

Référence du document :
Révision du document :
Date du document :
Classification

OTU.PC.0002
1.3
01/02/2015
PUBLIC



Autorité de Certification OTU

Politique de Certification



www.worldline.com

Table des matières

HISTORIQUE DES REVISIONS DE DOCUMENT	8
1. INTRODUCTION	9
1.1 OBJET DU DOCUMENT	9
1.2 IDENTIFICATION.....	10
1.2.1 <i>Identification du document</i>	10
1.2.2 <i>Identification de L'Autorité de Certification</i>	10
1.3 COMPOSANTES DE L'IGC.....	10
1.3.1 <i>Schéma fonctionnel de l'IGC</i>	10
1.3.2 <i>Hiérarchie d'AC</i>	11
1.3.3 <i>Autorités de certification AC OTU</i>	11
1.3.4 <i>Autorité d'Enregistrement (AE)</i>	12
1.3.5 <i>Porteur de certificats</i>	12
1.3.6 <i>L'Abonné et le Titulaire(Sujet)</i>	13
1.3.7 <i>Utilisateur de certificats</i>	13
1.3.8 <i>Organisation</i>	13
1.3.9 <i>Autres participants</i>	14
1.4 CATEGORIES DE CERTIFICATS	14
1.4.1 <i>Certificat à usage unique</i>	14
1.4.2 <i>Certificat d'Organisation</i>	14
1.5 USAGE DES CERTIFICATS	15
1.5.1 <i>Domaines d'utilisation applicables</i>	15
1.5.2 <i>Domaines d'utilisation interdits</i>	15
1.6 GESTION DE LA PC.....	16
1.6.1 <i>Entité gérant la PC</i>	16
1.6.1 <i>Contact</i>	16
1.6.2 <i>Entité déterminant la conformité d'une DPC avec cette PC</i>	16
1.6.3 <i>Procédure d'approbation de la conformité de la DPC</i>	16
1.7 DEFINITIONS ET ABBREVIATIONS	16
1.7.1 <i>Principales définitions</i>	16
1.7.2 <i>Abréviations</i>	19
1.8 DECLARATION DE CONFORMITE	19
2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES	20
2.1 ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS	20
2.2 INFORMATIONS DEVANT ETRE PUBLIEES.....	20
2.3 DELAIS ET FREQUENCES DE PUBLICATION	20
2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES	20
2.4.1 <i>L'accès aux autres documents</i>	20
3 IDENTIFICATION ET AUTHENTIFICATION	21
3.1 NOMMAGE	21
3.1.1 <i>Types de noms</i>	21
3.1.2 <i>Nécessité d'utilisation de noms explicites</i>	21
3.1.3 <i>Anonymisation ou pseudonymisation des Porteurs</i>	21
3.1.4 <i>Règles d'interprétation des différentes formes de nom</i>	21
3.1.5 <i>Unicité des noms</i>	21
3.1.6 <i>Identification, authentification et rôle des marques déposées</i>	21
3.2 VALIDATION INITIALE D'IDENTITE.....	22
3.2.1 <i>Méthode pour prouver la possession de la clé privée</i>	22
3.2.2 <i>Validation de l'identité des organismes</i>	22
3.2.3 <i>Validation de l'identité d'un individu</i>	23
3.2.4 <i>Informations non vérifiées</i>	25
3.2.5 <i>Validation de l'Autorité du demandeur Abonné</i>	25

3.2.6	Validation de l'AE.....	25
3.2.7	Critères d'interopérabilité.....	25
3.3	IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUELEMENT DES CLES	26
3.3.1	Certificat à usage unique.....	26
3.3.2	Certificat d'Organisation	26
3.4	IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION	26
3.4.1	Certificat à usage unique.....	26
3.4.2	Certificat d'Organisation	27
4	EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	28
4.1	DEMANDE DE CERTIFICAT	28
4.1.1	Origine d'une demande de certificat	28
4.1.2	Processus et responsabilités pour l'établissement d'une demande de certificat	28
4.2	TRAITEMENT D'UNE DEMANDE DE CERTIFICAT.....	29
4.2.1	Exécution des processus d'identification et de validation de la demande.....	29
4.2.2	Acceptation ou rejet de la demande.....	30
4.2.3	Délai d'établissement du certificat	30
4.3	DELIVRANCE DU CERTIFICAT	31
4.3.1	Actions de l'AC concernant la délivrance du certificat.....	31
4.3.2	Notification par l'AC de la délivrance du certificat au Porteur	31
4.4	ACCEPTATION DU CERTIFICAT	31
4.4.1	Démarche d'acceptation du certificat.....	31
4.4.2	Publication du certificat.....	31
4.4.3	Notification par l'AC aux autres entités de la délivrance du certificat.....	31
4.5	USAGES DE LA BI-CLE ET DU CERTIFICAT	32
4.5.1	Utilisation de la clé privée et du certificat par le Porteur	32
4.5.2	Utilisation de la clé publique et du certificat par les partie prenantes	32
4.6	RENOUELEMENT D'UN CERTIFICAT.....	33
4.6.1	Causes possibles de renouvellement d'un certificat	33
4.6.2	Origine d'une demande de renouvellement	33
4.6.3	Procédure de traitement d'une demande de renouvellement.....	33
4.6.4	Notification de l'établissement d'un certificat renouvelé.....	33
4.6.5	Démarche d'acceptation du nouveau certificat.....	33
4.6.6	Publication du nouveau certificat.....	33
4.6.7	Notification par l'AC aux autres entités de la délivrance du nouveau certificat.....	33
4.7	DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE	34
4.7.1	Causes possibles de changement d'une bi-clé.....	34
4.7.2	Origine d'une demande d'un nouveau certificat	34
4.7.3	Procédure de traitement d'une demande d'un nouveau certificat.....	34
4.7.4	Notification de l'établissement du nouveau certificat.....	34
4.7.5	Démarche d'acceptation du nouveau certificat.....	34
4.7.6	Publication du nouveau certificat	34
4.7.7	Notification par l'AC aux autres entités de la délivrance du nouveau certificat.....	34
4.8	MODIFICATION DU CERTIFICAT	35
4.8.1	Causes possibles de changement d'une bi-clé.....	35
4.8.2	Origine d'une demande d'un nouveau certificat	35
4.8.3	Procédure de traitement d'une demande d'un nouveau certificat.....	35
4.8.4	Notification de l'établissement du nouveau certificat.....	35
4.8.5	Démarche d'acceptation du nouveau certificat.....	35
4.8.6	Publication du nouveau certificat.....	35
4.8.7	Notification par l'AC aux autres entités de la délivrance du nouveau certificat.....	35
4.9	REVOCATION ET SUSPENSION DES CERTIFICATS.....	36
4.9.1	Causes possibles d'une révocation.....	36
4.9.2	Origine d'une demande de révocation.....	38
4.9.3	Procédure de traitement d'une demande de révocation	38
4.9.4	Délai accordé au Porteur pour formuler la demande de révocation	39
4.9.5	Délai de traitement par l'AC d'une demande de révocation.....	39
4.9.6	Exigences de vérification de la révocation par les utilisateurs de certificats.....	39

4.9.7	Fréquence d'établissement des LCR.....	39
4.9.8	Délai maximum de publication d'une LCR	39
4.9.9	Autres moyens disponibles d'information sur les révocations.....	39
4.9.10	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats	39
4.9.11	Autres moyens disponibles d'information sur les révocations.....	39
4.9.12	Exigences spécifiques en cas de compromission de la clé privée	40
4.9.13	Causes possibles d'une suspension	40
4.9.14	Origine d'une demande de suspension	40
4.9.15	Procédure de traitement d'une demande de suspension	40
4.9.16	Limites de la période de suspension d'un certificat	40
4.10	FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS	40
4.10.1	Caractéristiques opérationnelles	40
4.10.2	Disponibilité de la fonction	40
4.10.3	Dispositifs optionnels.....	40
4.11	FIN DE LA RELATION ENTRE L'ABONNE ET L'AC	40
4.12	SEQUESTRE DE CLE ET RECOUVREMENT	41
4.12.1	Politique et pratiques de recouvrement par séquestre des clés	41
4.12.2	Politique et pratiques de recouvrement par encapsulation des clés de session	41
5	MESURES DE SECURITE NON TECHNIQUES.....	42
5.1	MESURES DE SECURITE PHYSIQUE.....	42
5.2	MESURES DE SECURITE PROCEDURALES	42
5.2.1	Rôles de confiance	42
5.2.2	Nombre de personnes requises par tâches.....	42
5.2.3	Identification et authentification pour chaque rôle.....	42
5.2.4	Rôles exigeant une séparation des attributions	43
5.3	MESURES DE SECURITE VIS-A-VIS DU PERSONNEL	43
5.3.1	Qualifications, compétences et habilitations requises.....	43
5.3.2	Procédures de vérification des antécédents	43
5.3.3	Exigences en matière de formation initiale	43
5.3.4	Exigences et fréquence en matière de formation continue	43
5.3.5	Fréquence et séquence de rotation entre différentes attributions	43
5.3.6	Sanctions en cas d'actions non autorisées.....	43
5.3.7	Exigences vis-à-vis du personnel des prestataires externes.....	43
5.3.8	Documentation fournie au personnel.....	44
5.4	PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT.....	44
5.4.1	Type d'évènements enregistrés	44
5.4.2	Fréquence de traitement des journaux d'évènements.....	45
5.4.3	Période de conservation des journaux d'évènements.....	45
5.4.4	Protection des journaux d'évènements.....	45
5.4.5	Procédure de sauvegarde des journaux d'évènements	45
5.4.6	Système de collecte des journaux d'évènements.....	45
5.4.7	Notification de l'Enregistrement d'un évènement au responsable de l'évènement	45
5.4.8	Évaluation des vulnérabilités	45
5.5	ARCHIVAGE DES DONNEES	46
5.5.1	Types de données à archiver.....	46
5.5.2	Période de conservation des archives.....	46
5.5.3	Protection des archives.....	46
5.5.4	Procédure de sauvegarde des archives.....	46
5.5.5	Exigences d'horodatage des données.....	47
5.5.6	Système de collecte des archives	47
5.5.7	Récupération des archives	47
5.6	CHANGEMENT DE CLE D'AC	47
5.7	REPRISE SUITE A COMPROMISSION ET SINISTRE	47
5.7.1	Procédures de remontées et de traitement des incidents et des compromissions	47
5.7.2	Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données) 47	
5.7.3	Procédures de reprise en cas de compromission de la clé privée d'une composante	48

5.7.4	Capacités de continuité d'activité suite à un sinistre.....	48
5.8	FIN DE VIE DE L'IGC	48
5.8.1	Transfert d'activité ou cessation d'activité affectant une composante de l'IGC autre que l'AC.....	48
5.8.2	Cessation d'activité affectant l'AC.....	48
6	MESURES DE SECURITE TECHNIQUES	49
6.1	GENERATION ET INSTALLATION DE BI-CLES	49
6.1.1	Génération des bi-clés	49
6.1.2	Transmission de la clé privée à son propriétaire.....	49
6.1.3	Transmission de la clé publique à l'AC.....	50
6.1.4	Transmission de la clé publique de l'AC aux différents acteurs	50
6.1.5	Tailles des clés.....	50
6.1.6	Vérification de la génération des paramètres des bi-clés et de leur qualité.....	50
6.1.7	Objectifs d'usage de la clé	50
6.2	MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES	50
6.2.1	Standards et mesures de sécurité pour les modules cryptographiques.....	50
6.2.2	Contrôle de la clé privée	51
6.2.3	Séquestre de la clé privée	51
6.2.4	Copie de secours de clé privée	51
6.2.5	Archivage de clé privée	51
6.2.6	Transfert de la clé privée vers / depuis le module cryptographique	51
6.2.7	Stockage d'une clé privée dans un module cryptographique	51
6.2.8	Méthodes d'activation de la clé privée	51
6.2.9	Méthode de désactivation de la clé privée	52
6.2.10	Méthode de destruction des clés privées.....	52
6.2.11	Niveau de qualification du module cryptographique.....	52
6.3	AUTRES ASPECTS DE LA GESTION DES BI-CLES	52
6.3.1	Archivages des clés publiques.....	52
6.3.2	Durée de vie des bi-clés et des certificats	53
6.3.3	Inventaire des clés	53
6.4	DONNEES D'ACTIVATION	53
6.4.1	Génération et installation des données d'activation	53
6.4.2	Protection des données d'activation.....	53
6.4.3	Autres aspects liés aux données d'activation	53
6.5	MECANISMES DE SECURITE DES SYSTEMES INFORMATIQUES.....	54
6.5.1	Exigences de sécurité technique spécifiques aux systèmes informatiques.....	54
6.5.2	Niveau de qualification des systèmes informatiques.....	54
6.6	MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE.....	54
6.6.1	Mesures de sécurité liées au développement des systèmes	54
6.6.2	Mesures liées à la gestion de la sécurité.....	54
6.6.3	Niveau d'évaluation sécurité du cycle de vie des systèmes	54
6.7	MESURES DE SECURITE RESEAU.....	55
6.8	HORODATAGE / SYSTEME DE DATATION	55
7	PROFILS DES CERTIFICATS, OCSP ET DES LCR	56
7.1	PROFIL DES CERTIFICATS	56
7.1.1	Numéro de version.....	56
7.1.2	Extensions du certificat.....	56
7.1.3	OID des algorithmes	60
7.1.4	Forme des noms.....	60
7.1.5	Contraintes sur les noms.....	60
7.1.6	OID de la PC.....	60
7.1.7	Utilisation de l'extension "contraintes de politique"	60
7.2	PROFIL DES LCR	60
7.2.1	LCR et extensions	60
7.3	PROFIL OCSP	61
8	AUDIT DE CONFORMITE ET AUTRES EVALUATIONS.....	62

8.1	FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS	62
8.2	IDENTITES / QUALIFICATIONS DES EVALUATEURS	62
8.3	RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES.....	62
8.4	SUJETS COUVERTS PAR LES EVALUATIONS.....	62
8.5	ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS	62
8.5.1	<i>Réussite</i>	62
8.5.2	<i>A confirmer</i>	62
8.5.3	<i>Echec</i>	62
8.6	COMMUNICATION DES RESULTATS	63
9	AUTRES PROBLEMATIQUES METIERS ET LEGALES	64
9.1	TARIFS.....	64
9.2	ASSURANCE.....	64
9.2.1	<i>Couverture par les assurances</i>	64
9.2.2	<i>Autres ressources</i>	64
9.2.3	<i>Couverture et garantie concernant les entités utilisatrices</i>	64
9.3	CONFIDENTIALITE DES DONNEES PROFESSIONNELLES	64
9.3.1	<i>Périmètre des informations secrètes</i>	64
9.3.2	<i>Périmètre des informations confidentielles</i>	64
9.3.3	<i>Informations hors du périmètre des informations confidentielles</i>	64
9.3.4	<i>Responsabilités en terme de protection des informations confidentielles</i>	65
9.4	PROTECTION DES DONNEES PERSONNELLES	65
9.4.1	<i>Politique de protection des données personnelles</i>	65
9.4.2	<i>Informations à caractère personnel</i>	65
9.4.3	<i>Informations à caractère non personnel</i>	65
9.4.4	<i>Responsabilité en termes de protection des données personnelles</i>	65
9.4.5	<i>Notification et consentement d'utilisation des données personnelles</i>	65
9.4.6	<i>Conditions de divulgation d'informations personnelles aux Autorités judiciaires ou administratives</i>	65
9.4.7	<i>Autres circonstances de divulgation d'informations personnelles</i>	65
9.5	DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE	66
9.6	OBLIGATIONS ET GARANTIES	66
9.6.1	<i>Autorité de Certification</i>	66
9.6.2	<i>Autorité d'Enregistrement</i>	66
9.6.3	<i>Obligations incombant aux Porteurs</i>	66
9.6.4	<i>Abonnés</i>	66
9.6.5	<i>Titulaire</i>	67
9.6.6	<i>Utilisateurs de certificats</i>	67
9.6.7	<i>Autres participants</i>	67
9.7	LIMITE DE GARANTIE.....	67
9.8	LIMITE DE RESPONSABILITE	68
9.9	INDEMNITES	69
9.10	DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC.....	69
9.10.1	<i>Durée de validité</i>	69
9.10.2	<i>Fin anticipée</i>	69
9.10.3	<i>Effets de la fin de validité et clauses restant applicables</i>	69
9.11	NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS	69
9.12	PROCEDURES D'AMENDEMENTS.....	69
9.12.1	<i>Mécanisme et période d'information sur les amendements</i>	69
9.12.2	<i>Circonstances selon lesquelles l'OID doit être changé</i>	70
9.13	DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS.....	70
9.14	JURIDICTIONS COMPETENTES.....	70
9.15	CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS	70
9.16	DISPOSITIONS DIVERSES	70
9.16.1	<i>Accord global</i>	70
9.16.2	<i>Transfert d'activités</i>	70
9.16.3	<i>Conséquences d'une clause non valide</i>	70
9.16.4	<i>Application et renonciation</i>	70
9.16.5	<i>Force majeure</i>	71

9.17	AUTRES DISPOSITIONS	71
ANNEXE	72
10.1	REGLEMENTATION / NORMALISATION	72
10.2	DOCUMENT CONTRACTUEL	73
10.3	EXIGENCES SUR LES OBJECTIFS DE SECURITE	73
10.4	EXIGENCES SUR LA QUALIFICATION	73
FIN DU DOCUMENT	74



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 : <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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

1. Introduction

1.1 Objet du document

Ce document décrit la politique de certification (PC) de l'**AC OTU** créée pour émettre les certificats de signature dans le cadre du service de souscription en ligne OTU.

Cette PC présente :

- Les exigences auxquelles l'**AC OTU** se conforme dans les étapes d'Enregistrement et de contrôle des demandes de certificat,
- La gestion des certificats dans leur cycle de vie,
- les mesures de sécurité autour de l'infrastructure,
- Les usages pour lesquels ces certificats sont émis.

Cette PC concerne les certificats à destination de Porteurs de certificat.

En complément de cette PC, est établi un second document appelé Déclaration des Pratiques de Certification [DPC]. La DPC est l'énoncé des pratiques qu'une AC utilise dans la gestion des certificats. Ce document décrit comment est implémentée l'**AC OTU** :

- Moyens informatiques et réseaux,
- Progiciels externes et services propriétaires,
- Sécurité physique mise en œuvre sur les sites d'hébergement,
- Sécurité logique sur les moyens informatiques,
- Procédures de gestion des certificats,
- Procédures d'exploitation et formation du personnel,

La DPC est à ce titre la réponse au cahier des charges exprimé dans la PC.

1.2 Identification

1.2.1 Identification du document

Eléments	Valeur
Titre	Politique de Certification de l'Autorité de Certification OTU
Référence document	OTU.PC.0002
Version	1.3
Auteur	Worldline
Référence produit	Autorité de Certification OTU
Mots clé	Autorité de Certification, Politique de Certification, PC, Certification électronique, Signature électronique,

1.2.2 Identification de L'Autorité de Certification

Le nom de l'Autorité de Certification est « **OTU** ».

Le n° **1.2.250.1.111** a été attribué par l'AFNOR pour "Worldline"

Les OID sont basés sur l'OID de la Worldline et construit de la façon suivante : 1.2.250.1.111.x.y.z.w où:

- x : année de création de la PC : 2012 => 12
- y : numéro d'ordre de création de la PC dans l'année
- z : version de la PC
- w, type de certificat au sein de l'AC

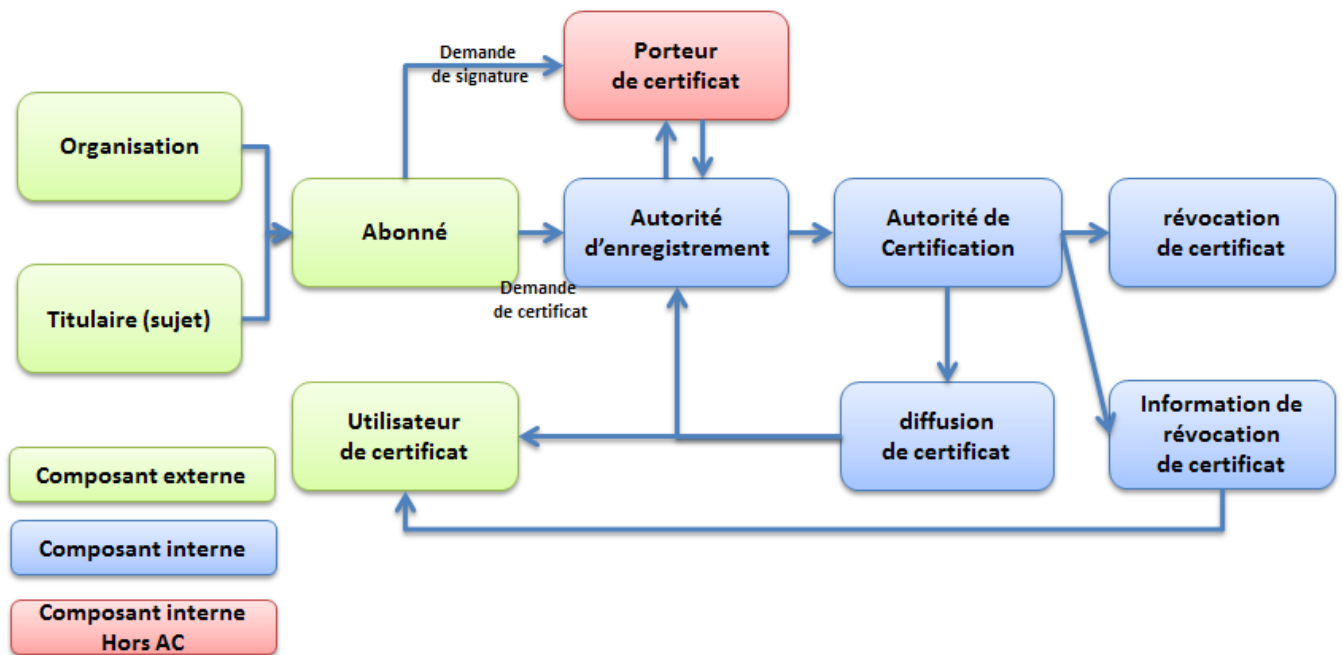
La PC de l'AC OTU a pour OID **1.2.250.1.111.12.7.1**

- OID Certificat à usage unique : 1.2.250.1.111.12.7.1.1
- OID Certificat d'Organisation : 1.2.250.1.111.12.7.1.2

1.3 Composantes de l'IGC

1.3.1 Schéma fonctionnel de l'IGC

L'IGC OTU mise en œuvre se compose de plusieurs blocs fonctionnels, le détail des composants est décrit au § 1.3



1.3.2 Hiérarchie d'AC

L'AC OTU est rattachée à une Autorité de Certification Racine Atos Worldline

DN:

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

OID : 1.2.250.1.111.12.4.1

1.3.3 Autorités de certification AC OTU

L'AC OTU a pour obligation l'application de la présente PC OTU.

L'AC OTU signe les certificats qu'elle émet avec sa clé privée et en est responsable.

L'AC OTU s'appuie pour cela sur une infrastructure technique : une infrastructure de gestion de clés (IGC).

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.

La décomposition fonctionnelle de l'IGC OTU est la suivante :

- Service d'Enregistrement,
- Service de génération de certificat,
- Service de remise de certificat,
- Service de révocation de certificat,
- Service d'information sur l'état des certificats.

1.3.3.1 Autorité de Certification

Désigne ici la partie technique de l'Autorité de Certification ou service de certification. Il s'agit de l'entité qui produit les certificats à la demande du service d'Enregistrement. Il a également en charge le cycle de vie complet du certificat (fabrication, publication, ...).

Ce service génère (signature électronique avec la clé privée de l'**AC OTU**) les certificats à partir des informations transmises par l'Autorité d'Enregistrement et de la clé publique du Porteur de certificat provenant de la fonction de génération des éléments secrets des Porteurs.

L'Autorité de Certification est également représentée par Un responsable d'Autorité désigné au sein Worldline

1.3.3.2 Service de diffusion de certificat

Cette fonction remet à l'Autorité d'Enregistrement le certificat signé par l'Autorité de Certification, celui-ci est ensuite transmis au Porteur de certificat pour utilisation dans le cadre décrit § 1.4

1.3.3.3 Service de révocation de certificat

Ce service traite les demandes de révocation de certificats. Les résultats des traitements sont diffusés via le service d'information sur l'état des certificats.

1.3.3.4 Service d'information sur l'état des certificats

Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, ...). Cette fonction est mise en œuvre via l'utilisation de liste de certificat révoqués (LCR).

1.3.4 Autorité d'Enregistrement (AE)

L'AE est l'entité interlocutrice des unités clientes (Abonnés) qui lui transmettent des demandes de certificats. C'est à ce niveau qu'ont lieu les opérations suivantes:

- Authentification de l'Abonné qui procède à la demande
- vérification du contenu des demandes de certificat,
- Enregistrement des demandes de certificat,
- Livraison des certificats,
- Archivage des demandes de certificat,
- Enregistrement des demandes de révocation,
- Acceptation ou refus des demandes de révocation,
- Archivage des demandes de révocation.

Pour rendre ces services, l'AE s'appuie sur des moyens techniques notamment sur un service d'Enregistrement qui permet la gestion du cycle de vie des certificats pour l'AC et constitue à ce titre un point d'accès unique à l'AC (serveurs permettant la transmission des demandes et la livraison des certificats)

1.3.5 Porteur de certificats

Dans le cadre de la présente PC, le Porteur de certificat n'est pas assimilé au titulaire du certificat

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

Le Porteur de certificat 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 transmis par l'Abonné.
- Utilisation de la clé privée et certificat à des fins de signature électronique pour le compte de l'organisation ou du titulaire de certificat.
- Destruction de la clé privée (selon les types de certificats cf 1.4).

Le Porteur de certificat assure une conservation sécurisée et un contrôle exclusif pour le compte du titulaire ou de l'organisation, des éléments secrets

1.3.6 L'Abonné et le Titulaire(Sujet)

Dans certains cas, les certificats peuvent être émis directement à leur demande, à des personnes physiques agissant pour elle-même et leur propre usage. Ces personnes sont dénommées Titulaires ont un lien direct avec l'Abonné, à qui elles formulent leur demande.

Il est précisé que dans le cadre de l'AC OTU, la demande de certificat au Service de Certification OTU, est faite, par l'Abonné pour son Client,

Dès lors que le Client a exprimé son souhait d'apposer sa signature électronique sur le document qui lui a été proposé par l'Abonné, dans un contexte de contractualisation électronique,

L'Abonné, qui a souscrit aux services de l'AC OTU, fait la demande de certificat

- pour son client qui sera le titulaire du certificat émis préalablement à la demande de certificat pour son Client, l'Abonné aura, en fonction notamment de ses besoins métier, identifié son Client de telle manière que le certificat émis au nom de son Client puisse reposer sur une identité fiable et raisonnablement vérifiée. L'Autorité de Certification produira dans ce cas de certificat de type usage unique (cf. 1.4.1). Le client de l'abonné peut être un particulier ou un représentant d'une société.
- Pour une ou plusieurs Organisations dépendant de l'Abonné, l'Autorité de Certification produit alors des certificats d'Organisation (cf. 1.4.2)

1.3.7 Utilisateur de certificats

L'utilisateur est la personne physique ou morale qui utilise les informations d'un certificat qu'elle reçoit (ici par le biais d'une signature électronique). Cette signature est associée à un document numérique, (un document PDF).

A noter que la signature d'un Document PDF 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 PDF ne disposent pas tous des fonctions de visualisation de signature.

1.3.8 Organisation

Une Organisation est rattachée à un Abonné qui va demander un certificat de signature contenant le nom de l'Organisation. Ce certificat est utilisé uniquement dans le cadre de service de signature de PDF opéré par Worldline.

L'Organisation utilise un Porteur de certificat opéré par Worldline, pour stocker et signer des documents à sa place dans le cadre d'une délégation entre Worldline et l'Abonné.

Bien que l'Abonné et l'Organisation soient dans la plupart des cas, une seule même entité il est possible de différencier ces deux entités.

Par exemple un Abonné peut souhaiter utiliser un nom de marque plutôt que le nom de l'entreprise, 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.

Un certificat d'Organisation fait référence à une personne représentant l'Abonné, et dument autorisée, le nom de cette personne figure dans le certificat produit par l'AC OTU.

Par rapport au document de spécifications de l'ETSI, une organisation est à considérer comme un sujet, toutefois dans la présente Politique de Certification, il est fait référence nommément, à l'organisation

1.3.9 Autres participants

Des moyens humains complètent le dispositif :

- Exploitants des systèmes informatiques, (maintien en condition opérationnelle)
- Equipes en charge du maintien en conformité.

1.4 Catégories de certificats

L'Autorité de Certification OTU produit deux types de certificats qui se distinguent principalement par leur OID (cf 7.1)

1.4.1 Certificat à usage unique

Un certificat à usage unique est produit par l'Autorité de Certification pour un titulaire humain, et pour lequel un certificat est produit à la demande de l'Abonné.

Ce certificat dispose d'une durée de vie très courte et permet de produire une signature de document PDF pour le compte du titulaire, à la demande de l'Abonné.

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 :

La DPC décrit comment la signature du message est validée lors de la demande de signature.

- Les données d'identification du titulaire
- Une signature électronique permettant de garantir l'intégrité des données d'identification, ainsi que l'identité de l'Abonné

L'Abonné est responsable des données d'identification transmises dans la demande et qui permettent de créer un certificat contenant des données vérifiées du titulaire.

La clé privée d'un titulaire est générée dans un équipement sécurisé et dédié (Hardware Secure Module) ayant obtenu le niveau de certification FIPS 140-2 level 2 ou supérieur.

Une fois que le certificat à usage unique a été utilisé à la demande de l'Abonné, la clé privée correspondante est détruite dans le HSM.

1.4.2 Certificat d'Organisation

Le certificat d'Organisation est délivré dans le cadre de service de signature de PDF opéré par Worldline dans ses propres locaux pour le compte de l'Organisation.

Le certificat d'Organisation permet à celle-ci de demander à Worldline une signature de document PDF par une Organisation (Certification).

L'Abonné transmet la demande de signature au Porteur au moyen d'un message signé électroniquement par l'Abonné.

La demande de certificat est une procédure entre un représentant habilité de l'Abonné et un Opérateur d'Enregistrement Worldline. Les informations à fournir pour la demande sont détaillées au § 4.1.1

La présente PC 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 (Hardware Secure Module) ayant obtenu le niveau de certification FIPS 140-2 level 2 ou supérieur.

1.5 Usage des certificats

1.5.1 Domaines d'utilisation applicables

1.5.1.1 Bi-clés et certificats des Porteurs

La présente PC traite des bi-clés et des certificats à destination des catégories de Porteurs identifiées au chapitre 1.3.5 ci-dessus, afin que ces Porteurs puissent signer électroniquement des documents PDF dans le cadre de procédure de souscription ou de transmission dématérialisée.

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 de Titulaire ou d'organisation et des LCR et dispose d'une seule bi-clé pour cela. Son certificat est signé par l'AC de niveau supérieur cf. § 1.3.2.

La chaîne de certification de l'IGC OTU possède la structure suivante :

- Certificat de l'AC racine : certificat électronique auto-signé AWL-RACINE.,
- Certificat d'AC Fille: certificat électronique délivré à une AC par l'AC racine,
- Certificat Porteur : certificat électronique délivré à un Porteur par une l'AC Fille OTU.

1.5.2 Domaines d'utilisation interdits

Toute utilisation de certificat émis par l'AC OTU en désaccord avec les usages décrit dans la présente PC au § 1.5.1.1 & 4.5, sont prohibés.

L'AC OTU ne peut être tenue pour responsable en cas d'une utilisation d'un certificat qu'elle émet contraire à celles indiquées dans la présente PC au § 1.5.1.1 & 4.5.

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. A cette fin, le comité sécurité statue à échéances régulières, sur la nécessité d'apporter des modifications à la PC.

1.6.1 Contact

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

Comité "MediaCert OTU"

Worldline

19, rue de la Vallée Maillard

B.P. 1311

41013 Blois Cedex

France

dlfr-mediacert-ac-otu@atos.net

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

Worldline procède à des contrôles de conformité de l'AC effectués par des auditeurs externes.

1.6.3 Procédure d'approbation de la conformité de la DPC

Worldline désigne les personnes déterminant la conformité de la DPC avec la présente PC. Ces personnes sont des personnels Worldline.

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 inscrite au service de délivrance de certificats OTU, pour la délivrance

- de certificats d'Organisation au nom de personnes dûment habilitées au sein de l'Abonné.
- de certificats à usage unique au nom des Titulaires dénommés dans la présente PC et qu'il aura préalablement identifiés.

Autorité de Certification (AC): Cf. § 1.3.3 Autorité chargée de l'application de la présente PC, 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 la PC.

Autorité d'Enregistrement (AE): Cf. § 1.3.4 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

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

Certificat : élément de données normalisé X509 permettant d'associer une clé publique à son détenteur. Un certificat contient des données comme :

- l'identité du détenteur,
- sa clé publique,
- l'identité de l'organisme ayant émis le certificat (l'AC),
- la période de validité,
- un numéro de série,
- une empreinte (thumbprint),
- des critères d'utilisation,

Le tout est signé par l'AC.

Il est délivré par une Autorité de Certification qui signe le certificat. contenant l'identité du Client de l'Abonné, sa capacité telle que déclarée par l'Abonné, , qu'il s'agisse d'un Client personne physique agissant pour ses propres besoins ou d'une personne physique dûment habilitée agissant au nom de son Organisation

Le certificat permet de valider le lien entre la signature électronique et son signataire déclaré, titulaire du certificat

Le certificat n'est pas un certificat qualifié dans le cadre de cette AC.

Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Certificat OTU : (One Time Usage) ou certificat à usage unique ; certificat produit dynamiquement lors du processus de contractualisation en ligne. Ce certificat est utilisé au cours d'une session unique de signature (signature des différents documents d'un contrat pour le titulaire) par la plateforme, puis la clé de signature est détruite.

Chaîne de confiance : ensemble des certificats nécessaires pour valider la filiation d'un certificat délivré à une entité. Pour cette PC, la chaîne de confiance se compose du certificat de l'**AC OTU**.

Common Name (CN) : élément du champ « subject » du certificat contenant l'identité de son détenteur.

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.

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

Distinguished Name (DN) : nom distinctif X. 500 pour lequel le certificat est émis. Le DN est composé de données dont le CN permettant de connaître avec précision et sans ambiguïté son identité.

Demande de certificat : Demande formulée par l'Abonné à l'Autorité d'Enregistrement en vue d'obtenir un certificat pour le Client de l'Abonné .Elle comprend un ensemble d'informations devant être fournies au service d'Enregistrement en accompagnement de la demande de certificat.

dossier d'enregistrement électronique : Container de données au format électronique, il est destiné à contenir l'ensemble des données transmises par un abonné lors d'une demande de certificat (informations pour le certificat, données d'identification du titulaire etc ...), ces données sont archivées dans un système d'archivage à valeur probante, 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.

lightweight certificate policy (LCP): Politique de certification qui offre une qualité de service moins onéreuse en comparaison des politique de certification pour certificat qualifié telle que définie par [ETSI]

Organisation : Entité représentant une entreprise ou pouvant faire référence à un nom de marque pour laquelle un certificat de signature va être délivré à la demande d'un Abonné

Partie prenante (relying party) : Dans le contexte de cette PC, 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 numérique, par exemple un PDF

Politique de Certification (PC) : Document publié décrivant l'ensemble de règles définissant les exigences auxquelles l'AC se conforme dans la mise en place et la fourniture de prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les différents acteurs, ainsi que de toutes les composantes intervenant dans la gestion du cycle de vie des certificats. La politique de certification est identifiée par un OID.

Porteur de certificat : composant logiciel qui obtient un (ou des) certificat(s) de l'AC. Ces certificats sont utilisés selon les applications et les types de certificat pour des usages de signature électronique. L'entité « Porteur de certificat » est représentée par des serveurs opérés conjointement à l'AC. et garantit le contrôle exclusif des bi-clés à cette entité uniquement.

Service d'Enregistrement: Voir Autorité d'Enregistrement

Service de gestion des révocations - Cf. § 1.3.3.3

Service d'information sur l'état des certificats - Cf. § 1.3.3.4

Session de signature :

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

Signature électronique :

« Une donnée sous forme électronique qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification ».

Au sens de la présente PC, la signature électronique suit la définition de la signature électronique donnée par la directive Européenne du Parlement Européen et du conseil du 13 décembre 1999 mais ne répond pas aux exigences des signatures reposant sur des certificats qualifiés

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 à l'entité « Porteur de certificat »

1.7.2 Abréviations

Les acronymes utilisés dans la présente PC sont les suivants :

- **AC** : Autorité de Certification
- **AC OTU : Autorité de Certification délivrant les certificats décrit dans cette PC**
- **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*
- **FQDN** : *Fully Qualified Domain Name*
- **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
- **OC** : Opérateur de Certification
- **OE** : Opérateur d'Enregistrement,
- **OID** : Object Identifier
- **PC** : Politique de Certification
- **PP** : Profil de Protection
- **PSCE** : Prestataire de Services de Certification Électronique
- **RSSI** : Responsable Sécurité des Systèmes d'Informations
- **RFC** : *Request For Comment*
- **RSA** : Rivest Shamir Adelman
- **SHA** : *Secure Hash Algorithm*
- **SP** : Service de Publication
- **SSI** : Sécurité des Systèmes d'Information
- **SSL** : *Secure Sockets Layer*
- **TLS** : *Transport Layer Security*
- **URL** : *Uniform Resource Locator*
- **UTC** : Temps universel coordonné

1.8 Déclaration de conformité

La Présente PC est conforme à la spécification technique [ETSI102 042] au niveau LCP.

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

2.1 Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des utilisateurs de certificats, l'AC met en œuvre une fonction de publication et une fonction d'information sur l'état des certificats

La présente PC est disponible de manière publique

La LCR est disponible de manière publique

2.2 Informations devant être publiées

L'AC OTU publie en http la liste des certificats révoqués (LCR).

L'AC OTU publie la présente politique de certification.

Les URLs pour accéder à la PC ainsi qu'à la CRL sont disponible dans des extensions des certificats délivrés par l'AC OTU ((cf. Profil § 7.1) respectivement :

- Extension CPS URI
- Extension CRL Distribution Point

L'AC OTU publie les documents de certification disponibles et fournis par un organisme agréé, sur son site <http://www.mediacert.com>

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 dans les § 4.8.1 & 4.10.

C'est la PC la plus récente et en vigueur, qui est à disposition en accès public

2.4 Contrôle d'accès aux informations publiées

La LCR, et la PC sont accessibles en lecture uniquement.

2.4.1 L'accès aux autres documents

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 internes habilitées de l'IGC OTU, au travers d'une authentification 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'OTU. Le contrôle d'accès repose sur un contrôle d'accès par des serveurs dédiés à cette fonction.

La DPC précise les moyens mis en œuvre.

3 Identification et authentification

3.1 Nommage

3.1.1 Types de noms

Les noms utilisés sont conformes aux spécifications de la norme X.500.

Dans chaque certificat X509v3 les champs « issuer » et « subject » sont identifiés par un "Distinguished Name" DN de type X.501 sous forme d'une chaîne imprimable ("PrintableString").

3.1.2 Nécessité d'utilisation de noms explicites

Dans le cas de certificat à usage unique, les certificats émis dans le cadre de cette PC contiennent Le nom et prénom explicites de titulaire.

Dans le cas de certification d'organisation, les certificats émis contiennent le nom et prénom explicites de l'individu habilité par l'abonné ainsi que le nom de l'organisation.

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 des différentes formes de nom

L'interprétation des informations du champ DN est indiquée dans le chapitre Profils de certificat de la PC de l'AC OTU (cf § 7)

3.1.5 Unicité des noms

Le champ « Distinguished Name » (DN) est unique pour chaque Porteur. Toute demande ne respectant pas cette règle est refusée. Durant toute la durée de vie de l'AC, un DN attribué à un Porteur ne peut donc être attribué à un autre Porteur. Le § 7.1.2.2 précise les règles appliquées pour obtenir cette unicité sur les noms.

- Pour les certificats à usage unique : l'unicité est assurée pendant toute la durée de vie de l'AC, ainsi un titulaire demandant deux certificats distincts via l'Abonné, obtiendra l'émission de 2 DN différents.
- Pour les certificats d'Organisation, l'unicité du DN est garantie lors de l'Enregistrement par l'Opérateur d'Enregistrement, pour une même Organisation, le DN sera inchangé lors des renouvellements.

3.1.6 Identification, authentification et rôle des marques déposées

Cf 3.2.2.2

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, le contrôle de possession de la clé est réalisé au moyen d'une vérification cryptographique bas niveau d'une première signature produite au moyen de la clé privée.

Si la vérification échoue, le document PDF n'est pas signé, la clé privée est détruite, 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 Porteur est garantie lors de sa génération de la demande, par la signature du message au moyen de la clé privée et qui correspond à la clé publique contenue dans le message PKCS#10 envoyé à l'AE.

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

L'individu habilité indiqué 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 initiale de l'Abonné

La validation initiale d'un Abonné est associée à la mise en place préalable d'une relation contractuelle entre l'Abonné et Worldline. Il s'agit du Contrat d'Abonnement au service de signature électronique OTU

Un représentant de l'Abonné doit être identifié, il sera l'interlocuteur de l'AC par la suite pour les demandes de certificats d'Organisation. L'Abonné peut désigner formellement des adjoints habilités à le représenter. Il doit pour cela en informer l'AC.

Lors de la mise en œuvre du contrat d'abonnement, le représentant de l'abonné désigné devra fournir une copie de document officiel d'identité en cours de validité comportant une photographie d'identité (carte nationale d'identité, passeport ou carte de séjour) en cours de validité, l'AE en conserve la copie

Il devra également fournir une adresse mail permettant de le contacter, cette adresse mail sera utilisée notamment pour transmettre les informations lors de la création de certificats d'organisation

Lors d'une demande de certificat d'organisation par le représentant de l'Abonné, l'authentification de celui-ci est effectuée par l'Opérateur d'Enregistrement.

Lors des demandes de certificat à usage unique auprès de l'AE, le représentant de l'Abonné devra s'authentifier et signer électroniquement ces demandes.

Lors des demandes de signature auprès du Porteur, l'Abonné devra s'authentifier et signer électroniquement ces demandes.

L'Abonné a obligation à utiliser les modes d'authentification et de signature requis par l'AE et le Porteur.

Les certificats utilisés par l'abonné pour s'authentifier et signer les demandes de certificat et de signature, doivent être émis par une autorité de certification approuvée par l'AC OTU.

La DPC décrit le mode d'authentification de l'Abonné basé sur l'usage et la vérification des certificats électroniques vis-à-vis de l'AE et du porteur. Ainsi que les contrôles effectués

L'AE conserve l'ensemble des documents transmis lors de cette souscription.

3.2.2.2 Validation d'une Organisation

Comme décrit au §1.3.8, l'Organisation est représentée par un individu habilité. Les informations à fournir par l'abonné sont les suivantes :

- Une demande signée, et datée de moins de 3 mois, par un représentant identifié de l'Abonné désignant
 - le nom de l'Organisation
 - le futur individu habilité et identifié dans le certificat. Cette demande doit être signée pour acceptation par l'individu habilité,
- toute pièce, valide lors de la demande de certificat
 - permettant de démontrer le droit de l'Abonné à faire figurer le nom de l'Organisation dans le certificat (Si le certificat est destiné à l'abonné lui-même (nom identique), ce document n'est pas requis),
 - attestant de l'existence de l'Organisation
 - portant le numéro SIREN ou assimilé de celle-ci, ou, à défaut, une autre pièce attestant l'identification unique de l'Organisation qui figurera dans le certificat,
- toute pièce, valide lors de la demande de certificat, permettant de démontrer l'appartenance de l'individu habilité dans l'organisation
- une copie de document officiel d'identité en cours de validité de l'individu habilité (carte nationale d'identité, passeport ou carte de séjour) en cours de validité, l'AE en conserve la copie,
- l'adresse postale et l'adresse mail, téléphone permettant à l'AC de contacter l'individu habilité,

L'AE conserve l'ensemble des documents transmis lors de cette demande.

Le présente PC ne formule pas d'exigences en matière de face à face physique, toutefois l'AE pourra 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 certificat pour le Titulaire est déposée par l'Abonné auprès de l'AE. La demande de l'Abonné est faite sous format électronique

Cette demande est créée par l'Abonné qui la signe au moyen d'une signature électronique.

La demande de l'Abonné contient à minima les données d'état civil du Titulaire suivantes :

- Le nom et prénom du Titulaire
- La civilité du Titulaire

L'Abonné peut également préciser (mais pas uniquement) :

- L'adresse postale du Titulaire
- Le numéro de téléphone du Titulaire
- L'adresse mail du Titulaire

- La date et lieu de naissance du Titulaire

Ces dernières informations ne figurant pas dans le certificat produit, seront toutefois conservées dans le dossier d'enregistrement au format électronique associé à l'émission du certificat.

La conservation de ces données est nécessaire, car elles sont fournies pour la constitution du dossier d'enregistrement qui sera associé à chaque émission de certificat. Ce dossier d'enregistrement rassemble ces données décrivant les processus et données d'identification du client final

Le gabarit de certificat tel que décrit au 7.1.2.2 définit commun l'unicité du nom dans le certificat est garantie.

L'Abonné doit préciser à l'AC

Le procédé fiable d'identification de l'utilisateur qu'il va utiliser seul ou en combinatoire, et permettant de vérifier l'identité civile déclarée par le futur titulaire tels que notamment :

- L'ajout d'une pièce justificative d'identité scannée (sous réserve de la vérification de l'image scannée)
- Des informations complémentaires connues préalablement et propres au futur titulaire, permettant de l'identifier au sein d'une base de données préétablie.
- Une identité numérique vérifiée. (par opposition à une identité numérique déclarée)
- Tout autre procédé permettant ou ayant permis préalablement, de vérifier l'identité déclarée d'un titulaire.

Sans que cette liste présente un caractère exhaustif, mais de telle manière que la signature électronique par le titulaire du document électronique présenté par l'Abonné au Titulaire, puisse garantir son lien avec le document électronique auquel elle s'attache.

Ce procédé d'identification aura été décrit au préalable par l'Abonné lors de sa demande d'abonnement. Le procédé peut être mis en œuvre par un Opérateur technique opérant pour le compte de l'Abonné.

Le procédé étant décrit par l'Abonné, il lui appartient

- de le mettre en œuvre (ou de le faire mettre en œuvre par son prestataire technique).
- de transmettre les données d'identification capturées lors de la mise en œuvre du procédé choisi dans un dossier d'enregistrement électronique.

La DPC décrit la mise en œuvre du dossier d'enregistrement électronique qui va être créée à cette occasion.

L'AC se réserve le droit d'apprécier la fiabilité du procédé d'identification et de ne pas délivrer de certificat si le procédé est évalué comme n'apportant pas un niveau suffisant de fiabilité.

L'Abonné doit fournir :

- Les informations techniques permettant de mettre en évidence comment le titulaire a explicitement donné son accord pour procéder à une signature électronique au moyen du certificat à usage unique. ces procédés peuvent par exemple être (mais pas uniquement) :
 - Une capture électronique de signature manuscrite
 - La fourniture d'un code reçu par SMS sur un téléphone portable
 - Un Enregistrement vocal du titulaire

Ce procédé d'identification aura été décrit au préalable par l'Abonné. Le procédé peut être mis en œuvre par un Opérateur technique opérant pour le compte de l'Abonné

L'AC contrôle que ce procédé est effectivement mis en œuvre par l'abonné.

L'ensemble des données sont archivées de manière électronique et conservées conformément au § 5.4

3.2.3.2 Enregistrement d'un Opérateur d'Enregistrement

L'AE peut être utilisé par des agents d'AE pour le traitement des demandes de certificat d'Organisation.

La DPC décrit comment sont désignés les agents d'AE

3.2.4 Informations non vérifiées

Toutes les informations du champ « Subject » dans le certificat sont vérifiées lors de la demande de certificat.

3.2.5 Validation de l'Autorité du demandeur Abonné

L'Abonné s'authentifie auprès de l'AE avant toute demande, la DPC décrit le mode d'authentification auprès de l'AE selon les types de certificats demandé :

- Certificats à usage unique : authentification par certificat
- Certificat d'authentification : authentification par l'Opérateur d'Enregistrement

3.2.6 Validation de l'AE

L'AE s'authentifie auprès de l'AC avant toute demande, la DPC décrit le mode d'authentification basé sur l'usage de certificat d'authentification de l'AE vis-à-vis de l'AC

3.2.7 Critères d'interopérabilité

La présente PC 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, il n'existe pas de fonction de renouvellement des clés pour cette catégorie de certificat

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

Une demande de renouvellement est traitée comme une demande de création. Par conséquent, un nouveau certificat Porteur ne peut pas être fourni sans renouvellement également de la bi-clé correspondante (cf. § 4.6).

3.3.2.1 Identification et validation pour un renouvellement courant

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

3.3.2.2 Identification et validation pour un renouvellement après révocation

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

La Présente PC autorise que le renouvellement et la révocation ne soit pas fait de manière synchrone, toutefois un délai raisonnable maximum doit être observé.

L'Abonné doit faire connaître à l'AC, du fait qu'il s'agisse d'un renouvellement suite à révocation.

Les cas de révocation (cf. 4.9.1.2) suivantes ne permettent pas de renouveler un certificat d'Organisation :

- cessation d'activité de l'Organisation ou de l'abonné
- fin de la relation contractuelle entre L'abonné et l'AC

3.4 Identification et validation d'une demande de révocation

3.4.1 Certificat à usage unique

Dans le cadre de l'utilisation de certificat ayant une durée de vie de 15 minutes, la révocation ne peut intervenir que lors de son utilisation dans une session de signature ; c'est pourquoi un certificat d'un titulaire ne peut être révoqué que sur la demande du Porteur de certificat tel que décrit au § 4.9, la demande est transmise à l'AE

La demande est transmise de l'AE vers l'AC qui effectue la révocation en direct.

La présente PC ne formule aucune exigence sur l'identification du Porteur qui demande une révocation.

3.4.2 Certificat d'Organisation

Un certificat d'Organisation peut être révoqué par les rôles suivants :

- L'Individu habilité et désigné dans le certificat, ou une personne qui aurait été désignée par lui.
- L'AC émettrice du certificat. L'opération est alors effectuée par un Opérateur d'Enregistrement de l'AC sous la supervision d'un responsable de l'AC

La demande de révocation est faite conformément au § 4.9



4 Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

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 par l'AC. Le consentement préalable du titulaire doit avoir été expressément obtenu par l'Abonné à cet effet, ce à quoi l'Abonné s'oblige avant de procéder à toute demande auprès de l'AC.

4.1.1.1 Certificat d'Organisation

La création d'un certificat Porteur ne peut être demandée que par un Abonné. S'il est différent du représentant légal, l'individu habilité et désigné dans le certificat d'Organisation doit avoir donné son accord préalable signé.

4.1.1.2 Enregistrement de l'Abonné

Lors de la prise d'abonnement au service, L'AC OTU identifie l'Abonné et l'informe au préalable de ses obligations concernant l'identification de ses titulaires. Un contrat spécifique est formé entre l'Abonné et l'AC OTU

L'Abonné signe un contrat qui sera enregistré et conservé par l'AC OTU.

L'AC OTU authentifie les demandes des Abonnés et vérifie leur habilitation à effectuer des demandes de certificat.

La DPC précise les modalités techniques des contrôles de l'Abonné mis en œuvre au moyen de certificats par l'AC OTU

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

4.1.2.1 Certificat à usage unique

Les informations minimum qui doivent faire partie de la demande sont précisées au § 3.2.2.1

La demande est établie par l'Abonné sur la base d'informations qu'il aura collectées de manière fiable auprès du titulaire.

L'Abonné s'engage vis-à-vis de l'AC au travers d'un accord signé, à

- mettre en œuvre un ou plusieurs procédés d'identification vérifiée du titulaire
- Informer l'AC pour avis, des procédés d'identification mis en œuvre
- Informer le titulaire des différentes étapes qu'il devra suivre en vue de l'attribution de certificats à son nom afin de pouvoir signer le document qui lui sera présentée par l'Abonné, au moyen d'une signature électronique
- Mettre en œuvre un ou plusieurs procédés permettant d'obtenir un accord explicite du titulaire pour pouvoir faire dans ce cadre une demande de certificat en son nom auprès de l'AE
- Fournir l'ensemble des informations nécessaires à l'émission du certificat

La demande est transmise directement à l'AE qui la transmet à l'AC

L'AC ne peut être tenu responsable si l'Abonné ne respecte pas les engagements avec l'AC.

L'AC se réserve la possibilité de refuser l'émission de certificat s'il s'avère que les obligations de l'Abonné ne sont pas respectées.

4.1.2.1 Certificat d'Organisation

Les informations minimum qui doivent faire partie de la demande sont précisées au § 3.2.2

Le dossier de demande est établi par le représentant légal de l'Organisation. Le dossier est transmis directement à l'AE. Par ailleurs, l'AE s'assure de disposer d'une information permettant de contacter le futur Porteur du certificat.

L'AC ne peut être tenu responsable si l'Abonné ne respecte pas les engagements qu'il a signés dans l'accord avec l'AC.

L'AC se réserve la possibilité de refuser l'émission de certificat 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 de validation de la demande

4.2.1.1 Certificat à usage unique

L'identité de l'Abonné et du titulaire sont vérifiées conformément aux exigences du § 3.2.2

L'AE effectue les opérations suivantes :

- Valider les données d'identité du titulaire (données correctement présentes),
- Vérifier l'identité de l'Abonné, et vérifier que celui-ci est connu de l'AE
- Vérifier que la demande de l'Abonné est signée électroniquement à son nom

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat. L'AE conserve ensuite une trace de la demande archivée au format électronique.

L'AC produira un certificat contenant les données d'identité du titulaire.

4.2.1.1 Certificat d'Organisation

L'identité de l'Organisation et de l'individu habilité vérifiées conformément aux exigences du § 3.2.2

L'AE effectue les opérations suivantes :

- Valider les données d'identité de l'Organisation et de l'individu habilité au sein de l'Organisation (complétion, exactitude),
- Vérifier la complétude du dossier de demande

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat. L'AE conserve ensuite une trace de la demande archivée au format électronique.

4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe l'Abonné en justifiant le rejet.

4.2.3 Délai d'établissement du certificat

Le traitement d'une demande de certificat est réalisé en « temps-réel ».

Pour les certificats d'Organisation, un document spécifique retraçant la génération du certificat ainsi que les intervenants technique 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

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération du certificat. Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux § 5 & 6. L'AC transmet le certificat produit au Porteur de certificat.

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

L'AC transmet le certificat au Porteur via l'AE en réponse du traitement de la demande de certificat, l'opération est tracée dans les journaux de l'AE, cette transmission vaut notification.

Dans le cas de certificat d'Organisation, le certificat est également transmis à l'Abonné pour validation explicite avant utilisation.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

4.4.1.1 Certificat à usage unique

La présente PC ne formule pas d'exigences sur ce point, un certificat produit par l'AC et utilisé par le Porteur est réputé conforme à la demande de certificat transmise par l'Abonné.

En complément, des contrôles faits par le Porteur permettent de détecter une non-conformité et révoquer le certificat produit, s'il ne correspond pas à la demande de l'Abonné

4.4.1.2 Certificat d'Organisation

Le certificat d'Organisation produit par l'AC est transmis à l'Abonné pour validation avant usage,

L'acceptation explicite est requise par la présente PC en provenance soit du représentant légal de l'Abonné qui a fait la demande, soit de l'individu habilité identifié dans le certificat.

L'acceptation par mail est considérée comme suffisante, l'adresse mail est communiquée lors la demande d'abonnement

L'adresse mail de l'émetteur tient lieu d'authentification de la provenance de l'acceptation du certificat.

Aucune utilisation de certificat d'Organisation par le Porteur, 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.

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

Sans objet.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le Porteur

L'utilisation de la clé privée par le Porteur et du certificat associé est strictement limitée au service de signature indiqué §1.5. Dans le cas contraire, sa responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé du Porteur et du certificat associé est par ailleurs indiqué dans le certificat via les extensions concernant les usages des clés.

4.5.2 Utilisation de la clé publique et du certificat par les partie prenantes

Les utilisateurs et les Abonnés doivent considérer l'usage stipulé sur les certificats produits par l'AC OTU (Cf. § précédent), et refuser toute autre utilisation de certificat, Dans le cas contraire, leur responsabilité pourrait être engagée.



4.6 Renouvellement d'un certificat

Dans le cadre de la présente PC, le renouvellement de certificat (nouveau certificat, sans changement de clé) est interdit.

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 d'un certificat renouvelé

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

Dans le contexte de délivrance de certificat à usage unique, la délivrance d'un nouveau certificat est sans objet.

Pour les certificats d'Organisation, La délivrance d'un nouveau certificat est traitée comme une demande de création. Une nouvelle bi-clé est systématiquement générée.

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

Dans le contexte de certificat d'Organisation, Les bi-clés des Organisations, et les certificats correspondants, sont renouvelées tous les 3 ans. Une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du Porteur (cf. § 4.9, notamment le § 4.9.1 pour les différentes causes possibles de révocation).

A noter que les causes de révocation (cf. § 4.9.1.2) suivantes, conduisent à une interdiction de délivrance d'un nouveau certificat :

- cessation d'activité de l'Organisation
- fin de la relation contractuelle entre l'Organisation et l'AC

4.7.2 Origine d'une demande d'un nouveau certificat

Cf § 4.1.1.1

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

Cf § 4.2.1.1

4.7.4 Notification de l'établissement du nouveau certificat

Cf § 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

Cf § 4.4.1.2

4.7.6 Publication du nouveau certificat

Cf § 4.4.2

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

Cf § 4.4.3

4.8 Modification du certificat

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

4.8.1 Causes possibles de changement d'une bi-clé

Sans objet.

4.8.2 Origine d'une demande d'un nouveau certificat

Sans objet.

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

Sans objet.

4.8.4 Notification de l'établissement du nouveau certificat

Sans objet.

4.8.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.8.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

La Politique de Certification de l'AC OTU n'autorise pas la suspension de certificat, un certificat révoqué ne pouvant être rendu réutilisable.

4.9.1.1 Certificats à usage unique

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

- Les informations du Titulaire figurant dans son certificat lors de son émission, ne sont pas en conformité avec l'identité du titulaire, ou l'usage prévu dans le certificat,
- Une erreur (intentionnelle ou non) a été détectée dans la demande d'Enregistrement du titulaire,
- Un incident est survenu lorsque le Porteur a utilisé le certificat pour une signature dans le cadre de l'usage normal prévue au § 1.4
- Les clés privées ou publiques ne correspondent pas

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance, le certificat concerné doit être révoqué sans délai

Toutefois compte tenu

- de l'utilisation des certificats à usage unique, produits dans le cadre de cette PC
- De la durée de vie courte de tels 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 les certificats à usage unique, la cause de révocation n'est pas publiée

4.9.1.2 Certificats d'Organisation

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat

- Les informations de l'Organisation figurant dans le certificat lors de son émission, ne sont pas en conformité avec l'identité ou l'utilisation prévue dans le certificat,
- Une erreur (intentionnelle ou non) a été détectée dans la demande d'Enregistrement de l'Organisation,
- La clé privée du porteur est suspectée de compromission ou est compromise ou est perdue ou est volée ou le contrôle sur l'utilisation de la clé est suspecté perdu,
- Les informations figurant dans le certificat ne sont plus exactes alors même que la date d'expiration de celui-ci n'est pas atteinte.
- Le Porteur demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du Porteur),
- cessation d'activité de l'Organisation ou de l'abonné,
- fin de la relation contractuelle entre l'Abonné et l'AC,

- Changement de réglementation technique ou juridique ou de recommandation s'appliquant à l'AC ou l'Organisation nécessitant la fin de l'utilisation du certificat.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance, le certificat concerné doit être révoqué sans délai.

Par ailleurs, Worldline peut révoquer de plein droit un Certificat dans les circonstances suivantes :

- non observation de l'une quelconque des obligations résultant du Contrat d'Abonné ou de tout autre document figurant au dossier, par un Titulaire ou l'Abonné, notamment utilisation du certificat, dans des conditions autres que celles prévues dans la présente Politique de Certification.
- Non-respect de la Politique de Certification.

Pour les certificats d'organisation, la cause de révocation est publiée, ceci constitue un moyen d'identifier le type de certificat dans le CRL.

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 (y compris un certificat d'AC pour la génération de certificats ou de LCR) :

- Suspicion de compromission, compromission, perte ou vol de la clé privée,
- Changement de contenu suite à une évolution (correction de non-conformité, évolution du gabarit de certificat, ...),
- Cessation d'activité,
- Évolutions réglementaires sur les algorithmes utilisés.

Worldline décide de la révocation d'une composante de l'IGC **OTU**.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats à usage unique

Seule l'entité « Porteur de certificat » tel que décrit au § 1.3.5, est habilitée à faire une demande de révocation de ce type de certificat dans les conditions prévues au 4.9.1.1

4.9.2.2 Certificats d'Organisation

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

- un représentant habilité de l'Abonné qui dispose des données d'identification / authentification lui permettant d'accéder à cette fonction
- L'AC selon les circonstances indiquées en § 4.9.1.2, c'est alors un Opérateur d'Enregistrement qui effectuera l'opération sous supervision d'un représentant de l'AC

4.9.2.3 Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ou des autres certificats de composantes ne peut être décidée que par Worldline, ou par les Autorités judiciaires via une décision de justice. La révocation est réalisée sans délai.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat à usage unique

La présente PC ne formule pas d'exigence sur l'identification de la demande de révocation, en effet seul le Porteur de certificat tel que décrit au § 1.3.5, est à même de demander une révocation sur la base d'une des causes possibles de révocation qu'il aura détectée.

L'opération est enregistrée dans les journaux d'évènements.

4.9.3.2 Révocation d'un certificat d'Organisation

Un représentant du Porteur ou de l'Organisation contacte un numéro d'appel disponible 7j/7 24h/24.

Un Opérateur va demander des éléments d'identification (nom de l'Organisation et du représentant habilité) et d'authentification (code secret fourni lors de la génération de certificat).

Lorsque les données d'identification et d'authentification sont validées, la révocation est autorisée

L'opération est enregistrée dans les journaux d'évènements.

4.9.3.3 Révocation d'un certificat d'une composante de l'IGC

L'AC précise dans sa DPC de l'AC OTU, les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, cf. § 5.7.3.

4.9.4 Délai accordé au Porteur pour formuler la demande de révocation

Dès que le représentant habilité (Porteur /Organisation) a connaissance d'une des causes possibles de révocation, il formule sa demande de révocation sans délai.

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

4.9.5.1 Révocation d'un certificat de Porteur

La fonction de gestion des révocations est disponible 24h/24 7j/7.

Toute demande de révocation d'un certificat Porteur est traitée immédiatement après sa réception par l'AC OTU.

L'indisponibilité maximum de la plateforme est de 8h/mois

4.9.5.2 Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat de signature de l'AC est organisée par Worldline.

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

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

Cette PC ne formule aucune exigence concernant l'obligation de vérification de la révocation d'un certificat.

4.9.7 Fréquence d'établissement des LCR

La fréquence de publication des LCR est de 24 heures.

4.9.8 Délai maximum de publication d'une LCR

La LCR est publiée dans un délai maximum de 5 minutes suivant sa génération.

4.9.9 Autres moyens disponibles d'information sur les révocations

Sans objet.

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

Sans objet.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

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.

Pour les certificats d'AC, la révocation suite à une compromission de la clé privée fait l'objet d'une information clairement diffusée sur le site Internet de l'AC.

4.9.13 Causes possibles d'une suspension

Dans le cadre de la présente PC, la suspension de certificat 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

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation publique de LCR. Ce sont des LCR au format V2 et publiés en HTTP à l'adresse précisée dans les certificats utilisateurs : extension CRL Distribution Point (cf. § 7.1)

La 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)

Un certificat révoqué et expiré ne figure plus dans la LCR.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7.

L'indisponibilité maximum de la plateforme est de 8h/mois

4.10.3 Dispositifs optionnels

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

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

La fin de relation entre l'Abonné et l'AC se concrétise par la résiliation ou le non renouvellement de l'accord signé avec l'AC.

L'AE ne reconnaît plus les demandes transmises et signées par l'Abonné.

L'AC demande à l'Abonné de révoquer sans délai, son certificat d'Organisation, s'il en utilise un ou plusieurs, cette révocation est vérifiable au moyen du service d'information sur le statut du certificat fourni par l'AC OU

4.12 Séquestre de clé et recouvrement

Le séquestre des clés privées d'AC et des Porteurs est interdit par la présente PC.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.



5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

La DPC fournit les modalités d'application des contrôles sur les points suivants :

- Situation géographique,
- Construction du site,
- Accès physique,
- Énergie et air conditionné,
- Exposition aux liquides,
- Sécurité incendie,
- Conservation des médias,
- Destructeurs des supports,
- Sauvegarde hors site.

Afin de garantir que :

- Les moyens et informations utilisés dans le cadre de la mise en œuvre opérationnelle de l'IGC OTU sont installés dans des locaux dont les accès sont contrôlés et réservés aux personnels 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.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les fonctions opérées sur toutes les composantes de l'AC OTU sont réparties sur plusieurs types d'intervenants afin de veiller à la séparation des connaissances pour les tâches sensibles ou rôles. Les différents types d'intervenants dans l'Organisation de l'AC sont notamment :

- Responsable sécurité,
- Responsable d'application,
- Ingénieurs systèmes,
- Administrateurs HSM,
- Porteurs de secrets,
- Responsable du centre (hébergeant l'AC),
- Témoins (auditeurs).

Les différents rôles sont décrits dans le document « Tableau des rôles et secrets » [ROLES_SECRETS]. Ainsi que dans le document de Key Ceremony, pour les personnes ayant un rôle opérationnel à ce moment.

Leurs tâches respectives sont décrites dans la DPC. Certains intervenants peuvent cumuler plusieurs tâches si cela reste compatible avec la séparation des connaissances.

La DPC précise les mesures mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services de l'AC OTU soient sortis du site sans autorisation.

5.2.2 Nombre de personnes requises par tâches

Selon le type d'opérations effectuées, le nombre et le type de rôles et de personnes devant nécessairement être présentes (en tant qu'acteurs ou témoins) peuvent être différents. L'annexe "Rôles" de la DPC permet de définir le nombre de personnes nécessaires à chaque opération.

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 des personnes extérieures intervenant sur les tâches sensibles. Ces contrôles sont décrits dans la DPC et sont conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC est notifiée par écrit. Ce rôle est clairement mentionné et décrit dans sa fiche de poste.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Les attributions associées à chaque rôle sont décrites dans la DPC et sont conformes à la politique de sécurité.

Les cumuls de rôles de confiance suivants sont interdits :

- Responsable de sécurité et ingénieur système / Opérateur,
- Ingénieur système et Opérateur,
- Contrôleur et tout autre rôle.
- Porteurs de secrets dans la mesure où ils disposeraient de secrets en contradiction avec le § 5.2.2 amenant ainsi à une situation qui diminuerait le nombre de personnes nécessaires à une opération.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Toute personne intervenant dans des rôles de confiance de l'OTU est informée :

- De ses responsabilités relatives,
- Des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

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 jouer un rôle sensible. Ces personnes ne doivent pas avoir de condamnation de justice en contradiction avec leurs attributions. Ils remettent à leur employeur une copie du bulletin n°3 de leur casier judiciaire dans le cadre de la procédure d'embauche réalisée par les services des Ressources Humaines.

5.3.3 Exigences en matière de formation initiale

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

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit la formation nécessaire préalablement à toute évolution dans les systèmes, dans les procédures, dans l'Organisation, etc. en fonction de la nature de ces évolutions.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

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

5.3.6 Sanctions en cas d'actions non autorisées

Le règlement intérieur de chaque entité indique que des sanctions sont applicables en cas de faute. Ceci est rappelé dans l'engagement de responsabilité.

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

Les personnels des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC doivent respecter les exigences énoncées dans les § 5.3.1, § 5.3.2, § 5.3.3 et § 5.3.4.

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 les politiques et pratiques générales de la composante au sein de laquelle il travaille.

5.4 Procédures de constitution des données d'audit

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

Le processus de journalisation est décrit plus en détail dans la DPC. Il 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'événements comprennent explicitement l'identifiant de l'exécutant (logiciel ou Opérateur) de l'opération.

5.4.1 Type d'événements enregistrés

Les événements suivants sont journalisés par l'IGC **OTU** :

- Démarrage et arrêt des systèmes informatiques,
- Démarrage et arrêt des applications,
- Démarrage, arrêt et modification des paramètres de la fonction de journalisation,
- Génération des clés pour les différents composants,
- Changements, corrections ou évolutions des différents composants,
- Réception d'une demande de certificat, de révocation,
- Validation / rejet d'une demande de certificat, de révocation,
- Génération des certificats des Porteurs,
- Transmission des certificats aux Porteurs,
- Révocation des certificats,
- Génération puis publication des LCR.

Les événements propres à la sécurité sont par exemple :

- Les accès physiques dans les locaux hébergeant l'**OTU**,
- Les actions de changements sur la plate-forme technique (maintenance, évolution des logiciels),
- Les changements dans le personnel intervenant sur l'**OTU**,
- Les épurations ou destruction.
- Les actions des Opérateurs dans le cadre de la surveillance et du pilotage,
- Création / modification / suppression de comptes utilisateur et des données d'authentification correspondantes,
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes,
- Événements liés aux clés de signature et aux certificats d'AC (génération lors d'une cérémonie des clés, sauvegarde / récupération, révocation, renouvellement, destruction,...).

Les événements journalisés reprennent l'ensemble des informations permettant de les identifier et de les analyser avec :

- Type d'événement ou d'opération,
- La date et l'heure de l'événement,
- Les intervenants (composante logicielle ou intervention Opérateur),
- Le contexte (opération planifiée avec demandeur, intervention opérationnelle procédurée suite à un dysfonctionnement, ...),
- Le résultat (échec ou réussite),

- Les liens éventuels avec d'autres événements.

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

5.4.2 Fréquence de traitement des journaux d'évènements

La fréquence de traitement sur les journaux d'évènements est décrit dans la DPC.

5.4.3 Période de conservation des journaux d'évènements

La durée de conservation des journaux d'évènements est indiquée dans la DPC.

5.4.4 Protection des journaux d'évènements

La protection des journaux d'évènements est décrite dans la DPC.

5.4.5 Procédure de sauvegarde des journaux d'évènements

La procédure de sauvegarde des journaux d'évènements est décrite dans la DPC.

5.4.6 Système de collecte des journaux d'évènements

Le système de collecte des journaux d'évènements est décrit dans la DPC.

5.4.7 Notification de l'Enregistrement d'un événement au responsable de l'évènement

La notification de l'Enregistrement d'un événement est décrite dans la DPC.

5.4.8 Évaluation des vulnérabilités

Le contrôle effectué sur les journaux d'évènements est décrit dans la DPC.

5.5 Archivage des données

5.5.1 Types de données à archiver

L'archivage est réalisé par l'**AC OTU** afin d'assurer la traçabilité et la non-répudiation des opérations. Les données à archiver sont notamment les suivantes :

- Pour l'AC et l'AE de l'**AC OTU** :
 - Les demandes de génération de certificat,
 - Les demandes de révocation,
 - Les certificats et LCR
- Pour la plate-forme technique de l'**OTU** :
 - 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'événement.
- Pour la documentation :
 - Les manuels de cérémonie de clefs,
 - Les versions et les révisions de la PC et de la DPC.

5.5.2 Période de conservation des archives

Pour l'AC et l'AE, la durée de conservation par défaut des archives des dossiers d'enregistrement est de 8 ans.

Toutefois la durée de conservation des dossiers d'enregistrement peut être modifiée,

- A la demande de l'abonné la durée peut être ramenée à 3 ans
- En cas de cessation de contrat avec le client, la restitution des dossiers d'enregistrement peut être opérée vers l'abonné (tout en conservant une durée minimum de 3 ans)
- Avec une prolongation expresse du client au-delà de 8 ans, justifiée uniquement par des contraintes réglementaires ou légales, et assortie d'une information correspondante auprès des personnes concernées dans les dossiers d'enregistrement

Pour la plateforme technique, la durée de conservation des journaux est de 8 ans.

Pour la documentation ; la durée de conservation des archives est de 3 ans après la fin de validité de l'IGC OTU.

5.5.3 Protection des archives

Durant la période de rétention, les archives sont protégées en intégrité. La DPC précise les mesures prises pour assurer leurs disponibilités et leurs consultations si nécessaire.

La demande d'accès à une archive est faite par le responsable d'application ou le responsable sécurité.

5.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes est équivalent au niveau de protection des archives. Les procédures de sauvegarde et le niveau de protection sont décrits dans la DPC.

5.5.5 Exigences d'horodatage des données

Le § 6.8 précise les exigences en matière de datation / horodatage.

5.5.6 Système de collecte des archives

Les archives sont produites une fois par mois. La DPC précise les moyens mis en œuvre pour collecter les archives ainsi que le niveau de protection associé.

5.5.7 Récupération des archives

Les archives (papier et électroniques) peuvent être récupérées dans un délai inférieur à 2 jours ouvrés.

5.6 Changement de clé d'AC

Le certificat de l'AC OTU a date d'expiration au 31/12/2020. L'AC OTU ne peut émettre de certificat dont les dates de validité (début ou fin) dépassent sa propre date d'expiration.

Dès qu'une nouvelle bi-clé de l'AC OTU est générée, seule la nouvelle clé privée est utilisée pour signer des certificats. Le certificat précédent n'est plus utilisable (y compris pour les LCR).

L'AC ne peut réutiliser la bi-clé précédemment en vigueur, qu'elle aurait fait re-certifié auprès de l'AC racine pour une nouvelle période de validité.

5.7 Reprise suite à compromission et sinistre

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

Les procédures de reconstruction du système informatique ou de remplacement d'un HSM sont indiquées dans la DPC.

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

Si le matériel de l'AC est endommagé ou hors service alors que les clés de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des services de révocation et de publication d'état de validité des certificats (LCR).

Un document de pilotage est disponible auprès du personnel ayant la responsabilité du pilotage opérationnel de l'IGC OTU.

Un test de simulation d'incident avec arrêt de service d'un composant de l'IGC OTU est réalisé au minimum une fois tous les 3 ans.

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 est traité dans le document de pilotage de la composante (cf. § 5.7.2) en tant que sinistre.

Si la clé privée de l'**AC OTU** est compromise ou soupçonnée de l'être ou détruite :

- Après enquête sur l'évènement, Worldline décide de révoquer ou non le certificat de l'**AC OTU**,
- Si le certificat de l'**AC OTU** est révoqué, tous les certificats Porteurs générés sont révoqués,
- Une nouvelle bi-clé est générée et un nouveau certificat d'**AC OTU** est émis,
- Worldline statue sur le plan de communication à destination des Abonnés et utilisateurs de certificats de l'AC.
- Worldline informe la société Adobe sous 2 jours ouvrés de la révocation de son certificat d'AC OTU

5.7.4 Capacités de continuité d'activité suite à un sinistre

La DPC décrit les procédures mises en œuvre en cas de sinistre.

5.8 Fin de vie de l'IGC

5.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'IGC autre que l'AC

La présente PC n'autorise pas le transfert de L'AC vers un tiers.

5.8.2 Cessation d'activité affectant l'AC

Dans le cas où l'AC déciderait d'interrompre son activité, elle en informerait ses partenaires, au moins six (6) mois avant la cessation de l'activité.

Dans ce type de situation, l'**AC OTU** :

- Révoque les certificats qu'elle a signés,
- Révoque son certificat,
- Informe les représentants d'entité des certificats révoqués ou à révoquer,
- Détruit sa bi-clé d'Autorité au cours d'une procédure audité de type Key Ceremony.
- conserve une image de ses données et ses archives.

A l'échéance fixée, l'AC révoque tous les certificats produits et publie une CRL.

De même au niveau de l'AC racine il y a révocation de l'AC OTU et publication d'une ARL.

La CRL publiée une seule fois, couvre la révocation des certificats sur la totalité de leur existence ; ainsi la CRL est paramétrée sur une durée de 3 ans.

Cette CRL reste en ligne à l'adresse habituelle pour une durée de 3 ans.

L'**AC OTU** s'interdit de transmettre ses clés privées.

6 Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

Dans tous les cas explicités ci-dessous, la clé privée d'une entité est toujours produite par l'entité elle-même. Aucune transmission de clé privée n'est autorisée.

6.1.1.1 Clés d'AC

La clé privée de l'AC est mise en œuvre et reste dans les locaux sécurisés de l'IGC OTU (cf. § 5). La génération des bi-clés de l'AC est réalisée dans un module cryptographique HSM, de niveau Critères Communs (CC) EAL 4+.

Les cérémonies de clés se déroulent sous le contrôle de deux (2) personnes (maître de cérémonie et auditeurs) dans les locaux de l'IGC OTU et suivant des scripts préalablement définis. La clé privée de l'AC est mise en œuvre et reste dans les locaux sécurisés de l'OTU.

Les rôles des personnels impliqués dans les cérémonies de clés sont précisés dans la DPC et le document de cérémonies de clés. Les témoins, dont un est externe à l'AC et est impartial, attestent du bon déroulement de la cérémonie sur la base du document décrivant le déroulement de la cérémonie de clés et remis préalablement.

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

Les clés permettant aux composants de l'IGC de s'authentifier, sont générés lors de procédure de cérémonie de clés (en même temps que pour les clés d'AC, ou non). Un document est créé, décrivant le déroulement de la cérémonie de clés, ainsi que les intervenants requis.

6.1.1.3 Clés d'Abonné

L'AC OTU ne produit pas les certificats attachés à la clé privée d'un Abonné, la DPC décrit comment l'Abonné est reconnu par l'AE

L'Abonné est informé des règles à respecter pour s'authentifier auprès de l'AE.

Il appartient à l'Abonné d'obtenir les certificats lui permettant de s'authentifier auprès de l'AC.

L'AC OTU n'est pas responsable de la délivrance de ces certificats.

6.1.1.4 Clés Porteurs générées par l'AC

L'AC OTU ne génère pas les clés des Porteurs.

6.1.1.5 Clés Porteurs générées pour le Porteur

Les bi-clés sont générées par le Porteur de certificat qui en conserve l'usage exclusif.

La DPC décrit les moyens de contrôles et protection, mis en œuvre par le Porteur pour protéger l'usage des clés privées

Le Porteur génère sa bi-clé Dans un boîtier HSM certification selon la spécification FIPS 140-2 level 2 ou supérieur, en respectant les exigences du § 7.1 notamment en matière de longueur de clé.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet

6.1.3 Transmission de la clé publique à l'AC

La clé publique est transmise par le Porteur à l'AC OTU au sein d'un gabarit au format PKCS#10 (CSR) pour la génération du certificat.

6.1.4 Transmission de la clé publique de l'AC aux différents acteurs

Le certificat de l'AC OTU est publié à l'URL :

www.mediacert.com

6.1.5 Tailles des clés

L'AC OTU utilise l'algorithme RSA avec la fonction de hachage SHA-2.

La taille des bi-clés de l'AC OTU est de 2048 bits,

La taille des clés des titulaires et des Organisations est de 2048 bits.

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

La génération des bi-clés de l'AC est réalisée dans un module cryptographique HSM, de niveau CC EAL 4+. Les paramètres de l'équipement de génération de bi-clés (HSM) sont décrits dans le document de cérémonie de clés.

6.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée de l'AC et du certificat associé est strictement limitée à la signature de certificats et de LCR. (cf. 1.5.1.2).

L'utilisation de la clé privée du Porteur et du certificat associé est strictement limitée au service de signature (cf. § 1.5.1.1 & 4.5).

L'utilisation du champ "keyUsage" dans le certificat Porteur est « Non Repudiation ».

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 cryptographique de l'AC

La génération des bi-clés de l'AC est réalisée dans un module cryptographique HSM, de niveau CC EAL 4+ et conforme aux exigences du § 10.4.

6.2.2 Contrôle de la clé privée

Le contrôle de la clé privée de l'AC est assuré par du personnel de confiance (Porteurs de secrets de l'OTU et administrateurs de HSM). L'activation de la clé privée de signature de l'AC se fait via un système de partage de secrets entre plusieurs rôles. Ces procédures sont détaillées dans les manuels de cérémonie de clés et la DPC.

6.2.3 Séquestre de la clé privée

Les clés privées des AC de l'OTU et des Porteurs ne sont pas séquestrées.

6.2.4 Copie de secours de clé privée

Les clés privées des Porteurs (titulaires et Organisation) ne font pas l'objet de copie de secours.

Les bi-clés des AC de l'OTU sont sauvegardées sous le contrôle de plusieurs personnes. Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles (HSM). Les procédures de copie de secours sont décrites dans le document de cérémonie de clés.

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

6.2.5 Archivage de clé privée

Les clés privées des AC de l'OTU et des Porteurs ne sont pas archivées.

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

Les clés d'AC sont générées et stockées dans des ressources cryptographiques matérielles (HSM).

Lorsque l'AC doit transférer une clé privée vers un autre HSM de l'IGC OTU, la procédure de transfert est opérée selon les spécifications du fournisseur des matériels cryptographique (HSM) de l'AC OTU.

Lors d'un transfert, la clé privée est chiffrée avec l'algorithme 3DES. Une clé privée d'AC chiffrée ne peut être déchiffrée sans l'utilisation de composants cryptographiques matériels et l'action des personnes identifiées dans les rôles de confiance.

6.2.7 Stockage d'une clé privée dans un module cryptographique

Les clés privées des AC de l'OTU sont stockées dans des ressources cryptographiques matérielles (HSM) répondant aux exigences du §10.4. Le niveau de sécurité est donc le même que dans le cadre de la génération de ces clés.

6.2.8 Méthodes d'activation de la clé privée

6.2.8.1 Clés privées d'AC

Les clés privées des AC de l'OTU ne peuvent être activées qu'avec deux (2) personnes dans des rôles de confiance et qui détiennent des données d'activation. Cette activation ne peut se faire que dans le cadre d'une cérémonie de clé, documentées et tracées

6.2.8.2 Clés privées des Porteurs

Les clés privées des Porteurs sont générées et stockées dans des équipements cryptographiques matériels(HSM) de niveau FIPS 140_2 level 2 ou plus.

Les clés de titulaires sont générées dynamiquement sur instruction de l'AE sur un unique équipement HSM, utilisées pour une session unique de signature puis détruites dans ce HSM. Cette suite d'opération est tracée dans les journaux de l'IGC

Les clés des Organisations sont générées par des Opérateurs de l'AC OTU lors d'une opération de génération de clé documentée et tracée. La clé est copiée sur les autres équipements HSM dédiés et prévus pour le même usage, en utilisant les processus de clonage préconisée par le fournisseur du HSM.

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 dans le module cryptographique est automatique dès qu'il y a arrêt ou déconnexion du module. Les ressources cryptographiques matérielles sont stockées dans une zone sécurisée sous contrôle.

6.2.9.2 Clés privées des Porteurs

La clé privée du titulaire est détruite après son utilisation.

La désactivation des clés privées de l'Organisation dans le module cryptographique est automatique 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 des AC de l'OTU et les copies de sauvegarde sont détruites par effacement sur la ressource cryptographique matérielle. En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.10.2 Clés privées des Porteurs

La clé privée des titulaires est détruite après une utilisation unique conformément au §1.5, la destruction est tracée par le Porteur de certificat

6.2.11 Niveau de qualification du module cryptographique

Les ressources cryptographiques des AC de l'OTU et de sauvegarde sont évaluées conformément aux exigences du § 10.4.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivages des clés publiques

Les clés publiques de l'AC sont archivées pendant 3 ans au-delà de leur utilisation.

6.3.2 Durée de vie des bi-clés et des certificats

L'AC OTU ne peut pas émettre des certificats Porteur dont la durée de vie est supérieure à celle de son certificat, cf. § 5.6.

- Les bi-clés et les certificats à usage unique ont une durée de vie de 15 minutes.
- Les certificats d'Organisation ont une durée de vie de 3 ans
- L'AC a une date d'expiration au 31/12/2020.

6.3.3 Inventaire des clés

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

La DPC décrit la façon dont l'inventaire est réalisé, le résultat obtenu et les procédures mises en œuvre.

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 des AC de l'OTU sont générées durant les cérémonies de clés (Voir § 5.2.1 et document de cérémonie de clés). Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (cf. § 5.2.1 et document de cérémonie de clés).

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

Les clés privées du Porteur sont générées par lui-même et protégé contre l'usage par un tiers par l'utilisation de HSM de niveau FIPS 140-2 level 2 ou supérieur, en génération et stockage de clé.

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 aux clés privées des Porteurs

La DPC décrit les moyens de protection du mécanisme d'authentification du Porteur pour l'activation /utilisation de sa clé privée.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mécanismes de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Le niveau minimal d'assurance de la sécurité est défini dans la DPC et répond aux objectifs suivants :

- Identification et authentification des utilisateurs pour l'accès au système,
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle 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).

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramètres du système (en particulier des éléments de routage) sont mis en place.

6.5.2 Niveau de qualification des systèmes informatiques

Les systèmes informatiques mis à disposition pour l'IGC OTU sont audités conformément aux spécifications [ETS1102042]

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 du système des composants ainsi que toute modification ou mise à jour sont documentées et contrôlées telles que définies dans la DPC associée.

6.6.2 Mesures liées à la gestion de la sécurité

Toute évolution d'un système d'une composante de l'**OTU** est tracée. Elle est documentée et apparaît dans les procédures de fonctionnement interne de la composante concernée.

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

Sans objet.

6.7 Mesures de sécurité réseau

L'**AC OTU** n'est pas en contact direct avec des réseaux ouverts. Les passerelles permettant les accès sont protégés contre des tentatives d'intrusion ou d'attaque. Ces passerelles limitent les services ouverts et protocoles aux seuls services indispensables au fonctionnement de l'**OTU**. Ces passerelles 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. Les composants du réseau local sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de leur conformité avec les exigences spécifiées par l'AC.

La DPC indique les mesures pour la protection des réseaux.

6.8 Horodatage / Système de datation

Il n'y a pas d'horodatage utilisé par l'**AC OTU**. L'heure système des serveurs de l'IGC **OTU** est utilisée pour dater les événements. Les horloges des systèmes de l'**OTU** sont synchronisées entre-elles par rapport à une source fiable de temps UTC.

La DPC précise la procédure et le contrôle de la synchronisation horaire des systèmes de l'**OTU**.



7 Profils des certificats, OCSP et des LCR

7.1 Profil des certificats

Les certificats émis par l'**AC OTU** contiennent les champs suivants :

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

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

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

7.1.1 Numéro de version

Les certificats des Porteurs sont des certificats X.509 v3.

7.1.2 Extensions du certificat

L'extension peut être critique ou non critique. Si l'extension est critique, l'application utilisatrice à qui le certificat est présenté doit savoir la traiter conformément à son usage. L'application doit rejeter le certificat dans le cas contraire, c'est à dire si elle ne sait pas traiter l'extension ou si l'extension n'est pas conforme à l'usage attendu par l'application.

Si l'extension est non critique, il n'y a pas de rejet du certificat. Dans ce cas l'application peut ignorer l'extension.

7.1.2.1 Certificat de l'AC OTU

Champ de base	Valeur
Version	2 (=version 3)
Serial number	Défini lors de la KC
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C = FR O = Atos Worldline OU 0002 378901946 (siren Worldline) CN = AC Racine - Root CA - 2012
Validity	Expiration au 31/12/2020
Subject	C = FR O = Atos Worldline OU = 0002 378901946 (siren Worldline) CN = AC OTU
Subject Public Key Info	rsaEncryption
Taille des clés	2048 bits
Extensions	Valeur
Authority Key Identifier (non critique)	Identifiant de la clé publique de l'Autorité racine
Subject Key Identifier (non critique)	Identifiant de la clé publique de l' AC OTU défini par l'AC racine
Key usage (critique) : Définition de l'usage de la clé	Signature du certificat, Signature de la liste de révocation de certificats. (Valeur hexadécimale : 0x06)
Certificate Policies (non critique)	1.2.250.1.111.12.4.1 (OID de l' AC Racine - Root CA - 2012)
CPS URI (non critique)	www.mediacert.com
User Notice Text (non critique)	Conformance claim : 0.4.0.2042.1.3 ETSI 102 042 LCP level
Basic Constraints (critique)	Autorité de Certification Profondeur maximale : 0
CRL Distribution Points (non critique)	http://root.mediacert.com/LatestCRL

7.1.2.2 Certificat à usage unique

Champ de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'AC (unique)
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C = FR O = Atos Worldline OU = 0002 378901946 (Siren Worldline) CN = AC OTU
Validity	15 minutes
Subject	CN = civilité [espace] Prénom [espace] Nom du Titulaire [espace] [TraceID] ⁽¹⁾ O = OTU OU = Atos Worldline OU = Nom Abonné serialNumber = ReqTime - DocId – ClientID ⁽²⁾ C = FR
Subject Public Key Info	rsaEncryption
Taille des clés	2048 bits
Extension	Valeur
Subject alt name (non critique)	RFC822 name : Email titulaire du certificat ⁽³⁾
Authority Key Identifier (non critique)	Identifiant de la clé publique de l' AC OTU
Subject Key Identifier (non critique)	Identifiant de la clé publique du certificat, défini par l'AC OTU
Key usage (critique)	nonRepudiation
Certificate Policies (non critique)	1.2.250.1.111.12.7.1.1 URL : www.mediacert.com
CPS URI (non critique)	www.mediacert.com
Basic Constraints (non critique)	Entité finale
CRL Distribution Points (non critique)	http://otu.mediacert.com/LatestCRL

(1)

TraceID : représente l'identification unique du container de trace pour la signature

(2)

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

- **ReqTime** : représente l'heure de demande du certificat
- **DocId** : 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 apparaît)
- **ClientId** : représente l'identification unique du client

La valeur **ReqTime** permet de se prémunir d'un cas de co-signatures par 2 personnes portant le même nom.

La concaténation des trois informations, garantit une valeur unique parmi tous les utilisateurs.
Ce champ a une longueur max de 128 caractères

(3) Le champ **subject alt name** est facultatif et peut ne pas apparaître

7.1.2.3 Certificat d'Organisation

Champ de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'AC (unique)
Signature	sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C = FR O = Atos Worldline OU = 0002 378901946 (Siren Worldline) CN = AC OTU
Validity	3 ans
Subject	CN = Nom Organisation OU = Nom unité dans l'organisation (optionnel) ^[1] OU = Nom Abonné OU = 0002 numéro d'Enregistrement de l'Organisation dans le pays GN = Prénom de l'individu habilité dans l'organisation (optionnel) ¹ SN = Nom de l'individu habilité dans l'organisation (optionnel) ¹ C = pays de l'Organisation
Subject Public Key Info	rsaEncryption
Taille des clés	2048 bits
Extension	Valeur
Subject alt name (non critique)	RFC822 name : Email point de contact Organisation
Authority Key Identifier (non critique)	Identifiant de la clé publique de l' AC OTU
Subject Key Identifier (non critique)	Identifiant de la clé publique du certificat, défini par l' AC OTU
Key usage (critique)	nonRepudiation, digital signature
Certificate Policies (non critique)	1.2.250.1.111.12.7.1.2 URL : www.mediacert.com
CPS URI (non critique)	www.mediacert.com
Basic Constraints (non critique)	Entité finale
CRL Distribution Points (non critique)	http://otu.mediacert.com/LatestCRL

^[1] Au moins l'une des deux informations doit être présente dans le sujet : nom unité dans l'organisation ou nom et prénom de l'individu habilité

7.1.3 OID des algorithmes

L'algorithme utilisé est sha256WithRSAEncryption. Son OID est : 1.2.840.113549.1.1.11.

7.1.4 Forme des noms

Les noms respectent les exigences du § 3.1

7.1.5 Contraintes sur les noms

L'attribut « commonName » (CN) est utilisé et comporte le premier prénom de l'état civil du Porteur. La Présente PC ne formule pas d'exigence sur les prénoms en dehors du premier prénom usuel. Pour les prénoms et noms composés, le tiret est utilisé comme élément séparateur. L'attribut « serialNumber » présent dans les certificats est utilisé pour traiter les cas d'homonymie.

La civilité contient :

- M pour monsieur
- MME pour Madame

Exemple :

- Jean François MARTIN DUPONT => commonName = Jean-François MARTIN-DUPONT M

7.1.6 OID de la PC

cf § 1.2.2

7.1.7 Utilisation de l'extension "contraintes de politique"

La présente PC ne formule pas d'exigence.

7.2 Profil des LCR

7.2.1 LCR et extensions

Les LCR émises par l'**OTU** comprennent les champs suivants :

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

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

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

Les extensions utilisées sont : **Authority Key Identifier** et **CRL Number**. La durée de validité de la LCR est de 7 jours. Les LCR sont publiées toutes les 24 H.

Champ de base	Valeur
Version	1 (=version 2)
Signature	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C = FR O = Atos Worldline OU = 0002 378901946 (Siren Worldline) CN = AC OTU
This Update	
Next Update	This Update + 7 jours
Revoked Certificates	Liste des certificats révoqués <ul style="list-style-type: none"> • userCertificate • revocationDate • revocation cause
Extension	Valeur
Authority Key Identifier (non critique)	Identifiant de la clé publique de l'AC AC OTU
CRL Number (non critique)	Numéro de la LCR, défini par l'AC AC OTU

7.3 Profil OCSP

L'AC OTU ne met pas en œuvre de service de type OCSP

8 Audit de conformité et autres évaluations

La reconnaissance du respect par l'AC des exigences de la présente PC est effectuée par un cabinet d'audit agréé à évaluer l'AC selon les spécifications techniques produites par [ETSI102042], la certification est délivrée par le COFRAC.

La suite du présent chapitre ne concerne que les audits et évaluation de la responsabilité de l'AC.

8.1 Fréquences et / ou circonstances des évaluations

L'AC procède à un contrôle de conformité une fois par an

En cas de modification importante l'AC peut demander un contrôle de conformité anticipé.

8.2 Identités / qualifications des évaluateurs

Le contrôle d'une composante est effectué par une équipe d'auditeurs autorisée à auditer l'AC OTU. Et disposant des habilitations nécessaires pour une évaluation selon les spécifications de [ETSI102042].

8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit (dûment autorisée) est différente de l'équipe gérant l'AC OTU.

8.4 Sujets couverts par les évaluations

Les contrôles effectués par les auditeurs dûment autorisés portent sur l'ensemble de l'AC. Le but est contrôler le respect de la présente PC et de la DPC associée et des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5 Actions prises suite aux conclusions des évaluations

L'équipe d'audit rend son avis au responsable d'exploitation de l'AC. Trois résultats d'audit sont possibles : Réussite / A confirmer / Echec.

8.5.1 Réussite

Si aucune non-conformité n'a été constatée, le responsable d'exploitation confirme la conformité à la composante de l'AC OTU auditée.

8.5.2 A confirmer

En cas de non-conformités mineure, le responsable d'exploitation de l'AC précise à la composante auditée les non-conformités à corriger et sous quel délai. Un contrôle ultérieur de confirmation est ensuite mené pour lever les non-conformités critiques constatées.

8.5.3 Echec

Si échec de l'audit et selon la criticité des non-conformités constatées, les auditeurs recommandent à l'AC :

- Cessation temporaire ou définitive d'activité,
- La révocation du certificat de la composante auditée,
- La révocation de l'ensemble des certificats émis depuis le dernier contrôle positif,
- La révocation du certificat de l'AC.

Le choix de la mesure à appliquer est effectué par Worldline.

8.6 Communication des résultats

Les résultats des contrôles de conformité sont publiés sur le site www.mediacert.com sous la forme d'un document de certification à jour.



9 Autres problématiques métiers et légales

9.1 Tarifs

L'AC OTU ne commercialise pas ses certificats seuls, mais uniquement au travers de services de plus haut niveau.

9.2 Assurance

9.2.1 Couverture par les assurances

Worldline dispose d'une couverture d'assurances pour les risques qui pourraient engager sa responsabilité.

9.2.2 Autres ressources

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

9.2.3 Couverture et garantie concernant les entités utilisatrices

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

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations secrètes

Seuls les Porteurs de secrets ont accès aux données secrètes telles que les informations relatives à la sécurité de l'IGC comme les données d'activation et les clés privées de l'AC et de ses Opérateurs.

9.3.2 Périmètre des informations confidentielles

Les informations suivantes sont considérées comme confidentielles :

- Les informations techniques relatives à la sécurité des fonctionnements des modules cryptographiques et les composantes de l'IGC,
- Les journaux d'évènements de l'AC,
- Les informations de suivi des interventions techniques
- La DPC et les procédures internes d'exploitation,
- Les rapports d'audits.

Seules les personnes habilitées par Worldline et ayant le besoin ou l'autorisation d'en connaître pourront consulter à la demande les informations confidentielles.

L'autorisation est donnée par le responsable d'application de l'IGC OTU

9.3.3 Informations hors du périmètre des informations confidentielles

Les informations non confidentielles de l'AC OTU sont publiques et accessible sur le site www.mediacert.com

Les informations hors périmètre des informations confidentielles sont considérées comme « Document interne » ou « Diffusion restreinte » conformément aux niveaux décrits dans la PSSI Worldline.

9.3.4 Responsabilités en terme de protection des informations confidentielles

La DPC précise les procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au § 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

L'AC respecte la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'Enregistrement à des tiers dans le cadre de procédures légales. Elle donne également l'accès à ces informations au Porteur.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

L'Autorité de Certification veille à la protection des données personnelles conformément à la réglementation, et notamment la loi informatique et Libertés.

La 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 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel s'applique à tous les documents détenus ou transmis par l'AC ou par une des composantes de l'IGC (site de la CNIL <http://www.cnil.fr>).

En vertu de la loi, les personnes physiques disposent d'un droit d'accès, de rectification ou d'opposition des données à caractère personnel les concernant. Ce droit peut être exercé auprès du point de contact de l'AC OTU

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

- Les données d'Enregistrement du titulaire ou des individus habilités telles que fournies par l'Abonné.

9.4.3 Informations à caractère non personnel

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

9.4.4 Responsabilité en termes de protection des données personnelles

L'AC agit conformément à la législation et à la réglementation en vigueur sur le territoire français.

9.4.5 Notification et consentement d'utilisation des données personnelles

Les informations que tout Abonné remet à l'AC sont protégées contre la divulgation sans le consentement de celui-ci. L'AC agit conformément à la législation et à la réglementation en vigueur sur le territoire français.

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

L'AC agit conformément à la législation et à la réglementation en vigueur sur le territoire français.

9.4.7 Autres circonstances de divulgation d'informations personnelles

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

9.5 Droits sur la propriété intellectuelle et industrielle

La législation et la réglementation en vigueur sur le territoire français s'appliquent.
Les documents publics, hors périmètre des informations confidentielles, demeurent propriétés Worldline

9.6 Obligations et Garanties

L'AC s'assure de :

- La protection (intégrité et confidentialité) de la clé privée lors de la génération et durant toute la période de validité de la clé ainsi que des données d'activation,
- L'utilisation des bi-clés et des certificats uniquement dans le cadre des applications définies au § 4.5 dans le respect des engagements,
- Le respect et de l'application de la DPC,
- La soumission aux contrôles de conformité effectués par des auditeurs externes et la mise en œuvre de ses préconisations,
- La mise en œuvre des moyens techniques et humains pour atteindre les engagements pris et notamment le niveau de service spécifié,
- Documenter les procédures internes de fonctionnement,

9.6.1 Autorité de Certification

L'AC a pour obligation de :

- Garantir et maintenir la cohérence entre la DPC et sa PC,
- Contrôler le respect de la PC et DPC de la part de l'AE,
- Collaborer avec les auditeurs lors des contrôles de conformités et la mise en œuvre des éventuelles mesures décidées avec ses auditeurs suite à ces contrôles.

9.6.2 Autorité d'Enregistrement

L'AE a pour obligation de :

- Respecter les procédures d'Enregistrement décrites dans la présente PC et DPC,

9.6.3 Obligations incombant aux Porteurs

Les Porteurs de certificat doivent :

- Protéger l'accès aux clés privées et certificats,
- N'utiliser leurs certificats que pour les usages prévus dans la PC associée,
- Révoquer ou faire révoquer son certificat en cas de compromission ou suspicion de compromission,
- Respecter les exigences des PC's et de la DPC les concernant.

9.6.4 Abonnés

Pour un certificat à usage unique, l'Abonné à l'AC OTU a pour obligation de :

- Collecter les informations d'identité communiquées par le titulaire
- Vérifier les informations d'identité communiquées par le titulaire
- Communiquer au titulaire ses obligations cf 9.6.5.
- Transmettre dans sa demande les données relatives à l'identification du titulaire
- Constituer et signer la demande de certificat du titulaire
- Garder le contrôle exclusif de ses moyens d'authentications auprès de l'AC OTU

- Communiquer dans les meilleurs délais à l'AC OTU tout évènement pouvant porter atteinte à la qualité de l'identification de ses titulaires
- Communiquer dans les meilleurs délais à l'AC OTU tout évènement pouvant porter atteinte à la fiabilité de ses moyens d'authentification
- Informer le titulaire du processus de demande de certificat et des conséquences de son utilisation (signature électronique) dans le cadre de la présente PC

Pour un certificat d'Organisation l'Abonné à l'AC OTU a pour obligation de :

- Compléter le dossier de demande de certificat
- Informer l'AC dans le cas où les données du certificat ne seraient plus valables du fait d'un changement au sein de l'Organisation
- Demander la révocation du certificat dans les cas listés par la PC.
- Communiquer immédiatement à l'AC OTU tout évènement pouvant porter atteinte à la fiabilité de ses moyens d'authentification
- Informer l'AC dans le cas où l'Organisation n'existerait plus

Dans le cas où l'Abonné fait appel à un prestataire technique, il lui appartient de faire respecter ces obligations par ce dernier.

De plus ce prestataire pourra être détenteur de secrets propre à l'Abonné : clé privées correspondants à des certificats d'authentification et de signature de message. Il appartient à l'Abonné de s'assurer que des mesures de protections d'accès à ces secrets sont bien mis en œuvre.

9.6.5 Titulaire

Le futur Titulaire d'un certificat a le devoir de communiquer des informations et justificatifs demandé par l'Abonné, exacts et à jour lors de la demande de certificat.

9.6.6 Utilisateurs de certificats

Les utilisateurs de certificats (personnes ou applications tiers) doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis,
- Vérifier la validité du certificat (non expiré, non révoqué, intégrité),
- Vérifier la validité de chaque certificat de la chaîne de certification,

9.6.7 Autres participants

Sans objet.

9.7 Limite de garantie

L'AC OTU permet via ses services :

- L'authentification de l'AC OTU avec son certificat,
- La génération de certificats conformément à la demande d'un Abonné préalablement authentifié,
- La mise à disposition des informations de validité des certificats selon la présente PC.

- Le contrôle exclusif de la clé privée par le Porteur de certificat la destruction de cette même clé à l'issu d'une session unique d'utilisation (cas des certificats à usage unique).

Aucune autre garantie n'est assurée.

9.8 Limite de responsabilité

La responsabilité de l'AC ne peut être engagée qu'en cas de non-respect de ses obligations.

L'AC ne pourrait en aucun cas être tenu responsable dans le cas d'une faute sur le périmètre d'une entité cliente 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 § 4.5.

L'AC s'engage à émettre les certificats conformément à la présente PC ainsi qu'à l'état de l'art et de la technique.



9.9 Indemnités

La délivrance de certificats par l'AC OTU est opérée dans le cadre de services plus complets de souscription électronique en ligne.

Le contrat cadre signé entre le Client et Worldline ou son mandataire dument habilité précisent les indemnités. 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 PC de l'AC **AC OTU** est effective uniquement après validation par l'entité gérant la PC. Elle reste en application jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée

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

9.10.3 Effets de la fin de validité et clauses restant applicables

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

9.11 Notifications individuelles et communications entre les participants

En cas de changement impactant la présente PC, l'AC devra au plus tard deux mois avant le début de l'opération, en informer les Abonnés.

L'AC informera également les Abonnés au plus tard un mois après la fin de l'opération.

La présente PC ne formule aucune exigence concernant la validation des changements de la part des Abonnés.

Toutes les composantes et acteurs de l'IGC sont tenus informés des amendements effectués sur la PC, et des impacts pour eux.

9.12 Procédures d'amendements

Les révisions de cette PC sont décidées par le comité sécurité gérant la PC. La rédaction de la PC est réalisée par Worldline. Les modifications de forme (orthographe, ...) ne sont pas soumises à validation et la PC peut être mise à jour sans notification préalable.

Le Comité Sécurité est en charge des modifications de cette PC. Il se réunit au moins une fois par an pour répertorier les révisions nécessaires afin de rester conforme aux règles et normes en vigueur. Il est notamment composé des responsables suivants :

- RSSI Worldline Local ou un membre de la même structure au sein Worldline,
- Représentant AC,
- Equipe suivi de conformité des plateformes,

9.12.1 Mécanisme et période d'information sur les amendements

Toutes les composantes et acteurs de l'IGC sont tenus informés des amendements effectués sur la PC, et des impacts pour eux.

9.12.2 Circonstances selon lesquelles l'OID doit être changé

Les OID des politiques de certification seront changés dans les cas suivants :

- Modifications des procédures d'enregistrement qui ne s'appliquent pas aux certificats déjà émis,
- Modifications des procédures de délivrance et de retrait des certificats et qui ne s'appliquent pas aux certificats déjà émis,
- Ajouts ou suppressions de champs ou d'extensions dans les gabarits de certificats,
- Renouvellement des certificats de la chaîne de confiance (AC Racine et/ou fille),
- Reprise suite à compromission de l'AC ou de l'une de ses composantes.

Toute autre modification est évaluée en comité sécurité. Si l'impact est jugé majeur, l'OID est modifié.

9.13 Dispositions concernant la résolution de conflits

La présente PC est soumise au droit français. La rédaction et l'application de la présente PC sont conformes à l'état de l'art, aux textes législatifs et réglementaires.

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

Le contact habilité pour toute remarque, demande d'information complémentaire, réclamation ou remise de dossier de litige concernant la présente PC est le Responsable Sécurité (RSSI) Worldline.

9.14 Juridictions compétentes

Application de la législation et de la réglementation en vigueur sur le territoire français.

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

9.15 Conformité aux législations et réglementations

Application de la législation et de la réglementation en vigueur sur le territoire français.

9.16 Dispositions diverses

9.16.1 Accord global

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

9.16.2 Transfert d'activités

Cf. § 5.8

9.16.3 Conséquences d'une clause non valide

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

9.16.4 Application et renonciation

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

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'AC 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 dûment habilité précisent cette disposition. En l'absence de contrat cadre, les Conditions Générales de Ventes de Worldline s'appliqueront.

9.17 Autres dispositions

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



10.1 Réglementation / normalisation

Référence	Document
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework
[ETSI102 042]	Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates V2.2.1 (2011-12)
[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

worldline
e-payment services

10.2 Document contractuel

Référence	Document
[DPC OTU]	déclaration des pratiques de certification de l'AC OTU Référence : OTU DPC 0003 Version 1.0

10.3 Exigences sur les objectifs de sécurité

Le module cryptographique (HSM), utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, et des LCR) répond aux exigences de sécurité suivantes :

- Assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie,
- Être capable d'identifier et d'authentifier ses utilisateurs,
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné,
- Être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur,
- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance des clés privées,
- Créer des Enregistrements d'audit pour chaque modification concernant la sécurité,
- Si une fonction de sauvegarde et de restauration des clés privée de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

10.4 Exigences sur la qualification

Le module cryptographique utilisé par l'AC pour la génération, le stockage et l'utilisation des clés de l'AC a fait l'objet d'une qualification au niveau renforcé par l'ANSSI

worldline
e-payment services