause de révocation) d'une clé privée de l'AC OTU, celle-ci est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer. Par ailleurs, dans le cas où la ressource cryptographique matérielle hébergeant les clés privées de l'AC OTU doit être mise hors service, alors celles-ci le sont aussi.

6.2.10.2 Clés privées des 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.

6.2.10.3 Clés privées des Certificats d'Organisation

Sans objet.

6.2.11 Niveau de qualification du module cryptographique

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

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

6.3 Autres aspects de la gestion des Bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC OTU sont archivées conformément au chapitre 5.5.2.1 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].

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

Bi-clés	Durée de vie
Certificats de l'AC OTU	10 ans
Certificats à usage unique	15 minutes
Certificats d'Organisation	3 ans
Certificats à usage unique de test	15 minutes

Certificats d'Organisation de test	3 ans

6.3.3 Inventaire des clés

Un inventaire est réalisé par l'AC OTU de manière à vérifier que toutes les clés privées produites par l'AC OTU 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 de l'AC

Les données d'activation des clés privées de l'AC OTU sont générées dans un module cryptographique (cf. chapitre 6.2.2.1) durant les cérémonies de clés sous le contrôle de deux (2) personnes dans des rôles de confiance, stockées sur des cartes à puces puis sont remises aux porteurs de secrets qui détiennent alors les données d'activation (cf. chapitre 6.2.8.1). Ces données d'activations ne sont connues que par les responsables nommément identifiées dans le cadre du rôle de confiance qui leur est attribué.

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

Sans objet.

6.4.2 Protection des données d'activation

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

Les données d'activation sont protégées par des mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de secret sont responsables de la protection des secrets dont ils ont la responsabilité. Un Porteur de secret ne détient pas plus d'une donnée d'activation de l'AC.

6.4.2.2 Protection des données d'activation correspondant à la clé privée du 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

Les exigences minimales de sécurité technique mises en œuvre par l'IGC OTU répondent aux objectifs suivants :

- identification et authentification forte des utilisateurs pour l'accès au système ;
- gestion de sessions d'utilisation : déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur ;
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- gestion des comptes et droits des utilisateurs ;

- protection du réseau contre toute intrusion d'une personne non-autorisée ;
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- fonctions d'audits : non-répudiation, imputabilité et nature des actions effectuées ;
- application de procédures de changement pour les actions de livraison, modification et résolution urgente de problèmes logiciels ;
- application de procédures de changement pour toute modification des configurations logicielles ;
- redondance des connexions réseau pour assurer l'accessibilité en cas de panne simple.

Des dispositifs de surveillance, avec enregistrement et alarme automatique, ainsi que des procédures d'audit des paramétrages du système, en particulier des éléments de routage, et des procédures de réaction en cas d'incident sont mis en place.

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

L'implémentation, la configuration et toute modification ou mise à jour d'un système permettant de mettre en œuvre les composantes de l'IGC est documentée et contrôlée.

6.6.2 Mesures liées à la gestion de la sécurité

Toute évolution d'un système d'une composante de l'IGC OTU 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

Sans objet.

6.7 Mesures de sécurité réseau

L'IGC OTU n'est pas en contact direct avec des réseaux ouverts. Les passerelles permettant les accès sont protégées contre des tentatives d'intrusion ou d'attaque.
Des tests de pénétration sont effectués lors de la mise en place de l'infrastructure puis à chaque évolution ou modification majeure et des tests de vulnérabilité sont régulièrement effectués.
Ces passerelles limitent les services ouverts et protocoles aux seuls services indispensables au fonctionnement de l'IGC OTU. Elles sont régulièrement mises à jour pour prendre en compte les évolutions des systèmes anti-intrusions et combler les failles de sécurité potentielles dès leur identification par la communauté des utilisateurs des réseaux.

La configuration des systèmes est réalisée en enlevant les comptes, applications, services, protocoles et ports non-utilisés.

Les composants critiques du réseau sont maintenus dans un environnement sécurisé et leurs configurations sont périodiquement auditées en vue de leur conformité avec les exigences spécifiées par la présente PC/DPC.

L'AC Racine est stockée dans une zone hautement sécurisé et n'est éveillée que si nécessaire.

6.8 Horodatage / Système de datation

Les évènements sont datés avec l'heure système des serveurs de l'IGC OTU. Les horloges des systèmes de l'IGC OTU sont synchronisées entre-elles par rapport à une source fiable de temps (UTC) toutes les 24h.

7 Profils des Certificats, OCSP et des LCR

7.1 Profil des Certificats

7.1.1 Définitions

Les Certificats émis par l'AC OTU, y compris les siens, 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 Certificats 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 : AC OTU

7.1.2.1 Champs et valeurs de base

Champs	Valeur
Version	V3 (valeur : 2)
Serial number	Généré automatiquement lors de la Cérémonie de Clé
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	DN de l'AC Racine
Validity	10 ans
Subject	DN de l'AC Technique (cf. chapitre 0)
Subject Public Key Info	RSA 2048 bits

7.1.2.2 Extensions du Certificat

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
Basic Constraint	Certificate Authority	Non	vrai
	Maximum Path Length		0
Certificate Policies	policyIdentifier	Non	anyPolicy (2.5.29.32.0)
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		Non	Non utilisée
Issuer Alternative Name		Non	Non utilisée
CRL Distribution Points		Non	http://root.mediacert.com/LatestCRL[2]
Authority Information Access		Non	Non utilisée

[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.

7.1.3 Certificat à usage unique

7.1.3.1 Champs de base

Champs		Valeur
Version		V3 (valeur : 2)
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 [3]	Numéro de série unique du DN
	CN	Identité du titulaire formée de telle manière : Prénom du Titulaire [espace] Nom du Titulaire [espace] [TraceID] [4]
Subject Public Key Info		RSA 2048 bits

7.1.3.2 Extensions du Certificat

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	1.2.250.1.111.17.0.3.1
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		Non	Non utilisée
Issuer Alternative Name		Non	Non utilisée
Extended Key Usage		Non	Non utilisée
CRL Distribution Points		Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [5]
Authority Information Access	ocsp	Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [5]
	calssuers		http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [5]

[3] 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.

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

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

7.1.4 Certificat d'Organisation

7.1.4.1 Champs de base

Champs		Valeur
Version		V3 (valeur : 2)
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 [6]	Identifiant de l'Organisation formé de telle manière : ICD [espace] Identifiant de l'Organisation
	SN [7]	Nom de l'individu habilité dans l'Organisation
	GN [7]	Prénom de l'individu habilité dans l'Organisation
	OU [7]	Nom de l'unité dans l'Organisation
	OU	Nom de l'Abonné
	SERIALNUMBER [8]	Numéro de série unique du DN
	CN	Identité de l'Organisation
Subject Public Key Info		RSA 2048 bits

7.1.4.2 Extensions du Certificat

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	1.2.250.1.111.17.0.3.2
	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
Issuer Alternative Name		Non	Non utilisée
Extended Key Usage		Non	Non utilisée
CRL Distribution Points		Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [9]
Authority Information Access	ocsp	Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [9]
	calssuers		http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [9]

[6] 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.
[7] 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.
[8] 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.
[9] Cette URL est donnée à titre indicatif. L'URL qui fait foi est celle qui figure dans le Certificat.

7.1.5 Certificat à usage unique de test

7.1.5.1 Champs de base

Champs		Valeur
Version		V3 (valeur : 2)
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 [10]	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] [11]
Subject Public Key Info		RSA 2048 bits

7.1.5.2 Extensions du Certificat

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	1.2.250.1.111.17.0.3.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		Non	Non utilisée
Issuer Alternative Name		Non	Non utilisée
Extended Key Usage		Non	Non utilisée
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]
	calssuers		https://pki-otu-ac[SERIALNUMBER ACT

[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.

			émettrice].mediacert.com/certificate [12]

7.1.6 Certificat d'Organisation de test

7.1.6.1 Champs de base

Champs		Valeur
Version		V3 (valeur : 2)
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 [14]	Prénom de l'individu habilité dans l'Organisation
	OU [14]	Nom de l'unité dans l'Organisation
	OU	Identité de l'Abonné
	SERIALNUMBER [15]	Numéro de série unique du DN
	CN	TEST Identité de l'Organisation [16]
Subject Public Key Info		RSA 2048 bits

7.1.6.2 Extensions du Certificat

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	1.2.250.1.111.17.0.3.4
	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
Issuer Alternative Name		Non	Non utilisée
Extended Key Usage		Non	Non utilisée
CRL Distribution Points		Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/crl [17]
Authority Information Access	ocsp	Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [17]
	calssuers		http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [17]

[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] Le mot « TEST » et l'identité de l'Organisation ne sont pas séparés par un espace.
[17] Cette URL est donnée à titre indicatif. L'URL qui fait foi est celle qui figure dans le Certificat.

7.2 Profil des LCR

7.2.1 Champs de base

Champs		Valeur
Version		V2 (valeur : 1)
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 [18]
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 de LCR

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
Issuer Alternative Name	Non	Non utilisée
Delta CRL Indicator	Oui	Non utilisée
Fresh CRL	Non	Non utilisée

7.2.3 Extensions d'entrée de LCR

Champs	Critique	Valeur
Reason Code	Non	[RFC 5280] : code correspondant à la raison de révocation correcte
Invalidity Date	Non	Non utilisée
Certificate Issuer	Non	Non utilisée

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

7.3 Profil des OCSP

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

Champs		Valeur
Version		V3 (valeur : 2)
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 [19]	Numéro de série unique du DN
	CN	Service OCSP PKI OTU
Subject Public Key Info		RSA 2048 bits

7.3.2 Extensions du Certificat

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	1.2.250.1.111.17.0.3
	policyQualifierId		1.3.6.1.5.5.7.2.1
	qualifier		https://www.mediacert.com
Subject Alternative Name		Non	Non utilisée
Issuer Alternative Name		Non	Non utilisée
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
Authority Information Access	ocsp	Non	http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/ocsp [20]
	calssuers		http://pki-otu-ac[SERIALNUMBER ACT émettrice].mediacert.com/certificate [20]

[19] 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.

[20] 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 procède à un audit de conformité à la PC/DPC en vigueur lors de la mise en œuvre opérationnelle d'une composante de l'IGC OTU et lors de toute modification significative au sein d'une composante par un organisme accrédité.

Worldline procède à un audit externe de Certification à la norme [ETSI EN 319 411-1] de l'IGC OTU tous les deux ans par un organisme accrédité.

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

8.2 Identités / qualifications des évaluateurs

8.2.1 Audit externe

Le contrôle de la composante est effectué par une équipe d'auditeurs faisant partie d'un organisme d'audit habilité et accrédité à procéder à des évaluations selon les spécifications de [ETSI EN 319 411-1].

8.2.2 Audit interne

Le contrôle de la composante est effectué par une équipe indépendante de l'IGC OTU en charge des contrôles de conformité.

8.3 Relations entre évaluateurs et entités évaluées

8.3.1 Audit externe

Le ou les évaluateurs effectuant le contrôle de la ou des composantes de l'IGC OTU doivent être indépendants et exempt de tout conflit d'intérêts.

8.3.2 Audit interne

Le ou les évaluateurs effectuant le contrôle de la ou des composantes de l'IGC OTU ne doivent pas avoir un quelconque rôle de confiance au sein de la composante de l'IGC qui est évaluée.

8.4 Sujets couverts par les évaluations

Les contrôles effectués par les auditeurs portent sur une partie ou sur l'ensemble des composantes de l'IGC OTU afin de contrôler le respect de la mise en œuvre de la présente PC/DPC ainsi que la conformité des procédures et pratiques de l'AC OTU vis-à-vis des exigences auxquelles elle est sujette.

A cet égard, avant chaque audit, l'évaluateur responsable de l'audit envoie à l'IGC OTU un plan d'audit, spécifiant les composantes et procédures qu'il souhaitera contrôler lors de l'audit avec son ou ses confrères ainsi que le programme détaillé de l'audit.

8.5 Actions prises suite aux conclusions des évaluations

A l'issue d'une évaluation, l'équipe d'audit rend à Worldline son avis parmi les possibilités suivantes :

- réussite : l'audit n'a relevé aucune non-conformité et aucune action nouvelle n'est à mener. Worldline confirme la conformité de la composante auditée aux engagements du présent document et aux pratiques annoncées ;

- à confirmer : l'audit a relevé une ou plusieurs non-conformités non-bloquantes. Worldline doit alors présenter un plan d'actions correctives avec un délai de réalisation. Un nouveau contrôle pourra être effectué pour vérifier la mise en place des corrections ;

- échec : l'audit a relevé une ou plusieurs non-conformités bloquantes. L'équipe d'audit émet alors des recommandations à Worldline qui peuvent être la cessation temporaire ou définitive d'activité, la révocation du Certificat de l'AC, etc. Le choix de la mesure à appliquer appartient à Worldline.

8.6 Communication des résultats

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de Certification en charge de la Certification de l'IGC OTU.

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 de 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

Worldline dispose auprès d'une compagnie notoirement solvable, d'une police d'assurance garantissant les dommages pouvant survenir à ses biens, son personnel, ainsi qu'une police couvrant sa responsabilité professionnelle dans le cadre des prestations fournies.

9.2.2 Autres ressources

Worldline dispose des ressources financières pour assurer la fourniture des services de l'IGC OTU.

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

Les informations suivantes sont considérées comme confidentielles :

- les informations techniques relatives à la sécurité des fonctionnements des modules cryptographiques et de certaines composantes de l'IGC ;
- les clés privées de l'AC OTU, de ses composantes et des Certificats émis ;
- les données d'activation des clés privées de l'AC OTU ;
- le document DTPC ;
- les procédures internes d'exploitation ;
- le plan de continuité et de reprise d'activité ;
- le plan de cessation d'activité ;
- les journaux d'évènements ;
- les dossiers d'enregistrements ;
- les rapports d'audit ;

Seules les personnes habilitées par Worldline et ayant le besoin ou l'autorisation d'en connaître le contenu ont la possibilité de consulter, à la demande, les informations confidentielles susvisées. Cette demande doit être transmise au responsable de l'AC OTU ou à un de ses adjoints qui donnera, ou non, son approbation à la requête qui lui a été fournie.

9.3.2 Informations hors du périmètre des informations confidentielles

Les informations de l'IGC OTU considérées comme publiques et donc non-confidentielles sont rendues accessibles comme défini au chapitre 2.2 du présent document.

9.3.3 Responsabilités en terme de protection des informations confidentielles

9.3.3.1 Législation applicable

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 l'IGC OTU soient protégées de toute compromission, atteinte à la sécurité ou perte d'intégrité qui pourrait avoir une incidence importante sur le service de confiance fourni et les données à caractère personnel qui y sont conservées.

A cet effet, l'IGC OTU 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 OTU

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 de l'IGC OTU par les Abonnés ou leur représentant.

9.3.3.2.1 Certificat 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, avant de transmettre les données personnelles de ces futurs Titulaires à l'Autorité d'Enregistrement de l'IGC OTU, 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.

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 du futur Titulaire préalablement informé des conséquences de son choix et disposant des moyens de l'exercer.

Il est en effet 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 OTU 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.

9.3.3.2.2 Certificat 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 attachées 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, acceptent 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 Droit d'accès aux données

Conformément à l'Article 40 de la loi informatique et libertés modifiée par LOI n°2016-1321 du 7 octobre 2016 - art. 63 ,Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé auxdites opérations.

En conséquence de ce qui précède, les personnes qui ont donné leur consentement préalable au traitement de leurs données personnelles par l'IGC OTU comme exposé ci-dessus peuvent, conformément à la loi, accéder à l'ensemble des informations les concernant, détenues par l'Autorité d'Enregistrement et en obtenir la copie.

Cependant, il est rappelé que, s'agissant 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 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 pour les données personnelles des représentants d'Abonnés et des

représentants d'Organisation qui doivent être maintenues et conservées par l'Autorité d'Enregistrement pendant la durée définie au chapitre 5.5.2 du présent document.
En outre, il est rappelé que ces mêmes données personnelles pourront être rectifiées, complétées ou mises à jour sur demande de la personne concernée par ces données, sous réserve que les données personnelles ayant servi à l'identification et l'authentification de cette personne, communiquées au cours du processus de signature électronique ou de la constitution du dossier d'enregistrement restent dans l'historique de traces de la transaction et de la signature électronique opérée ou de la demande de création de Certificat d'Organisation, ceci jusqu'à l'épuisement de la finalité pour laquelle ces données personnelles ont été collectées et les traitements opérés.
Ces réserves constituent une restriction aux droits prévus dans l'article 40 et s'appuient sur les finalités qui justifient les traitements de ces données dans le cadre des prestations de services de confiance.
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 OTU, 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 de l'AC OTU, adresse présente au chapitre 1.6.2 de ce document ou présente sur le site web de l'AC OTU (cf. chapitre 2.2), accompagné d'une copie d'une pièce d'identité. Idéalement, en recommandé avec accusé de réception.

9.3.3.4 Condition 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 OTU 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

Worldline veille à la protection des données personnelles qu'elle détient ou est amenée à détenir, conformément aux règles susvisées relatives à la protection des données personnelles en vigueur sur le territoire à partir duquel elle exerce ses prestations de service.

A cet effet, l'Autorité d'Enregistrement de l'IGC OTU 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), comme des informations à caractère personnel.

Ces données sont protégées suivant la loi française nationale applicable à ses prestations laquelle en France, s'inscrit en conformité à la réglementation Européenne.

Ainsi, conformément au règlement e-IDAS, l'IGC OTU prend les mesures techniques et Organisationnelles adéquates pour gérer les risques liés à la sécurité des services de confiance qu'elle fournit. Compte tenu des évolutions technologiques les plus récentes, ces mesures garantissent que le niveau de sécurité est proportionné au degré de risque. Des mesures sont notamment prises en vue de prévenir et de limiter les conséquences d'incidents liés à la sécurité et d'informer les parties concernées des effets préjudiciables de tels incidents.

En cas de violation des données personnelles, l'IGC OTU se réfère à la Procédure de Traitement des Violations de Donnés Personnelles [PTVDP] de Worldline mise à sa disposition.

L'IGC OTU s'engage à mettre en œuvre la Politique de Sécurité Opérationnelle [PSO] en vigueur, et agit conformément aux obligations de type LRC (Légales Réglementaires et Contractuelles).

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.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en terme de protection des données personnelles

L'IGC OTU agit conformément à la législation et à la réglementation défini au chapitre 9.4.1 du présent document.

9.4.5 Notification et consentement d'utilisation des données personnelles

L'IGC OTU agit conformément à la législation et à la réglementation tel que rappelé au chapitre 9.4.1 du présent document. Les informations que tout Abonné remet à l'Autorité d'Enregistrement sont protégées contre la divulgation sans le consentement de l'Abonné et des personnes qui l'ont mandaté pour transmettre lesdites informations à l'IGC OTU.

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

L'IGC OTU agit conformément à la législation et à la réglementation défini au chapitre 9.4.1 du présent document.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5 Droits sur la propriété intellectuelle et industrielle

L'IGC OTU agit conformément à la législation et à la réglementation défini au chapitre 9.4.1 du présent document. Les documents publics, hors périmètre des informations confidentielles, demeurent propriété de Worldline.

9.6 Interprétations contractuelles et garanties

Les différentes composantes de l'IGC OTU doivent s'assurer :

- de la protection (intégrité et confidentialité) de leurs clés privées et de leur(s) éventuelle(s) donnée(s) d'activations tout au long de leur cycle de vie ;
- de l'utilisation des Bi-clés et des Certificats dans le cadre pour lesquelles elles ont été émises, conformément aux applications définies dans la présente PC/DPC au chapitre 1.5 ;
- du respect et de l'application de la présente PC/DPC ;
- de la soumission aux contrôles de conformité effectués par des auditeurs externes et de la mise en œuvre des préconisations qui en découlent ;
- de la mise en œuvre des moyens techniques et humains afin d'atteindre les engagements pris, notamment le niveau de service spécifié ;
- de documenter leurs procédures internes de fonctionnement ;

- d'avoir des pratiques non-discriminatoires dans leurs politiques et leurs procédures.

9.6.1 Autorité de Certification

L'AC OTU a pour obligation de :

- contrôler à ce que l'Autorité d'Enregistrement agissant au nom de l'AC OTU respecte la présente PC/DPC ;
- publier les informations publiques citées au chapitre 2.2 du présent document, notamment les Conditions Générales d'Abonnement et les Conditions Générales des Services, de façon durable et sécurisée ;
- garantir le respect de la Politique de Sécurité Opérationnelle de l'IGC OTU par les différentes composantes de celle-ci ;
- rendre accessible ses services à tout Abonné ayant accepté les Conditions Générales d'Abonnement ;
- 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 Bénéficiaires 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 ;
- vérifier et respecter les obligations qui leur incombent décrites dans le présent document et dans les Conditions Générales des Services.

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.

9.6.3.1.1 Certificat à usage unique

Pour un Certificat à usage unique, l'Abonné à l'AC OTU 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 de l'IGC OTU ;

- 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.

9.6.3.1.2 Certificat d'Organisation

Pour un Certificat d'Organisation, l'Abonné à l'AC OTU 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 Titulaire

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 Certificats

Les utilisateurs de Certificats fournis par l'AC OTU ont pour obligation de :

- vérifier et respecter les obligations qui leur incombent dans le présent document et dans les Conditions Générales des Services. Ces obligations seront pour les Certificats à usage unique décrites par l'Abonné dans le contrat qui le lie au futur Titulaire. 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 ;
- vérifier la validité du Certificat (expiration, révocation, intégrité) et celle de chaque Certificat de la Chaîne de Certification.

9.6.5 Autres participants

9.6.5.1 Comité Sécurité

Le Comité Sécurité a pour obligation, entre autres, de :

- prendre connaissance et maîtriser l'ensemble du set documentaire de l'IGC OTU ;
- garantir et maintenir la cohérence de la présente PC/DPC ;
- valider la PSO et l'Analyse de Risque de l'IGC OTU ;

9.7 Limite de garantie

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

L'IGC OTU 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 l'AC OTU 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 de l'IGC OTU ne peut être engagée qu'en cas de non-respect prouvé de ses obligations.

L'AC OTU 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.

L'AC OTU 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 de l'AC OTU à laquelle elle ne saurait en aucun cas se substituer.

9.9 Indemnités

La délivrance de Certificats par l'AC OTU 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 anticipée de validité de la PC

9.10.1 Durée de validité

La présente PC/DPC est rendue effective lors de sa publication sur le site de l'IGC OTU à la fin de la période de préavis (cf. chapitre 9.11), après avoir été validée par l'entité gérant ce document (cf. chapitre 1.6.1). Elle reste en application, pour les Certificats émis dans le cadre de ce présent document, jusqu'à la fin de vie du dernier Certificat émis au titre de cette PC/DPC.

9.10.2 Fin anticipée

La présente PC/DPC reste en vigueur jusqu'à son remplacement par 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 Notification individuelles et communications entre les participants

L'IGC OTU 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 de l'IGC OTU 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

Les révisions de cette PC/DPC sont décidées par l'entité gérant le document : le Comité Sécurité (cf. chapitre 1.6.1). Les modifications de forme (orthographe, …) ou les clarifications rédactionnelles ne sont pas soumises à validation et le présent document peut être mis à jour sans notification préalable.

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

Si le Comité Sécurité estime qu'une modification de la PC/DPC a un impact sur le niveau de sécurité ou sur le niveau de confiance en l'IGC OTU, il pourra définir une nouvelle version de la Politique de Certification avec un nouvel OID.

9.13 Dispositions concernant la résolution de conflits

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'IGC OTU dans toutes ses composantes et y compris documentaires est régie par la législation et la réglementation en vigueur sur le territoire français qui lui est applicable, bien que ses activités qui découlent de la présente PC/DPC puissent avoir des effets juridiques en dehors du territoire français.

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'IGC OTU est sujette et applique la législation et la réglementation en vigueur sur le territoire français. Une veille régulière est effectuée pour vérifier le respect de ces contraintes légales par l'IGC.

Par ailleurs, seule la version française des documents contractuels (dont la présente PC-DPC), énumérés au sein des Conditions Générales d'Abonnement, est opposable aux parties, même en présence de traductions. En effet, les traductions de convention expresse sont prévues à titre de simple commodité et ne peuvent avoir aucun effet juridique, notamment sur l'interprétation du Contrat d'Abonnement ou de la commune intention des parties.

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

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible. A ce titre, l'IGC OTU ne peut être tenue pour responsable de tout dommage indirect et interruption de ses services relevant de la force majeure.

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

Les rôles au sein de l'IGC OTU chargés de la génération de Certificats et de la gestion de la révocation sont des rôles dédiés et séparés des autres rôles fonctionnellement, techniquement et hiérarchiquement. Ces rôles sont exercés de façon indépendante et ne sont donc sujets à aucune éventuelle pression commerciale qui pourrait nuire à l'éthique et à la déontologie des services de confiances fournis par l'IGC OTU.

L'émission de Certificats à la demande de l'Abonné, conformément à la présente PC/DPC, ne fait pas de l'AC OTU y compris l'ensemble de ceux qui la composent et la représente, les mandataires ou les représentants de quelque façon que ce soit de l'Abonné, de l'Organisation ou du Titulaire. Ces participants au présent document ne constituent ni une association, ni une société ou autre groupement.

L'Organisation mise en place dans le cadre de l'IGC OTU, dédiée à ces activités avec une étanchéité des rôles, permet de préserver l'impartialité des opérations. Par ailleurs, l'IGC OTU s'assure que les activités de confiance fournies sont pratiquées de façon équivalente pour l'ensemble des bénéficiaires.

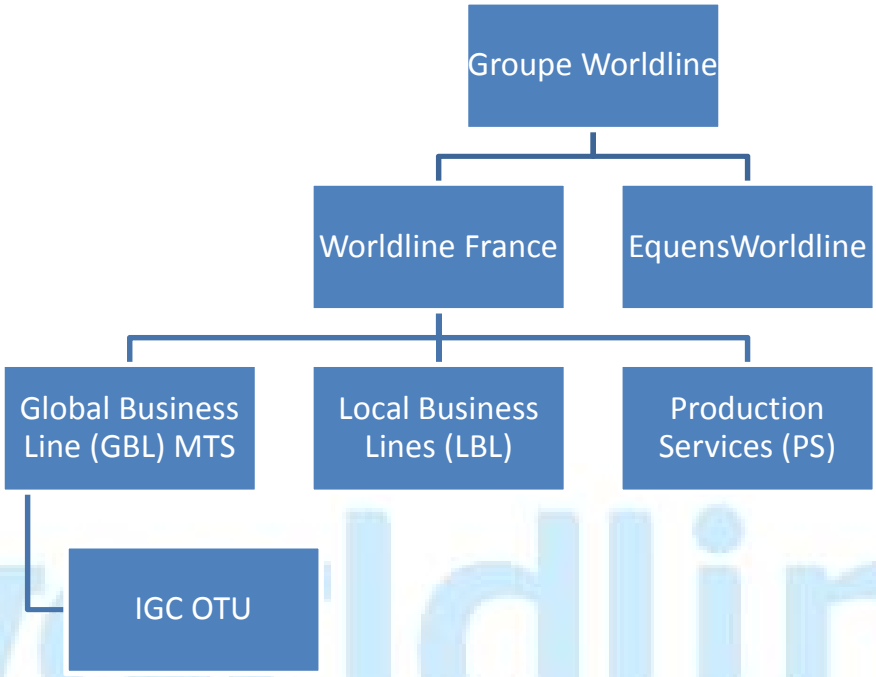

Figure 3 - Schéma organisationnel

L'IGC OTU est centralisée au sein de la Global Business Line (GBL), une unité transversale aux autres de Worldline. L'Organisation mise en place par Worldline dans le cadre de l'IGC OTU, dédiée à ces activités avec une étanchéité des rôles, permet de préserver l'impartialité des opérations (cf. Figure 3 - Schéma organisationnel).

9.17.2 Analyse de risques

Dans le cadre des activités de l'IGC OTU, une analyse de risque est réalisée par le responsable sécurité de cette IGC sur son périmètre.

Elle a pour objectif de permettre l'identification des risques SSI et des mesures SSI mises en œuvre pour les traiter. Elle permet d'assurer la cohérence de la Politique de Sécurité de l'Information de l'AC OTU au regard du niveau de risque.

Ce document permet notamment d'identifier la dépréciation des algorithmes, les actifs et leurs besoins en termes de sécurité applicables aux systèmes de l'IGC. Il tient compte de l'état de l'art en la matière et fait l'objet d'une révision régulière effectuée par le responsable sécurité de l'IGC OTU. Elle est validée par le Comité Sécurité suite à sa révision au maximum tous les vingt-quatre (24) mois.

9.17.3 Documents contractuels

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

10 Annexes

REGLEMENTATION	
Référence	**Description**
[CNIL]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2004-801 du 6 août 2004
[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

REGLEMENTATION 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 v1.2.1 (2017-05) Electronic Signature and Infrastructures (ESI); Cryptographic Suites
[ETSI EN 319 401]	ETSI EN 319 401 v2.1.1 (2016-02) Electronic Signature and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
[ETSI EN 319 411-1]	ETSI EN 319 411-1 v1.1.1 (2016-02) 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

DOCUMENTATION TECHNIQUE DE L'IGC OTU	
Référence	**Description**
[DTPC]	Documentation Technique des Pratiques de Certification Autorité de Certification OTU Référence : OTU DTPC 0003
[CGA]	Conditions Générales d'Abonnement au service de signature électronique OTU et/ou cachet électronique Autorité de Certification OTU Référence : OTU CG 0008
[CGS]	Conditions Générales des Services Autorité de Certification OTU Référence : OTU CG 0022
[PCA]	Plan de Cessation d'Activité Autorité de Certification OTU Référence : OTU PCA 0027

[PCRA]	Plan de Continuité et de Reprise d'Activité Autorité de Certification OTU Référence : OTU PCRA 0029
[PESV]	Protocole d'Externalisation des Sauvegardes de Vendôme Worldline Référence : Protocole d'Externalisation des Sauvegardes de Vendôme
[PGI]	Politique de Gestion des Incidents Worldline Référence : WLM-SEC-0008
[PSO]	Politique de Sécurité Opérationnelle de l'IGC OTU Autorité de Certification OTU Référence : OTU PSO 0015
[PTVDP]	Procédure de Traitement des Violations de Donnés Personnelles Worldline Référence : WLP-DPO-F017