

**Conditions générales d'utilisation du service  
de délivrance de certificats de Signature électronique de l'Autorité de Certification du TSP Mediacer de  
Worldline par l' Autorité d'Enregistrement externe**

**OBJET**

A. Les présentes conditions ont pour objet de préciser les Conditions Générales d'Utilisation du service de délivrance de certificats de Signature électronique fourni par Worldline, en sa qualité d'Autorité de Certification du TSP Mediacer (Service de Confiance de Worldline), à ses Autorités d'Enregistrement Externes (AEE) .

B. A cet égard, Il est précisé que ces AEE sont le plus généralement :

Elles même les Organisations qui souhaitent pouvoir disposer de Certificats pour le compte de personnes physiques qui les ont mandatées à cet effet (employés, clients ..) dénommés « Titulaires » dans le présent document afin que ces dernières puissent signer électroniquement des Documents (Certificat à usage unique pour réaliser des signatures OTU) ;

Ces Organisations peuvent, en outre, s'appuyer sur des Partenaires qui leur sont rattachés contractuellement, pour distribuer les offres de l'Organisation auprès des propres Clients des Partenaires. Dans ce cadre, les Organisations sont mandatées par les propres Clients des Partenaires pour obtenir la délivrance d'un certificat à usage unique en leur nom qui leur permette de réaliser une signature OTU sur des Documents.

Les présentes conditions générales d'Utilisation comprennent en conséquence les obligations à la charge des Organisations qui se sont constituées comme Autorités d'Enregistrement vis-à-vis de l'Autorité de Certification du TSP Mediacer.

C. La distribution et la gestion des Certificats sont régies par la Politique de Certification – Déclaration des Pratiques de Certification des AC dites « en ligne » qui est sous la responsabilité de L'Autorité de Certification du TSP Mediacer de Worldline. Il est toutefois précisé que la responsabilité d'Autorité d'Enregistrement est assumée ici non pas par l'Autorité de Certification du TSP Mediacer mais par l'Organisation qui possède une expertise dans ce domaine et qui est certifiée à cet effet pour pouvoir opérer ce rôle.

D. Tout au long du document, le terme « PC-DPC » fera référence au document cité dans ce paragraphe.

Cette PC-DPC est référencée sous un identifiant public structuré de la façon suivante :

(OID) : 1.2.250.1.111.20.5.v

1.2.250.1 : OID de haut niveau identifiant l'AFNOR

111 : identifiant Worldline

20 : activité liée au service de confiance

5 : numéro attribué aux PC-DPC des AC dites « en ligne »

v : numéro de version de la PC-DPC.

L'OID courant de la PC-DPC des AC en ligne à la date de publication du présent document est :

(OID) : 1.2..250.1.111.20.5.5

Les versions de PC-DPC peuvent être consultées à l'adresse <https://www.mediacer.com/>

E. La PC-DPC des AC en ligne a été évaluée par un cabinet d'audit indépendant afin de valider la conformité avec la norme ETSI pour l'émission de certificats électroniques au niveau LCP (Lightweight

Certificate Policy). Le référentiel ETSI utilisé pour l'audit de conformité 2020 des AC est la norme EN 319 411-1 comme recommandé, dans le cadre de l'application du règlement européen No 910/2014, pour le maintien de la Certification au niveau LCP.

**1. DEFINITIONS**

Les termes qui suivent auront la signification suivante :

**Autorité de Certification (AC) :** Autorité chargée de l'application de la PC-DPC. L'Autorité de Certification du TSP Mediacer opère les AC dites « en ligne », dans le cadre de la signature de personnes physiques, dénommées :

- MediaCert OTU LCP CA 2018 et Mediacer OTU LCP CA S2 2019;
- Mediacer OTU CA 2019 et Mediacer OTU CA S2 2019 ;

lesquelles régissent les 2 types de Certificats :

- les Certificats à usage unique « standard » émis par les AC MediaCert OTU LCP CA 2018 et Mediacer OTU LCP CA S2 2019;
- les Certificats à usage unique « renforcés » émis par les AC Mediacer OTU CA 2019 et Mediacer OTU CA S2 2019.

On appelle « AC cible » dans le présent document l'AC qui est désignée suivant le type de Certificat émis ou à émettre.

Le terme désigne également les entités techniques qui émettent les Certificats sur demande de l'AEE. Elles sont responsables des Certificats signés en leur nom et assurent les fonctions suivantes :

- publier les informations publiques citées au chapitre 2.2 de la PC-DPC, notamment les présentes Conditions Générales d'Abonnement et les Conditions Générales des Services, de façon durable et sécurisée ;
- garantir le respect de la Politique de Sécurité des Systèmes de l'Information de Worldline par les différentes composantes de celle-ci ;
- rendre accessible ses services à toute Organisation ayant accepté les présentes Conditions Générales d'Utilisation ;
- collaborer avec les auditeurs lors des contrôles de conformité et mettre en œuvre d'éventuelles mesures décidées avec les auditeurs suite aux contrôles de conformité.

Tout au long du document, le terme « les AC » fera référence aux AC dites « en ligne » concernées par la PC-DPC.

**Autorité d'Enregistrement (AE) :** Autorité en charge de la réception des demandes de Certificat des Titulaires, de la vérification de ces demandes conformément aux contrôles décrits dans la PC-DPC en fonction du type de Certificat demandé, de l'archivage de ces demandes et de leur transmission à l'AC cible. L'AE a également pour tâche de réceptionner et de traiter les demandes de Révocation de Certificats.

Dans le cadre des présentes Conditions Générales d'Utilisation, l'Organisation agit comme Autorité d'Enregistrement Externe, dans le cadre de la demande de création de certificat électronique à usage unique. Elle est certifiée aux fins de pouvoir opérer ce rôle et assumer les responsabilités y afférentes.



L'AEE respecte les exigences de l'AC concernant les fonctions de hachage autorisées, disponibles au sein de la PC-DPC.

L'AEE applique la ou les Politique(s) d'Enregistrement qu'elle a établie(s) et mis(es) en place.

La ou les Politiques d'enregistrement de l'AEE s'adapte aux contextes d'émission des Certificats à usage unique tout en respectant strictement les principes et obligations figurant dans la Politique de Certification.

L'Autorité de Certification du TSP Mediacert s'appuie sur les engagements de contrôles d'identité pris par l'AEE, directement ou au travers de ses Rattachés conventionnels, conformément à ce qui est décrit dans le(s) document(s) dénommé(s) Politique d'Enregistrement pour délivrer ses certificats.

Un document de ce type sera établi pour chaque parcours dont les conditions d'identification et/ou de consentement du futur Titulaire diffèrent. Le procédé d'identification étant décrit par l'AEE, il lui appartient de le mettre en œuvre ou de le faire mettre en œuvre sous sa responsabilité. Si des personnes sont désignées et habilitées par l'AEE pour réaliser cette identification sous sa responsabilité, cela doit alors être stipulé par l'AEE dans la politique d'Enregistrement. Il peut s'agir des rattachés conventionnels de l'Organisation. La Politique d'Enregistrement suit les règles décrites au sein de l'ETSI 319411-1 concernant l'identification des titulaires de certificats et détaille les contrôles qui seront mis en place par l'AEE .

Par ailleurs, suivant le niveau de contrôle d'identité mis en place, l'AEE pourra se voir fournir un Certificat à usage unique dit :

- « standard » : où le contrôle d'identité du futur Titulaire est conforme aux exigences imposées par l'ETSI EN 319 411-1 niveau LCP ;
- « renforcé » : où le contrôle d'identité du futur Titulaire est conforme aux exigences imposées par l'ETSI EN 319 411-1 niveau LCP et soumis à des exigences supplémentaires imposées par l'AC.

**L'AEE s'assure du respect du dispositif d'identification décrit dans la ou les Politique(s) d'enregistrement.**

**Authentification** : l'Authentification est un processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique. En résumé, s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité. *ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information.*

**Certificat** : Fichier électronique émis par Worldline, en sa qualité d'Autorité de Certification du du TSP Mediacert .

Suivant le Règlement eIDAS :

- quand il s'agit d'un « certificat de Signature électronique », désigne une attestation électronique qui associe les données de validation d'une Signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne ;

Le Certificat à usage unique désigne un Certificat produit dynamiquement lors d'un processus de Signature électronique. Ce Certificat est utilisé au cours d'une session unique de signature par la plateforme, puis la clé de signature est détruite. Sa durée de vie est limitée à quelques minutes conformément à la PC-DPC applicable. Ce Certificat est généré sur requête de l'AEE pour réaliser une signature à la demande d'un Utilisateur final, sur un Document.

Dans le cadre d'un Certificat à usage unique, en signant le Certificat, l'AC valide le lien entre l'identité de la personne physique et la bi-clé.

Ces Certificats sont signés par les AC en ligne de l'Autorité de Certification du TSP Mediacert de Worldline établi par Worldline.

**Chaîne de confiance** : ensemble de Certificats nécessaires pour valider la filiation d'un Certificat délivré à une entité. Les chaînes de confiance des AC sont présentées au sein de la PC-DPC.

**Clé Privée** : clé d'Authentification, de signature ou de chiffrement, devant être conservée secrète par le Dispositif Porteur de Certificats, qui est associée à une clé Publique contenue dans un Certificat.

**Demande de Certificat** :

L'AEE qui souhaite faire une demande de Certificat à usage unique pour ses futurs Titulaires devra la présenter sous forme électronique. Cette demande est constituée d'un message (requête) signé par l'AEE et conservé par l'AC comme justification de cette demande.

**Dispositif Porteur de Certificat** : composant logiciel qui obtient un (ou des) Certificat(s) porteurs de l'AC et garantit le contrôle exclusif des bi-clés au Titulaire du Certificat et à lui seul. Ces Certificats sont utilisés selon les applications et les types de Certificat pour des usages de Signature électronique.

**Document** : document statique électronique au format PDF.

**Documents Contractuels** : l'ensemble des documents référencés ci-dessous.

**Données d'identification personnelle** : un ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale ;

**Dossier d'enregistrement des Titulaires** :

Désigne l'ensemble des formulaires et des pièces justificatives permettant à l'AEE de justifier l'émission et/ou l'utilisation de certificats électroniques pour réaliser des signatures et qui sont gardés par elle et transmis sur simple demande à l'Autorité de Certification en cas de besoin pour justifier l'émission de certificats

**Élément de preuve** : par opposition à la preuve (notion juridique), on parle d'éléments de preuve pour désigner les données et les documents qui visent à établir la preuve. Il peut notamment s'agir de traces informatiques, de fichiers d'horodatage, de fichiers signés électroniquement ou de tout autre document, fichier, pouvant servir à l'Organisation à démontrer l'existence et la validité de la transaction réalisée.

**Horodatage électronique** : des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant.

**Identification** : action d'établir l'identité d'une personne physique ou morale ou d'une personne physique représentant une personne morale sur la base notamment de justificatifs légaux valides vérifiés.

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

**Journaux d'activité des services** : ensemble des journaux applicatifs du service OTU (production de certificat et signature).

**Jour Ouvré** : tous les jours de la semaine sauf le samedi, le dimanche et les jours fériés.

**Liste des Certificats Révoqués (ou LCR)** : liste de numéros de série des Certificats ayant fait l'objet d'une Révocation. L'url est visible dans le Certificat émis par l'Autorité de Certification du TSP Mediacert de Worldline.



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

**Organisation** : entité représentant notamment une entreprise, une Administration publique, etc. et pouvant faire référence à un nom de marque . Ce terme désigne ici la même société que celle qui s'est constituée comme AEE ; Elles sont désignées de façon distincte comme AEE et comme Organisation pour dissocier les rôles qui leur sont impartis.

Cette Organisation accède dans le cadre de ces conditions Générales d'Utilisation au service de délivrance de Certificats produit par les Autorités de Certification en ligne et peut obtenir la délivrance au choix :

- de Certificats à usage unique « standards » au nom des Titulaires que l'AEE aura préalablement identifiés ou dont elle aura déléguée, par contrat aux Rattachés conventionnels et sous sa responsabilité, l'identification en sa qualité d'Autorité d'Enregistrement.
- de Certificats à usage unique « renforcés » au nom des Titulaires que l'AEE aura préalablement identifiés ou dont elle aura déléguée, par contrat aux Rattachés conventionnels et sous sa responsabilité, l'identification en sa qualité d'Autorité d'Enregistrement.

Les notions de « standard » et « renforcé » pour la qualification des certificats à usage unique sont spécifiés dans la définition d'**Autorité d'Enregistrement** ci-dessus.

**Online Certificate Status Protocol (OCSP)** : protocole de vérification de certificat en ligne, permettant ainsi de vérifier l'état d'un certificat numérique X.509.

**Parcours** : cinématique fonctionnelle menant à la signature OTU d'un ou plusieurs Documents. L'Organisation peut définir plusieurs parcours. Les parcours sont à différencier notamment lorsque les conditions d'identification des titulaires sont différentes, nécessitant la définition et la validation par l'AEE, de Politiques d'Enregistrement distincts.

**Partie** : Worldline et /ou l'Organisation agissant soit comme bénéficiaire du service de certificats de signature électronique soit comme Autorité d'Enregistrement Externe.

**Politique de Certification – Déclaration des Pratiques de Certification (PC-DPC)** : ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses 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.

La PC-DPC décrit d'un point de vue Organisationnel la prestation de Worldline, au travers du TSP Mediacert (Autorité d'Enregistrement et de Certification), de fourniture de Certificats et notamment leur processus d'émission, d'utilisation et de Révocation.

La PC-DPC est disponible en ligne : <https://www.mediacer.com/>

Référence : « WLM-OTU-F002 ».

**Politique de Gestion de Preuves** : Politique de Gestion de Preuves de l'Autorité de Certification est un document qui décrit la politique suivie pour constituer les preuves des échanges électroniques intervenus et les conserver. Les Principes de Gestion de Preuve décrivent les règles, les procédés, le contexte relatif à l'établissement et à la conservation d'Eléments de preuve dans le cadre des services dématérialisés. Ils explicitent les propriétés de sécurité recherchées (intégrité, authenticité, ...) et la façon dont elles sont assurées (certificats de Signature électronique, horodatage, traces informatiques notamment).

**Elle décrit le rôle de l'ensemble des parties qui concourent à la transaction .**

**Politique d'enregistrement** : document établi par l'AEE à l'appui des demandes de Certificat à usage unique, Elle décrit les procédés d'identification des Titulaires, ou utilisateurs finaux, que l'AEE met en œuvre ou dont elle délègue par contrat la mise en œuvre sous sa responsabilité. De ces procédés d'identification dépend l'AC qui sera ciblée. La Politique d'Enregistrement doit se conformer aux exigences décrites au sein du règlement ETSI 319411-1 concernant l'identification des titulaires de certificat et conformément aux exigences de la PC-DPC des AC « en ligne » ;

**Modalités de recueil du consentement** : Il devra être décrit également le procédé permettant à l'AEE de recueillir via l'Organisation en ce compris ses Rattachés conventionnels l'accord explicite et éclairé de l'utilisateur final.(Titulaire) préalablement à toute Demande par l'AEE de Certificat à usage unique pour le compte de l'utilisateur final. Il énonce notamment les actions à réaliser en amont du processus de délivrance de Certificat OTU pour que le Titulaire puisse donner son accord au procédé mis en œuvre, donner son consentement au Document qui lui a été présenté et le signer par voie électronique.

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

**Rattachés conventionnels** : Partenaires ou Organisations qui sont liées par contrat avec l'Organisation pour l'exercice par eux d'un certain nombre d'obligations telles que notamment l'application et le respect de la Politique d'Enregistrement préalablement définie par l'AEE et rappelé par l'Organisation en contrepartie de leur accès au service de délivrance de Certificats à usage unique produit par les AC. Les rattachés conventionnels doivent être expressément mandatés par les Futurs Titulaires pour pouvoir requérir auprès de l'AEE un certificat en leur nom. Ils peuvent aussi être nommés Ayant droit dans le cadre du présent document.

**Représentant habilité** : désigne toute personne physique disposant des pouvoirs de représenter légalement une Organisation. Une preuve de cette habilitation doit être fournie à l'AEE.

**Renouvellement d'un Certificat** : opération qui consiste à générer et mettre à disposition un nouveau Certificat pour un Titulaire. Il n'y a pas de renouvellement dans les AC pour les Certificats à usage unique.

**Révocation** :

Le Certificat peut devenir invalide pour de nombreuses raisons autres que l'expiration naturelle, telle que la perte ou la compromission de la Clé Privée associée au Certificat ou le changement d'au moins un champ inclus dans le nom du Titulaire/détenteur du Certificat. L'opération de Révocation est considérée comme terminée lorsque le numéro de série du Certificat à révoquer et la date de Révocation sont publiés dans la Liste des Certificats Révoqués (LCR). La révocation de certificat n'a pas d'impact sur la validité des Documents signés ou scellés avec ce certificat dans la période qui précède la révocation de celui-ci. Néanmoins, en raison de sa courte durée de vie, un certificat à usage unique ne peut être révoqué dans les délais définis par les engagements de service.

**Service** : service de Certification proposé par Worldline, en sa qualité de Service de Confiance de l'Autorité de Certification du TSP Mediacert pour répondre à des besoins d'émission de certificats pour procéder à la Signature de Documents.

**Site Internet** : site Internet du TSP Mediacert dédié aux Services.

**Signataire** : une personne physique qui crée une Signature électronique;

**Signature électronique** : désigne, en France, selon l'article 1367, alinéa 2 1ère phrase du Code Civil ci-dessous :



« l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. »

Selon le Règlement No 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 : des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer.

Dans le cadre des présentes, la Signature électronique ne constitue pas une signature qualifiée.

**Titulaire** : personne physique ou morale identifiée dans le Certificat comme le détenteur de ce Certificat.

Lorsqu'il s'agit d'un Certificat à usage unique, le Titulaire est ici une personne physique qui a mandaté l'AEE pour obtenir la délivrance de ce type de certificat électronique pour pouvoir signer (client, employé..)ou des Rattachés conventionnels habilités par les Titulaires pour mandater l'AEE à requérir un certificat en leur nom.

**Définition du TSP Mediacert** : Fournisseur de services de confiance comprenant les services de signature électronique, de Cachet électronique, Horodatage, et Archivage.

**Utilisateur final** : désigne la personne physique signataire ayant conclu une transaction avec l'Organisation, ou les Partenaires ou les Organisations, rattachés conventionnellement à l'Organisation et qui utilise le service de signature électronique mis à disposition par l'Organisation. L'Utilisateur final est le Titulaire d'un Certificat à usage unique.

L'Utilisateur final peut bénéficier du Service de fourniture de certificat de signature électronique sous réserve de respecter les prérequis suivants :

- disposer de la capacité juridique lui permettant de s'engager au titre du respect des dispositions applicables à l'utilisation du service ;
- disposer de justificatifs d'identité valides et à jour pour pouvoir s'identifier.

## 2. CONDITIONS PREALABLES A LA CONSTITUTION DE LA QUALITE D'Autorité d'Enregistrement Externe

2.1. L'acceptation de l'attribution de la qualité d'Autorité d'Enregistrement Externe repose sur notamment :

- la signature des présentes Conditions Générales d'Utilisation du service ;
- la fourniture d'une ou plusieurs Politique(s) d'Enregistrement. La désignation ou la nomination de représentants au sein de l'Organisation de l'AEE comme Autorité d'Enregistrement Externe pour les Demandes de Création de Certificats à usage uniques.

2.2. La signature des présentes Conditions Générales d'Utilisation du service de Signature électronique de l'Autorité de Certification emporte reconnaissance, notamment par l'AEE, des obligations contenues dans les présentes clause 12, dans le règlement ETSI EN 319411-1 et dans la PC-DPC.

## 3. CONDITIONS PREALABLES A L'OBTENTION DE CERTIFICATS

Pour obtenir des Certificats, l'AEE doit remplir les formalités suivantes auprès de l'AC :

3.1. L'AEE devra réaliser sa Demande de Création de Certificat auprès de l'Autorité de Certification du TSP Mediacert. L'AEE devra faire son affaire de l'adéquation des Certificats et/ou du niveau de Signature électronique choisi aux besoins de l'Organisation et de ses éventuels Rattachés conventionnels : avant toute demande de création de Certificat, et fera son affaire de ce que le type de Certificat à délivrer dans le cadre du service soit adapté aux règles de délégations internes aux besoins métier

et aux contraintes juridiques de l'Organisation ainsi qu'à celles de ses Rattachés conventionnels.

## 4. POUR LA DELIVRANCE D'UN CERTIFICAT A USAGE UNIQUE

4.1. L'AEE au service de signature utilisant des Certificats à usage unique établit en sa qualité d'Autorité d'Enregistrement une ou des Politiques d'Enregistrement en relation aux obligations figurant au sein de l'ETSI EN 39411-1 et pour laquelle elle est certifiée.

L'AEE qui demande la délivrance de Certificats à usage unique veillera, conformément à la PC-DPC applicable, à mettre en œuvre ou faire mettre en œuvre sous sa responsabilité les procédés d'identification fiable, reconnus des futurs Titulaires de Certificats de ce type, qu'il aura préalablement décrits dans le document susvisé. L'AEE garantit la vérification des informations fournies et la validité des pièces justificatives qui les accompagnent. L'Autorité de Certification du TSP Mediacert n'assume aucune responsabilité à l'égard de l'AEE quant à la forme, l'exactitude, l'authenticité ou l'effet juridique des pièces justificatives collectées et traitées par celle-ci. **Demande de Certificats**. Dans le cas des Certificats à usage unique, le message électronique de l'AEE (requête) à l'AC doit comprendre les informations telles que décrites au chapitre 4.1.2.1 « *Processus et responsabilités pour l'établissement d'une demande de certificat* » de la PC-DPC et doit être signée électroniquement par l'AEE. L'AEE reconnaît que la demande de Certificat qui sera émis au nom du Titulaire contiendra les informations suivantes vérifiées relatives à l'identité du Titulaire : son prénom, son nom, sa date et son lieu de naissance. De plus, la demande de certificat doit respecter les modalités suivantes :

- Taille des bi-clés : 2048 bits
- Fonction de hachage : SHA-256
- Algorithme : RSA.

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

4.3. La durée de validité d'un Certificat à usage unique est définie dans la PC-DPC.

## 5. UTILISATION D'UN CERTIFICAT A USAGE UNIQUE

5.1. L'usage des certificats de ce type doit être conformes à la PC-DPC applicable. En effet, L'AEE veillera à ce que l'Organisation s'oblige à n'utiliser les Certificats délivrés par les AC qu'exclusivement pour les applications permettant l'usage d'un Certificat à usage unique tel que décrit dans la PC-DPC au paragraphe 1.5 « *Usages des certificats* ». En cas de violation de cette obligation, Worldline ne pourra voir sa responsabilité engagée. Entre autre, l'AEE et le porteur de certificat ont l'interdiction d'utiliser les certificats émis si :

- le certificat est expiré ;
- le certificat est révoqué ;
- le certificat est utilisé dans le cadre d'une application autre que celles décrites au chapitre 4.5 « *Usages de la Bi-clé et du Certificat* » de la PC-DPC.

5.2. L'AEE veillera à ce que l'Organisation, en ce compris ses Rattachés conventionnels, présentent la cinématique de Signature électronique mise en œuvre de façon claire à l'utilisateur final. Cet utilisateur final doit pouvoir l'accepter avant qu'elle ne soit mise en œuvre et donner à cette occasion mandat à l'Organisation pour qu'elle puisse requérir pour lui auprès de l'AEE un certificat à usage unique afin de pouvoir signer le ou les Documents qui lui sont présentés.



## 6. REVOCATION D'UN CERTIFICAT A USAGE UNIQUE

Les certificats à usage unique ont une durée de vie inférieure au délai de révocation des certificats émis par le service. Pour cette raison et conformément à la norme ETSI EN 319411-1, la révocation n'est pas autorisée.

## 7. ENGAGEMENTS DE L'AUTORITE D'ENREGISTREMENT EXTERNE

### 7.1. Fourniture de documents

#### Certificats à usage unique

L'Autorité d'Enregistrement Externe, devra établir et valider, la ou les Politiques d'Enregistrement rédigée(s) par lui-même et / ou par ses ayant droit avec son assistance et sous sa responsabilité.

Ce document contient :

- une description écrite du procédé d'identification des Titulaires de Certificat à usage unique. Le procédé d'identification devra comprendre obligatoirement la présentation d'une pièce ou d'une copie de pièce d'identité du Titulaire et des contrôles permettant d'attester de la validité de la pièce, en amont ou au cours du processus de Signature électronique ;
- les modalités de recueil de consentement doivent décrire le procédé permettant à l'Organisation en ce compris ses éventuels Rattachés conventionnels de recueillir l'accord explicite et éclairé de l'utilisateur final sur un certain nombre de points préalablement à toute demande pour son compte de Certificat à usage unique ;
- parmi les points soumis au consentement du Titulaire, figurent notamment :
- l'acceptation du Titulaire pour donner à l'AEE le pouvoir d'initier une requête auprès des AC portant sur l'obtention d'un certificat au nom du Titulaire ;
- l'accord explicite du Titulaire pour que les AC collectent et traitent ses données dans le but de lui fournir un certificat électronique et les conservent en vue de répondre à leurs obligations vis-à-vis des Auditeurs.
- L'accord explicite sur les données qui seront contenues dans le certificat et comportant les données d'identité déclarées et vérifiées du futur titulaire telles que son nom et son prénom ;
- Le consentement explicite du Titulaire aux Conditions Générales de Service (CGS) préalablement communiquées au futur titulaire de Certificat et qui explique les conditions régissant l'utilisation du service de signature électronique.

### 7.2. Obligation générale d'information des Titulaires par l'Organisation.

L'Autorité d'Enregistrement externe veillera à ce que l'Organisation informe l'utilisateur final, en sa qualité de Titulaire, des obligations à sa charge décrites dans les Conditions Générales d'Utilisation du service et dans la PC-DPC. A ce titre, l'Organisation devra garantir fournir préalablement à toute action de l'utilisateur final, les informations nécessaires à sa compréhension des modalités de la procédure de contractualisation, en ligne notamment :

- en l'informant sur la cinématique d'expression de son consentement, le procédé de Signature électronique utilisé et en lui exposant les conséquences juridiques de ses différentes actions dont notamment le traitement par l'AC cible de ses données personnelles ;
- en l'informant de sa possibilité d'abandon de la procédure qu'il a initiée ;

- en l'informant sur les modalités de mise à sa disposition du Document contractuel qu'il a signé, les modalités de conservation de celui-ci ;
- en l'invitant à consulter les Conditions Générales des Services des AC en ligne disponibles en ligne à l'adresse : <https://www.mediacert.com/>.

7.3. **Vérification des Demandes de Création de Certificat.** L'Autorité d'Enregistrement Externe a l'obligation de vérifier l'exactitude et la complétude des informations fournies à l'AC dans le message électronique signé (requête) et qui est nécessaire à l'émission du Certificat à usage unique

7.4. **Pratiques non-discriminatoires.** L'AEE s'engage en outre à ne pas avoir de pratiques discriminatoires dans le cadre des services qu'il délivre et qui pourraient être préjudiciables à ceux fournis par les AC.

7.5. **Respect des obligations par le(s) Titulaire(s) de Certificats à usage unique.** L'AEE s'engage en outre à faire respecter par l'Organisation en relation avec les futurs Titulaires les dispositions qui leur sont applicables et qui découlent des présentes Conditions Générales d'Utilisation et de la PC-DPC en vigueur.

A cet effet, il veillera notamment à s'assurer du respect de ces dispositions par l'Organisation et les Rattachés conventionnels vis-à-vis des Titulaires.

Le Certificat doit être utilisé conformément aux stipulations de la PC-DPC en vigueur.

### 7.6. Information de l'AEE par l'Organisation

#### Certificats à usage unique

L'AEE obtient l'engagement de l'Organisation en ce compris ses rattachés conventionnels de :

- communiquer dans les meilleurs délais à l'Autorité d'Enregistrement Externe tout événement pouvant porter atteinte à la qualité de l'identification de ses futurs Titulaires ;
- communiquer dans les meilleurs délais à l'Autorité d'Enregistrement Externe tout événement pouvant porter atteinte à la fiabilité de ses moyens d'authentification auprès de celle-ci.

## 8. ENGAGEMENTS DE WORLDLINE

8.1. Worldline s'engage à mettre en œuvre les moyens (techniques et humains) nécessaires à la fourniture des Services. Worldline, au travers de l'Autorité de Certification du TSP Mediacer , s'engage à utiliser les clés générées exclusivement pour produire la ou les signatures électroniques nécessaires à l'accomplissement d'une transaction demandée par l'AEE.

8.2. Worldline s'engage, au travers de l'Autorité de Certification du TSP Mediacer et son Dispositif Porteur de Certificats, à utiliser la Clé Privée de l'utilisateur final uniquement aux fins prévues par la PC-DPC.

8.3. Worldline, au travers de l'Autorité de Certification du TSP Mediacer , s'engage à authentifier toute requête de l'AEE portant sur une demande de Certificat et s'engage à conserver notamment la preuve de cette requête.

8.4. Worldline, en sa qualité d'Autorité de Certification du TSP Mediacer , conserve l'ensemble des données nécessaires aux AC définies au chapitre 5.5.2 « Période de conservation des archives » de la PC-DPC, notamment :

- huit (8) ans pour les dossiers constitués depuis les requêtes de l'AEE avec les données des Titulaires concernant les certificats à usage unique ;
- les journaux d'activité des services : dix (10) ans.



8.5. L'intervention de l'Autorité de Certification du TSP Mediacer se limite, à une prestation technique qui permet à l'AEE de fournir à l'Organisation ou ses ayant droit de des certificats de Signature électronique conformément à la PC-DPC applicable. Worldline n'a aucune action sur l'identification des futurs Titulaires qui est à la charge de l'AEE et des Organisations en ce compris leurs ayant-droit sinon celle de demander à l'AEE de respecter et faire respecter les engagements qu'elle a souscrits lors de sa certification dans le cadre de sa Politique d'Enregistrement de manière à ne pas compromettre les engagements de l'Autorité de Certification du TSP Mediacer. Worldline n'a aucune action non plus sur le contenu des éventuels Documents sujets aux services fournis par L'Autorité de Certification du TSP Mediacer, hormis l'insertion de certificats de Signatures électroniques et n'accède d'ailleurs pas au contenu des Documents pour fournir ses services. Worldline ne saurait voir sa responsabilité engagée relativement à la valeur ou la validité du contenu des Documents.

## 9. INTERRUPTION DE SERVICE

L'AEE reconnaît que Worldline, en sa qualité d'Autorité de Certification du TSP Mediacer, peut être amenée à interrompre le Service, en tout ou partie, afin d'en assurer la maintenance ou effectuer des améliorations. L'Autorité de Certification du TSP Mediacer informe dans les meilleurs délais l'Organisation agissant en tant qu'AEE de toute interruption envisagée (notamment par e-mail ou par une information sur le Site Internet) et limite la durée de l'interruption et son impact sur le Service.

L'AEE communiquera cette disposition à l'Organisation en ce compris ses éventuels Rattachés conventionnels

## 10. CONVENTION DE PREUVE

Les Parties conviennent expressément que dans le cadre de leurs relations contractuelles, les messages électroniques datés valent preuve entre elles. Les parties conviennent que dès lors qu'il y a transmission électronique d'un message par un émetteur, à un destinataire, le destinataire est réputé l'avoir reçu par retour d'accusé de réception.

## 11. CONDITIONS FINANCIERES

L'Autorité de Certification du TSP Mediacer ne commercialise pas les Certificats seuls, mais uniquement dans le cadre d'un contrat de service plus global associé à la présente prestation de fourniture de certificats avec AE externe et aux présentes Conditions Générales d'Utilisation. Ce contrat détaille l'ensemble des conditions financières pour la revente du service de fourniture de certificats avec AEE externe par le TSP Mediacer de Worldline.

## 12. RESPONSABILITE DE L'AUTORITE D'ENREGISTREMENT EXTERNE ET GARANTIE PAR CELUI-CI

### 12.1. Responsabilités

L'AEE demeure à l'égard de Worldline, en sa qualité d'Autorité de Certification du TSP Mediacer, l'unique responsable du bon accomplissement des étapes d'identification et d'Authentification des Titulaires et en sa qualité d'Organisation responsable de l'adéquation du choix du procédé électronique de signature à ses besoins et ceux de ses éventuels Rattachés conventionnels.

Worldline, en sa qualité d'Autorité de Certification du TSP Mediacer n'est pas destinataire des justificatifs recueillis par l'AEE en ce compris ceux collectés l'Organisation et ses éventuels Rattachés conventionnels, à l'appui de l'identification des Titulaires, l'AEE garde les preuves de ce contrôle conformément à l'exigence de la réglementation ETSI EN 319411-1.

### 12.2. Garanties

Cas où l'AEE et l'Organisation sont les mêmes.

L'Organisation agissant comme AEE et comme bénéficiaire du service de certificats de signature électronique garantit Worldline, en sa qualité d'Autorité de Certification du TSP Mediacer, contre toute action, réclamation ou demande qui pourrait être introduite à son encontre par un Titulaire ou un tiers, et tout dommage en résultant, ayant, directement ou indirectement, comme origine ou fondement le non-respect par l'AEE ou l'Organisation, ses ayant droit ou un Titulaire de l'une quelconque des dispositions qui leur est applicable résultant des Conditions Générales d'Utilisation du service, de la PC-DPC en vigueur, et des documents y afférents tels que repris à l'article 14.

L'Organisation, bénéficiaire du service en ce compris ses rattachés conventionnels, garantit l'Autorité de Certification du TSP Mediacer d'une façon générale que le contenu des documents transmis par lui et/ou ses rattachés conventionnels est licite et ne permet pas d'effectuer des actes contraires aux lois et réglementations applicables et en vigueur.

l'AEE et l'Organisation s'interdisent de prendre un engagement au nom et pour le compte de l'Autorité de Certification du TSP Mediacer auquel elles ne sauraient en aucun cas se substituer.

## 13. RESPONSABILITE DE WORLDLINE ET GARANTIE PAR CELLE-CI

### 13.1. Responsabilités

L'Autorité de Certification du TSP Mediacer fournit une prestation technique.

L'Autorité de Certification du TSP Mediacer n'a pas d'action sur le contenu des Documents émis par celui-ci, hormis l'éventuelle insertion par les AC de l'Autorité de Certification du TSP Mediacer de certificats de Signatures sur lesdits Documents et ne saurait en conséquence être tenue pour responsable des contenus et informations qu'ils contiennent.

La responsabilité de l'Autorité de Certification du TSP Mediacer de Worldline est limitée aux dommages matériels directs qui pourraient être occasionnés du fait du TSP Mediacer à l'Organisation comme AEE et bénéficiaire du service de certificats de signature électronique ou à l'AEE si le bénéficiaire du service est une Organisation liée à l'AEE à l'exclusion de tout dommage indirect (en ce compris notamment préjudice de tiers)

Au cas où la responsabilité de Worldline en sa qualité de prestataire de confiance serait retenue, il est expressément convenu que Worldline ne pourra être tenue à réparation que dans la limite d'un montant qui ne saurait excéder le montant précisé dans le Contrat de prestations de Service dans lequel la présente prestation est revendue joint aux présentes Conditions Générales d'Utilisation.

Worldline n'assume aucune responsabilité quant aux conséquences des retards, altérations ou pertes que pourrait subir l'AEE ou l'Organisation dans la transmission de tous messages électroniques, lettres ou documents.

Worldline ne pourra voir sa responsabilité engagée en cas d'interruption, totale ou partielle, du Service conformément à l'article 9 ci-dessus.

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

L'Autorité de Certification du TSP Mediacer ne pourra être tenu responsable dans le cas d'une faute sur le périmètre de l'AEE, notamment en cas :

- d'utilisation d'un certificat expiré ;
- d'utilisation d'un certificat révoqué ;
- d'utilisation d'un certificat dans le cadre d'une application autre que celles décrites au chapitre 4.5 « Usages de la Bi-clé et du Certificat » de la PC-DPC.



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

Pour le cas où la responsabilité de Worldline serait engagée en qualité d'Autorité de Certification en cas de manquement de l'Organisation et ou de l'AEE en ce compris l'ensemble de ses ayant droit, à l'une des obligations mises à leur charge, l'Organisation se subrogerait à Worldline pour tout règlement des différends ou toute action judiciaire qui pourrait en résulter provenant d'un Ayant droit, d'un Utilisateur ou d'un tiers.

### 13.2. Force majeure

Worldline ne saurait être tenue responsable des pertes, dommages, retards ou manquement à l'exécution d'obligations résultant des Conditions Générales lorsque les circonstances y donnant lieu relèvent de la force majeure au sens de l'article 1148 du Code civil. Les Parties conviennent, en outre, que seront assimilables à un cas de force majeure: décisions d'une autorité publique, modifications législatives et/ou réglementaires, fait de tiers imprévisible ayant causé des dommages rendant impossible la fourniture du Service. Dans l'hypothèse où le cas de force majeure empêche l'exécution par l'une des Parties de ses obligations pour une durée supérieure à deux (2) mois, chacune des Parties pourra résilier le présent Contrat, de plein droit et sans formalité judiciaire, sans que l'autre partie ne puisse prétendre à aucune indemnité.

### 13.3. Garanties

Worldline, en sa qualité d'Autorité de Certification du TSP Mediacert, garantit à l'AEE et l'Organisation que les services fournis sont conformes à la PC-DPC applicable accessible sur le Site internet du TSP Mediacert au jour de l'utilisation du Service;

Il est rappelé que Worldline ne peut se substituer à l'Organisation dans le choix du niveau de service de certificats souscrit en lien aux régimes juridiques applicables aux Documents métier pour lesquels l'Organisation a décidé de recourir à de la Signature électronique.

En conséquence, la fourniture du Service par Worldline ne saurait dispenser l'AEE et l'Organisation d'une analyse et de vérifications concernant les exigences légales ou réglementaires en vigueur afférentes auxdits Documents métier.

L'Autorité de Certification du TSP Mediacert s'engage à émettre des certificats en conformité avec la PC-DPC concernée, ainsi qu'avec l'état de l'art et de la technique.

L'Autorité de Certification du TSP Mediacert garantit via ses services :

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

## 14. MODIFICATION DES DOCUMENTS ET CONDITIONS CONTRACTUELLES

### Evolutions documentaires du fait de contraintes externes

#### 14.1. Conditions Générales d'Utilisation.

Les Conditions Générales d'Utilisation ayant vocation à évoluer pour tenir compte de

contraintes légales, techniques, ou commerciales feront l'objet de mises à jour.

L'Autorité de Certification du TSP Mediacert devra dans cette hypothèse modifier ou actualiser les présentes Conditions Générales par simple mise à jour du contenu, pour tenir compte de ces évolutions.

L'Autorité de Certification du TSP Mediacert notifiera, via un communiqué par e-mail signé, les mises à jour opérées sur les Conditions Générales d'Utilisation au plus tôt.

Cette notification précisera la date de prise d'effet desdites mises à jour.

#### 14.2. PC-DPC et/ou les Conditions Générales des Services.

En cas de changement impactant la PC-DPC et/ou les Conditions Générales des Services des AC en ligne en vigueur, les Abonnés seront informés, via un communiqué par e-mail signé, au plus tard un (1) mois avant la publication de la nouvelle version du document modifié conformément au changement l'impactant. Cette notification précisera la date de prise d'effet desdites mises à jour.

14.3. Toute notification de convention expresse entre les parties sera valablement faite auprès de l'Organisation, et ou l'AEE à leur adresse e-mail renseignées ou ou par simple courrier ordinaire .

14.4. En cas de changement susceptible d'impact majeur, ces mises à jour seront notifiées à l'Organisation et ou l'AEE conformément au paragraphe 9.11 « *Notifications individuelles et communications entre les participants* » de la PC-DPC.

14.5. Les documents susvisés mis à jour seront par ailleurs disponibles et accessibles en ligne dès l'entrée en vigueur de ces derniers à l'adresse suivante : <https://www.mediacer.com/>

14.6. L'Organisation et ou l'AEE en ce compris ses ayant droitS est informée qu'elle a la possibilité de sauvegarder et/ou d'imprimer les Conditions Générales d'Utilisation applicables.

14.7. **Evolutions documentaires du fait du TSP Mediacert.** Les modifications apportées à un Document Contractuel à l'initiative du TSP Mediacert seront portées à la connaissance de l'Organisation et ou l'AEE par tout moyen, au moins un (1) mois avant leur entrée en vigueur.

14.8. **Autres évolutions.** Si des évolutions s'avérant nécessaires dans le cadre du service devaient avoir une incidence sur l'économie du contrat de , prestations de services de plus haut niveau qui a été conclu avec l'Organisation, l'AEE et ou l'Organisation aura alors la possibilité de résilier son contrat en cas de désaccord, sans aucune pénalité à sa charge. En l'absence de résiliation et si le(s) Titulaire(s) continue(nt) à utiliser le service ou le(s) Certificat(s) à l'expiration du délai ci-dessus, l'Organisation et ou l'AEE sera réputée(s) avoir accepté lesdites modifications.

## 15. DUREE

L'acceptation des présentes Conditions Générales d'Utilisation prend effet à compter de sa date de signature par l'Organisation agissant comme AEE et comme Organisation pour une durée indéterminée, sans toutefois dépasser la durée du contrat de prestations de services de plus haut niveau associé.

## 16. RESILIATION

16.1. L'acceptation des présentes Conditions Générales d'Utilisation pourra être résiliée, de plein droit et sans formalité judiciaire, par lettre recommandée avec avis de réception (LRAR), par l'Organisation, l'AEE, ou l'Autorité de Certification :

- pour convenance, suivant le respect du préavis stipulé au Contrat de prestations de Service de plus haut niveau associé ;
- sans préavis, en cas de manquement par l'autre partie à l'une quelconque de ses obligations contractuelles, s'il n'a



pas été remédié au manquement dans un délai d'un (1) mois à compter d'une mise en demeure par lettre recommandée avec avis de réception (1<sup>ère</sup> présentation) restée sans effet ;

- en cas de force majeure, dans les conditions décrites à l'article 13.2 du présent document ;
- de plein droit, en cas de résiliation du Contrat de prestations de Services de plus haut niveau associé à la présente prestation.

16.2. En cas de résiliation des présentes Conditions Générales d'Utilisation et à la date d'effet de la résiliation, l'accès au service sera coupé. L'AEE s'interdit de faire une demande de création de Certificat auprès de l'Autorité de Certification à la date d'effet de la Résiliation.

## 17. PROPRIETE INTELLECTUELLE

La mise à disposition d'un Certificat ne confère aucun droit de propriété à l'Organisation, l'AEE ou aux Titulaires sur le Certificat.

## 18. PROTECTION DES DONNEES PERSONNELLES

18.1. **Certificats à usage unique.** Dans le cadre des certificats à usage unique, il est rappelé que l'AEE en ce compris l'Organisation et ses Rattachés conventionnels veillera à obtenir l'acceptation expresse des futurs Titulaires, avant de transmettre les données personnelles de ces futurs Titulaires à l'Autorité de Certification du TSP Mediacert pour le traitement des demandes de création de Certificats de ce type.

A cet effet, le futur Titulaire devra accepter que les données personnelles le concernant recueillies par l'AEE fassent l'objet d'un traitement informatique aux seules fins de :

- constituer son identification et permettre son authentification par l'AEE afin de permettre à l'Autorité de Certification du TSP Mediacert de générer un certificat en son nom ;
- pouvoir lui communiquer les données d'activation de sa Clé Privée, le cas échéant ;
- permettre d'étayer ses obligations de tiers de confiance. De son côté, l'Autorité de Certification du TSP Mediacert conservera les données personnelles strictement nécessaires à l'exercice de son rôle en sa qualité d'Autorité de Certification, soit :
  - Le nom et prénom du titulaire
  - La date de naissance du titulaire

Il est en effet précisé que toute opposition à la conservation de données à caractère personnel empêchera la délivrance de ce type de Certificat. En effet, en acceptant la fourniture du Certificat pour procéder à une Signature électronique, le Titulaire accepte que l'AEE conserve, les données à caractère personnel pendant la durée nécessaire à l'exercice des finalités des traitements opérés dans le cadre de la fourniture et la gestion du Certificat à usage unique. De même, l'Autorité de Certification les conservant pendant la durée de huit (8) ans.

18.2. L'AEE veillera à ce que l'Organisation en ce compris ses éventuels Rattachés conventionnels communique aux Titulaires les conditions d'exercice de leurs droits auprès de l'AEE pour les données conservées dans les certificats auprès du TSP Mediacert de Worldline à l'adresse indiquée ci-dessous :

Comité Mediacert  
Worldline  
23, rue de la Pointe  
Zone Industrielle A  
59113 Seclin  
France  
[dl-mediacer-tsp@worldline.com](mailto:dl-mediacer-tsp@worldline.com)

18.3. L'AEE rappellera aux Titulaires qu'ils disposent dans les conditions légales applicables d'un droit d'accès, de rectification, de suppression et d'opposition relatifs aux données personnelles qu'ils lui ont communiquées pour permettre l'émission d'un certificat électronique de signature à leur nom et qu'ils peuvent exercer ces droits principalement auprès de l'AEE et auprès du TSP Mediacert de Worldline pour les données personnelles traitées à l'occasion des certificats émis à l'adresse indiquée ci-dessous :

Comité Mediacert  
Worldline  
23, rue de la Pointe  
Zone Industrielle A  
59113 Seclin  
France  
[dl-mediacer-tsp@worldline.com](mailto:dl-mediacer-tsp@worldline.com)

Ce droit de rectification, de suppression et d'opposition ne doit pas cependant faire obstacle au droit de garder les données permettant d'établir la preuve d'un droit ou d'un contrat aussi longtemps que la finalité pour laquelle ces données sont conservées l'exige.

18.4. Worldline a mis en œuvre et respecte des procédures de protection des données personnelles pour garantir la sécurité des données transmises par l'AEE concernant les Titulaires;

- Il appartient à l'AEE d'obtenir des Titulaires, personnes physiques, leur acceptation pour que les données personnelles les concernant recueillies par elle aux fins de les identifier et les authentifier, soient transmises à l'AC pour faire l'objet d'un traitement informatique, en vue de permettre la délivrance par l'AC de Certificats au nom des Titulaires, ceci afin que les Titulaires puissent signer en ligne les Documents présentés par l'Organisation. Il est précisé que les données personnelles communiquées par les Rattachés conventionnels à l'AEE pour être ensuite transmises à l'AC doivent, de la même manière, avoir été soumises aux mêmes procédures d'autorisation et de consentement, de telle manière que l'AC puissent les traiter.

18.5. Les Titulaires doivent garantir sur l'honneur à l'AEE l'exactitude des données qu'ils transmettent à cet effet. Les Titulaires doivent être informés de leurs droits de faire rectifier les informations les concernant en cas de survenance de modification de ces informations.

18.6. Les Titulaires doivent être informés de la nature des informations les concernant, qui sont conservées par l'AEE et l'AC dans le cadre de la mise en œuvre des services de l'Autorité de Certification du TSP Mediacert et donner leur accord préalable au traitement.

18.7. Les Titulaires doivent être informés des éléments tracés pour apporter si besoin la preuve des échanges électroniques réalisés. Ces informations sont détaillées dans la Politique de Gestion de Preuves, disponible sur demande électronique (e-mail). Elles comportent le descriptif des traces gardées par l'Autorité de Certification

18.8. Les Parties s'engagent à respecter les dispositions de la loi Informatique et Libertés du 6 janvier 1978 n° 78-17 relative à l'informatique, aux fichiers et aux libertés sur la protection des données personnelles. A ce titre, chacune des Parties s'engage à assurer la sécurité des données personnelles lors de leur transmission à l'autre Partie quel que soit le support de transmission utilisé conformément à la loi précitée.

Chacune des Parties est responsable de ses propres fichiers et assume l'entière responsabilité des traitements qui y sont appliqués.

18.9. Les Parties s'engagent à respecter les lois qui leur sont applicables.



Les Parties garantissent le respect des obligations figurant au présent article par l'ensemble de leur personnel, leurs mandataires ou rattachés conventionnels et toute autre personne dont elles sont responsables.

18.10. Les obligations figurant au présent article valent pour la durée du présent Contrat et sans limitation de durée après son expiration.

18.11. Les Parties conviennent de se communiquer toutes informations utiles au bon déroulement des opérations traitées, dans le respect notamment de la loi Informatique et Libertés et du RGPD.

## 19. DOCUMENTS CONTRACTUELS

19.1. Le présent Contrat est constitué des documents, qui forment un ensemble indissociable, énumérés ci-dessous :

- les présentes Conditions Générales d'Utilisation au service de délivrance de certificats de Signature électronique ;
- la ou les Politique(s) d'Enregistrement de l'AEE ;
- la Politique de Certification – Déclaration des Pratiques de Certification disponible en ligne à l'adresse définie en Article 1.
- Le contrat de Prestations de services auquel les présentes Conditions renvoient en Article

Par ailleurs, il s'inscrit dans le processus d'attribution de la qualité d'AEE comme défini à l'article 2 du présent document.

19.2. L'ensemble des documents susvisés constitue le cadre technique dans lequel s'effectuera le service de délivrance de certificats de Signature électronique à l'Organisation. Il est complété des dispositions du contrat de service de plus haut niveau précisant notamment l'article 11 des présentes portant sur

les conditions financières, l'article 15 portant sur la durée, l'article 12 et 13 portant sur la Responsabilité du TSP Mediacert de Worldline, de l'Organisation et de l'Autorité d'Enregistrement Externe.

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

## 20. LOI APPLICABLE

Il est précisé que l'interprétation, la validité et l'exécution du présent Contrat sont soumises au droit français.

Les services de L'Autorité de Certification du TSP Mediacert , , dans toutes ses composantes y compris documentaires sont régis par la législation et la réglementation en vigueur sur le territoire français qui lui est applicable, bien que ses activités qui découlent de la PC-DPC associée aux présentes Conditions Générales puissent avoir des effets juridiques en dehors du territoire français.

Par ailleurs, seule la version française des documents contractuels, énumérés à l'article 19.1 du présent document, est opposable aux parties, même en présence de traductions. En effet, les traductions de convention expresse sont prévues à titre de simple commodité et ne peuvent avoir aucun effet juridique.

## 21. REGLEMENT DES LITIGES

En cas de litige relatif à l'interprétation, la formation ou l'exécution du présent contrat et faute de parvenir à un accord amiable, tout différend sera porté devant les tribunaux compétents de Paris.

