Conditions générales d'abonnement au service de Signature électronique et / ou Cachet électronique

OBJET

A. Les présentes conditions ont pour objet de préciser les Conditions Générales d'Abonnement au service de Signature électronique et/ou Cachet électronique fourni par Worldline, en sa qualité de TSP Mediacert (Service de Confiance de Worldline), à ses Abonnés.

B. Il est précisé que ces Abonnés sont :

- soit des Organisations agissant pour elles-mêmes ou pour le compte d'autres Organisations qui les ont mandatées à cet effet, pour assurer par la délivrance d'un Certificat au nom de leur Organisation, l'Authentification de l'origine des Documents émis et la garantie de leur intégrité (Certificat d'Organisation ou Cachet électronique) ;

- soit des Organisations qui contractent avec Worldline pour 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) ; soit des Personnes Physiques agissant pour elles-mêmes, pour assurer par la délivrance d'un Certificat à leur nom afin qu'elles puissent signer électroniquement des Documents (Certificat Permanent) ;

Ces Abonnés peuvent, en outre, s'appuyer sur des Partenaires qui leur sont rattachés contractuellement, pour distribuer les offres de l'Abonné auprès des propres Clients des Partenaires. Dans ce cadre, les Abonnés sont mandatés 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.

C. La distribution et la gestion des Certificats, quelle que soit le type de Certificats (à usage unique , d'Organisation ou Permanent), sont régies par la Politique de Certification – Déclaration des Pratiques de Certification des AC dites « en ligne » qui est sous la responsabilité du TSP MediaCert de Worldline. 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 services 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.mediacert.com/

D. 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 :

Abonné : désigne la société signataire du Contrat d'Abonnement joint aux présentes, inscrite au service de délivrance de Certificats produit par les Autorités de Certification en ligne et qui souhaite obtenir la délivrance au choix**:**

- de Certificats d'Organisation « LCP » ou « NCP » au nom d'Organisations qui dépendent de l'Abonné ou au nom d'Organisations qui lui donnent expressément mandat à cet effet ;

- de Certificats Permanents au nom des Personnes Physiques dénommées aussi 'Abonné', dont l'identification aura préalablement été contrôlée ;

- de Certificats à usage unique « standards » au nom des Titulaires qu'il aura préalablement identifiés ou dont il aura délégué, par contrat aux Rattachés conventionnels et sous sa responsabilité, l'identification.

- de Certificats à usage unique « renforcés » au nom des Titulaires qu'il aura préalablement identifiés ou dont il aura délégué, par contrat aux Rattachés conventionnels et sous sa responsabilité, l'identification.

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

Autorité de Certification (AC) : Autorité chargée de l'application de la PC-DPC. Le TSP MediaCert opère les AC dites « en ligne » dénommées :

- MediaCert OTU LCP CA 2018 et Mediacert OTU LCP CA S2 2019;
- Mediacert OTU CA 2019 et Mediacert OTU CA S2 2019 ;
- Mediacert ORG CA 2019 et Mediacert ORG CA S2 2019 ;
- Mediacert ORG NCP CA 2019 et Mediacert ORG NCP CA S2 2019 ;
- Mediacert PERM CA 2019 et Mediacert PERM CA S2 2019 ;
- AC OTU ;

lesquelles régissent les cinq types de Certificats :

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

- les Certificats à usage unique « renforcés » émis par les AC 2019Mediacert OTU CA 2019 et Mediacert OTU CA S2 2019;

- les Certificats d'Organisation « LCP » émis par les AC Mediacert ORG CA 2019 et Mediacert ORG CA S2 2019 ;

- les Certificats d'Organisation « NCP » émis par les AC Mediacert ORG NCP CA 2019 et Mediacert ORG NCP CA S2 2019 ;

- les Certificats Permanents émis par les AC Mediacert PERM CA 2019 et Mediacert PERM CA S2 2019.

Paraphe

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'Autorité d'Enregistrement. Elles sont responsables des Certificats signés en leur nom et assurent les fonctions suivantes :

- contrôler le respect de la PC-DPC en vigueur par l'Autorité d'Enregistrement agissant au nom des AC en ligne ;
- 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 tout Abonné ayant accepté les présentes Conditions Générales d'Abonnement ;
- collaborer avec les auditeurs lors des contrôles de conformité et mettre en œuvre d'éventuelles mesures décidées avec les auditeurs suite aux contrôles de conformité.

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 de l'Abonné, 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, la responsabilité de l'AE incombe au TSP Mediacert, qui s'appuie sur les engagements de contrôles d'identité pris par l'Abonné, directement ou au travers de ses Rattachés conventionnels et qui sont décrits dans la ou les Politiques d'identification de l'Abonné, qui peuvent être différentes suivant les contextes d'émission de Certificats à usage unique.

La délivrance de Certificat à usage unique nécessite que l'Abonné, directement ou au travers de ses Rattachés conventionnels, ait préalablement identifié les demandeurs de ce type de Certificats conformément au dispositif qu'il a décrit dans le document dénommé « *Politique d'identification OTU et modalités de recueil du consentement* » fourni sous forme de formulaire par le TSP MediaCert et qu'il s'est engagé à compléter et suivre. Un document de ce type sera établi pour chaque parcours d'un même abonné dont les conditions d'identification et/ou de consentement diffèrent. Le procédé d'identification étant décrit par l'Abonné, il lui appartient de le mettre en œuvre ou de le faire mettre en œuvre sous sa responsabilité. Si des personnes sont désignées et habilitées par l'Abonné pour réaliser cette identification sous sa responsabilité, cela doit alors être stipulé par l'Abonné dans la politique d'identification qu'il fournit à l'Autorité d'Enregistrement

Le document « *Politique d'identification OTU et modalités de recueil de consentement* » décrit par l'Abonné a dû être accepté, avant sa mise en œuvre, par l'AC cible et l'AE lors de la demande d'Abonnement ou lors de la mise en œuvre d'un nouveau parcours.

La politique d'identification suit les règles décrites au paragraphe 3.2 « *Validation initiale d'identité* » décrits dans la PC-DPC et détaille les contrôles qui seront mis en place par l'Abonné, directement ou au travers de ses mandataires ou Partenaires avec lesquels il est lié contractuellement, pour répondre à un procédé d'identification fiable de ses Clients (Titulaires). Par ailleurs, suivant le niveau de contrôle d'identité mis en place, l'Abonné 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'Autorité d'Enregistrement procède par échantillonnage à des contrôles auprès de l'Abonné, en ce compris ses Rattachés conventionnels, pour vérifier le respect du dispositif d'identification décrit par l'Abonné.

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*.

Ayant droit de l'Abonné : l'ayant droit est la personne détenant un droit du fait de son lien qu'il soit de nature contractuelle, ou légale avec l'Abonné.

Cachet électronique : le « Cachet électronique » est un procédé utilisé par un service applicatif, se différenciant ainsi de la « Signature électronique » qui est un terme consacré réservé à une personne physique. Le Cachet électronique désigne des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières. Il contient une contremarque de temps correspondant à l'horodatage de la production du cachet.

Certificat : Fichier électronique émis par Worldline, en sa qualité de service de confiance 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 ;
- quand il s'agit d'un « certificat de Cachet électronique », désigne une attestation électronique qui associe les données de validation d'un Cachet électronique à une personne morale et confirme le nom 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'Abonné 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.

Le certificat de Cachet électronique garantit l'origine d'un message émis par une personne morale mais aussi est utilisé pour chiffrer des échanges, afin d'en assurer la confidentialité, l'Authentification et l'intégrité. Dans ce cadre, l'Organisation scelle le Document en son nom tel qu'identifié dans le Certificat, ou au nom du représentant habilité de l'Organisation identifié dans le Certificat. Le Certificat d'Organisation est demandé par un représentant habilité par l'Organisation.

Ce Certificat de Cachet électronique ou d'Organisation a une durée de vie de plusieurs années, conformément à la PC-DPC.

Le Certificat Permanent désigne un Certificat de Signature Electronique généré sur requête du Titulaire (personne physique)

Paraphe Abonné

du Certificat au TSP Mediacert Sa durée de vie est de plusieurs années, conformément à la PC-DPC.

Ces Certificats sont signés par les AC en ligne du TSP MediaCert 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.

Contrat d'Abonnement : désigne le contrat d'abonnement au service de Signature électronique et/ou Cachet électronique. Il est constitué des documents désignés à l'article 22 qui forment un tout indissociable.

Demande de Certificat :

l'Abonné qui souhaite faire une demande de Certificat de Cachet électronique ou d'Organisation devra remplir un document inclus dans le Dossier de Souscription précisant notamment les coordonnées du ou des demandeur(s) d'un Certificat de ce type émis par l'AC concernée.

l'Abonné qui souhaite faire une demande de Certificat à usage unique devra quant à lui la présenter sous forme électronique. Cette demande est constituée d'un message (requête) signé par l'Abonné 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 à l'article 22 des Conditions Générales d'Abonnement.

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 : ensemble des formulaires et des pièces justificatives permettant à l'AC de justifier l'émission et/ou l'utilisation de certificats électroniques pour réaliser des signatures ou des cachets électroniques pour le compte de l'Abonné.

Elément 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'Abonné 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/scellement).

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 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. ou pouvant faire référence à un nom de marque ou de société pour laquelle un Certificat d'Organisation ou de Cachet électronique va être délivré à la demande d'un Abonné.

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. Un Abonné 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'AE, de documents « *Politique d'identification OTU et modalités de recueil de consentement* » distincts.

Partie : Worldline ou l'Abonné.

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, de fourniture de Certificats et notamment leur processus d'émission, d'utilisation et de Révocation.

La PC-DPC est disponible en ligne : https://www.mediacert.com/

Référence : « WLM-OTU-F002 ».

Politique de Gestion de Preuves : document qui décrit la politique suivie par les AC 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 (Signature électronique, horodatage, traces informatiques notamment).

Politique d'identification OTU et modalités de recueil du consentement : document en deux parties établi par l'Abonné, à l'appui des demandes de Certificat à usage unique, à partir du formulaire *« WLF-OTU-F018 »* :

- la première partie décrit les procédés d'identification des Titulaires, ou utilisateurs finaux, que l'Abonné met en œuvre ou dont il délègue par contrat la mise en œuvre sous sa responsabilité. De ces procédés d'identification dépend l'AC qui sera ciblée. La Politique d'identification fait l'objet d'une approbation par l'AE après vérification de la conformité aux exigences décrites au paragraphe 3.2.3.1 *« Validation de l'identité d'un individu - Certificat à usage unique »* de la PC-DPC ;

- la seconde partie détaille le procédé permettant à l'Abonné, directement ou via ses Rattachés conventionnels, de

Paraphe Abonné

recueillir l'accord explicite et éclairé de l'utilisateur final, préalablement à toute Demande par l'Abonné 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'Abonné pour l'exercice par eux d'un certain nombre d'obligations à la charge de l'Abonné, telles que notamment l'application et le respect de la Politique d'identification préalablement définie par l'Abonné, en contrepartie de leur accès via l'Abonné 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'Abonné 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 société abonnée ou une Organisation. Une preuve de cette habilitation doit être fournie à l'AE.

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 : opération demandée par le Dispositif Porteur de Certificat, le représentant de l'Abonné ou un des représentants adjoint de l'Abonné qui dispose des données d'identification et d'authentification lui permettant d'accéder à cette fonction, ou le TSP MediaCert (conformément à la PC-DPC) pour rendre invalide un Certificat donné avant la fin de sa période de validité. 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.

Service : service de Certification proposé par Worldline, en sa qualité de Service de Confiance du TSP Mediacert, à l'Abonné pour répondre à des besoins de Signature électronique 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 Ière 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.

Dans le cas de l'utilisation de Certificat d'Organisation ou certificat de Cachet électronique, il ne s'agit pas de Signature électronique de personne physique. L'utilisation éventuelle du terme « signature Cachet électronique » doit être entendue comme l'application d'un scellement qui garantit l'origine et l'intégrité d'un message.

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

Définition Worldline TSP Mediacert

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

Lorsqu'il s'agit d'un Certificat d'Organisation, le Titulaire est l'Organisation ou un représentant de l'Organisation. La génération et l'utilisation exclusive de la Clé Privée associé à la clé publique indiquée dans le Certificat est confiée à l'entité « Dispositif Porteur de Certificat ».

Lorsqu'il s'agit d'un Certificat Permanent, le Titulaire est une personne physique identifiée au sein du TSP Mediacert tel un Abonné, et ayant effectuée une requête de génération de Certificat permettant de signer électroniquement des Documents. La génération et l'utilisation exclusive de la Clé Privée associé à la clé publique indiquée dans le Certificat est confiée à l'entité « Dispositif Porteur de Certificat ».

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

L'Utilisateur final peut bénéficier du Service de signature électronique offert par l'Abonné 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 ;
- éventuellement disposer, pour certains Services, d'une adresse e-mail ou d'un numéro de téléphone. Dans cette hypothèse, ces informations doivent être actives, exactes et personnelles.

2. CONDITIONS PREALABLES A LA CONSTITUTION DE LA QUALITE D'ABONNE

2.1. L'acceptation de l'attribution de la qualité d'Abonné repose sur un ensemble d'élément définis au chapitre 3.2.2.1 *« Validation d'un Abonné »* de la PC-DPC. Ceci inclut, notamment :

- la signature d'un Contrat d'Abonnement (cf. article 22) ;
- la désignation ou la nomination de Représentants au sein de l'Abonné pour les Demandes de Création de Certificats à usage uniques et / ou d'Organisation ;
- la fourniture d'un ensemble de documents justificatifs.

2.2. Dans le cas où une Organisation est différente de l'Abonné, l'Abonné doit fournir à l'AE les informations concernant l'Organisation définies au paragraphe 3.2.2.2 *« Validation d'une Organisation »* de la PC-DPC.

2.3. La signature du Contrat d'Abonnement emporte reconnaissance, notamment par l'Abonné, des obligations contenues dans les présentes clause 8 et dans la PC-DPC.

3. CONDITIONS PREALABLES A L'OBTENTION DE CERTIFICATS

Pour obtenir des Certificats, l'Abonné doit remplir les formalités suivantes auprès de L'AE :

3.1. L'Abonné devra réaliser sa Demande de Création de Certificat (réf. *« WLF-OTU-F007 »*), en accord avec le service qu'il a souscrit auprès du TSP MediaCert, suivant qu'il s'agit d'un Certificat d'Organisation (ou de Cachet électronique) et/ou d'un Certificat à usage unique et/ou d'un Certificat Permanent

3.2. L'Abonné devra faire son affaire de l'adéquation des Certificats et/ou du niveau de Signature électronique choisi à ses besoins et aux besoins de ses éventuels Rattachés conventionnels : avant toute demande de création de Certificat auprès de l'AE, l'Abonné fera son affaire de ce que le type de Certificat à délivrer dans le cadre du service soit adapté à ses règles de délégations internes à ses besoins métier et à ses contraintes juridiques ainsi qu'à celles de ses Rattachés conventionnels.

4. POUR LA DELIVRANCE D'UN CERTIFICAT D'ORGANISATION

4.1. **Dossier de l'Abonné**. Le Dossier de l'Abonné au service de Cachet électronique utilisant des Certificats Organisation doit être accompagné de pièces justificatives telles que décrites au paragraphe 3.2.4 *« Validation de l'autorité du demandeur »* dans la PC-DPC.

Tout Dossier non complété pourra être refusé par l'AE. Les informations fournies dans le Dossier doivent être complètes, exactes et à jour. L'Abonné garantit la vérification des informations fournies et la validité des pièces justificatives qui les accompagnent. Toute modification des informations contenues dans le Dossier doit engager la procédure de révocation du certificat émis pour l'une quelconque des raisons suivantes : décès, départ ou démission d'un Titulaire de Certificat d'Organisation. L'AE se réserve le droit de refuser le Dossier dans l'hypothèse où l'Abonné est insolvable, fait l'objet de poursuites judiciaires ou porte atteinte, de quelque façon que ce soit, aux bonnes mœurs.

4.2. **Demande de Certificats.** L'Abonné est garant de la vérification des informations, relatives à l'Abonné, fournies et de la validité des pièces justificatives qui les accompagnent, ainsi que de la mise à jour régulière desdites informations. L'AE n'assume aucune responsabilité à l'égard de l'Abonné quant à la forme, l'exactitude, l'authenticité ou l'effet juridique des pièces justificatives remises par l'Abonné. Le Certificat de Cachet électronique ou d'Organisation produit par l'AC est transmis à l'Abonné pour acceptation du Certificat.

4.3. **Acceptation du certificat.** L'acceptation explicite des informations contenues dans le Certificat est requise de la part, soit du représentant légal de l'Abonné qui a fait la demande, soit de l'individu habilité par le représentant légal de l'Abonné, identifié dans le Certificat. Le formalisme de cette acceptation est détaillée dans la PC-DPC ainsi que dans le mail de notification de délivrance du Certificat de Cachet électronique ou Organisation envoyé par l'Autorité de Certification émettrice.

L'Abonné est tenu d'avertir le TSP Mediacert par écrit de toute inexactitude dans les dix (10) jours ouvrés consécutifs à la génération dudit Certificat, notamment dans l'hypothèse où les données inscrites sur le Certificat ne correspondent pas aux informations contenues dans le Dossier d'Abonnement. A défaut de notification dans ce délai, le Certificat sera réputé avoir été accepté. En cas de notification dans le délai indiqué ci-dessus, l'AE statuera sur la mise à disposition auprès de l'Organisation d'un nouveau Certificat.

4.4. La durée de validité d'un Certificat de Cachet électronique, Permanent ou d'Organisation est définie dans la PC-DPC.Deux (2) mois avant la date de fin de validité du Certificat d'Organisation ou du Certificat Permanent, une notification est transmise à l'Abonné, l'invitant à procéder à une nouvelle demande de Certificat d'Organisation ou de Certificat Permanent. Faute de nouvelle demande de l'Abonné, le service est interrompu à l'échéance du certificat.

4.5. Le nouveau Certificat est généré obligatoirement avec un changement de Clé Privée.

5. POUR LA DELIVRANCE D'UN CERTIFICAT A USAGE UNIQUE

5.1. **Dossier de l'Abonné.** Le Dossier d'Abonné au service de signature utilisant des Certificats à usage unique doit être accompagné de pièces justificatives telles que décrites au paragraphe 3.2.3.1 *« Validation de l'identité d'un individu - Certificat à usage unique »* dans la PC-DPC.

Il doit notamment contenir le document « Politique d'Identification et modalités de recueil de consentement ».

L'Abonné 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 par l'AE, des futurs Titulaires de Certificats de ce type, qu'il aura préalablement décrits dans le document susvisé. L'Abonné garantit la vérification des informations fournies et la validité des pièces justificatives qui les accompagnent. L'AE n'assume aucune responsabilité à l'égard de l'Abonné quant à la forme, l'exactitude, l'authenticité ou l'effet juridique des pièces justificatives remises par l'Abonné et le(s) Titulaire(s).

Tout Dossier dont la Politique d'Identification ne présente pas les contrôles nécessaires à l'identification fiable des clients, futurs Titulaires de Certificats de ce type, sera refusé par l'AE.

5.2. **Demande de Certificats.** Dans le cas des Certificats à usage unique, le message électronique de l'Abonné pour demander un Certificat à l'AE (requête) 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'Abonné.

L'Abonné 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.

5.3. **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.

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

6. UTILISATION D'UN CERTIFICAT D'ORGANISATION

6.1. L'usage des certificats de ce type doit être conforme à la PC-DPC applicable. En effet, l'Abonné s'oblige à n'utiliser les Certificats délivrés par l'AC qu'exclusivement pour les applications permettant l'usage d'un Certificat d'Organisation tel que décrit dans la PC-DPC au paragraphe 1.5 « *Usages des certificats* ». En cas de violation de cette obligation, Worldline, au travers du TSP Mediacert, ne pourra voir sa responsabilité engagée.

6.2. Dans le cadre des Certificats de Cachet électronique ou d'Organisation, l'Abonné autorise l'AC à utiliser la Clé Privée attachée au Certificat à des fins de mise en œuvre de cachets électroniques.

6.3. L'utilisateur doit vérifier, a minima avant utilisation, les informations sur le statut du certificat qu'il compte utiliser conformément à l'usage prévu. Il peut, pour cela, utiliser les différents moyens mis à disposition conformément au paragraphe

Paraphe Abonné

4.9.6.2 *« Exigences de vérification de la révocation par les utilisateurs de Certificats – Certificat d'Organisation ou Permanent »* de la PC-DPC.

7. UTILISATION D'UN CERTIFICAT A USAGE UNIQUE

7.1. L'usage des certificats de ce type doit être conformes à la PC-DPC applicable. En effet, l'Abonné 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.

7.2. L'Abonné, en ce compris ses Rattachés conventionnels, reconnaît que la cinématique de Signature électronique mise en œuvre doit être présentée 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'Abonné pour qu'il puisse requérir pour lui un certificat à usage unique afin de pouvoir signer le ou les Documents qui lui sont présentés.

8. REVOCATION D'UN CERTIFICAT D'ORGANISATION OU PERMANENT

8.1. **Origine de la Révocation.** Les personnes ou entités habilitées sont décrites au paragraphe 4.9.2.2 *« Origine d'une demande de Révocation – Certificat d'Organisation ou Permanent»* de la PC-DPC.

8.2. **Cause de la Révocation.** Les causes de révocation sont décrites au paragraphe 4.9.1.2 de la PC-DPC *« Causes possibles d'une révocations – Certificat d'Organisation ou Permanent»*.

8.3. **Responsabilité.** Worldline, au travers du TSP Mediacert, ne pourra en aucun cas voir sa responsabilité engagée dès lors qu'un représentant habilité de l'Abonné n'aura pas effectué de demande de Révocation du Certificat de Cachet électronique lorsque l'une des circonstances décrites dans le paragraphe susvisé de la PC-DPC, et dont il a connaissance, se réalise.

8.4. **Procédure de Révocation.** Les Procédures de traitement d'une demande de révocation sont décrites au paragraphe 4.9.3.2 de la PC-DPC *« Procédure de traitement d'une demande de révocation – Certificat d'Organisation ou Permanent »*.

La révocation d'un Certificat d'Organisation conduit à la génération d'une Liste des Certificats Révoqués. Le numéro du Certificat concerné par la demande de Révocation est alors inscrit dans la Liste des Certificats Révoqués.

L'AC concernée publie ensuite cette liste des Certificats révoqués à l'adresse définie au paragraphe 4.10 *« Fonction d'information sur l'état des Certificats »* de la PC-DPC.

Les utilisateurs de ce type de Certificats peuvent consulter cette liste sans limitation.

8.5. **Confirmation de la révocation.** Le TSP Mediacert confirmera, dans le cadre d'une demande de révocation de ce type de Certificat, par e-mail au demandeur l'exécution de la demande de Révocation du Certificat.

9. REVOCATION D'UN CERTIFICAT A USAGE UNIQUE

9.1. **Origine de la Révocation.** Les personnes ou entités habilitées sont décrites au paragraphe 4.9.2.1 *« Origine d'une demande de Révocation – Certificat à usage unique »* de la PC-DPC.

9.2. **Cause de la Révocation.** Les causes de révocation sont décrites au paragraphe 4.9.1.1 de la PC-DPC *« Causes possibles d'une révocations – Certificat à usage unique »*.

9.3. **Responsabilité.** Worldline, au travers du TSP Mediacert, ne pourra en aucun cas voir sa responsabilité engagée dès lors qu'un représentant habilité de l'Abonné n'aura pas effectué de demande de Révocation du Certificat à usage unique lorsque l'une des circonstances décrites dans le paragraphe susvisé de la PC-DPC, et dont il a connaissance, se réalise.

9.4. **Procédure de Révocation.** Les Procédures de traitement d'une demande de révocation sont décrites au paragraphe 4.9.3.1 de la PC-DPC *« Procédure de traitement d'une demande de révocation – Certificat à usage unique »*.

La révocation d'un Certificat, quel qu'il soit, conduit à la génération d'une Liste des Certificats Révoqués. Le numéro du Certificat concerné par la demande de Révocation est alors inscrit dans la Liste des Certificats Révoqués.

L'AC concernée publie ensuite cette liste des Certificats révoqués à l'adresse définie au paragraphe 4.10 *« Fonction d'information sur l'état des Certificats »* de la PC-DPC.

Les utilisateurs de ce type de Certificats peuvent consulter cette liste sans limitation.

9.5. **Confirmation de la révocation.** La demande de Révocation étant automatiquement autorisé, le Titulaire concerné est informé du changement de statut de son certificat via la publication de la Liste des Certificats Révoqués à l'adresses définies ci-dessus.

10. ENGAGEMENTS DE L'ABONNÉ

10.1. **Fourniture de documents par l'Abonné à l'AE.**

Certificat de Cachet électronique ou d'Organisation

L'Abonné doit fournir à l'Autorité d'Enregistrement :

- le document de Demande de Création de Certificat de Cachet électronique ou Cachet d'Organisation renseigné par un représentant d'Abonné habilité s'il souhaite la création d'un certificat de ce type ;
- les documents justificatifs étayant le contenu du Certificat qui sera produit par l'AC ;
- et notamment, au cas où le nom d'Organisation à mettre dans le Certificat serait différent de celui de l'Abonné :
    - un justificatif (mandat) en bonne et due forme émanant du représentant légal ou habilité de l'Organisation en question permettant à l'Abonné de demander la délivrance de Certificat au nom de cette Organisation ;
    - toute pièce, valide lors de la demande de création de Certificat, attestant de l'existence de l'Organisation (extrait de KBIS datant de moins de trois (3) mois ou, original ou copie de tout acte ou extrait de registre officiel datant de moins de trois (3) mois constatant la dénomination, la forme juridique, l'adresse du siège social et l'identité des associés et dirigeants sociaux mentionnés aux 1° et 2° de l'article R. 123-54 du code de commerce ou de leurs équivalents en droit étranger, …) ;
    - tous justificatifs nécessaires à étayer les pouvoirs du représentant de cette Organisation si la personne physique amenée à représenter cette Organisation n'est pas le représentant légal de cette Organisation (délégation de pouvoir valide et non révoquée) et justificatif de l'appartenance de cette personne physique à l'Organisation.

Il est précisé qu'il est de la responsabilité de l'Abonné de vérifier la validité et la complétude des documents qu'il fournit à l'Autorité d'Enregistrement à l'occasion de sa demande d'abonnement.

Certificat Permanent

L'Abonné doit fournir à l'Autorité d'Enregistrement :

- le document de Demande de Création de Certificat Permanent renseigné;
- les informations et justificatifs (ou copies) valides de l'identité de l'Abonné, étayant le contenu du Certificat qui sera produit par l'AC ;

Il est précisé qu'il est de la responsabilité de l'Abonné de vérifier la validité et la complétude des documents qu'il fournit à l'Autorité d'Enregistrement à l'occasion de sa demande d'abonnement.

Certificats à usage unique

L'Abonné doit fournir à l'AE, qui devra la valider, le document « *Politique d'Identification et modalités de recueil du consentement* » complété 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'Abonné 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'Abonné 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 de la génération d'un certificat au nom du futur titulaire ;
    - Le consentement explicite de l'acception des Conditions Générales de Service du Service de Signature Electronique, préalablement communiquées au futur titulaire de Certificat.

10.2. **Obligation générale d'information des Titulaires par l'Abonné.** L'Abonné garantit informer l'utilisateur final, en sa qualité de Titulaire, conformément aux obligations décrites dans son Contrat d'Abonnement. A ce titre, l'Abonné garantit 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 sur le contenu de la preuve constituée et en lui indiquant qui est le prestataire de gestion et de conservation de preuves ;
- en l'informant de sa possibilité d'abandon de la procédure qu'il a initiée ;
- en l'informant sur la possibilité qui lui est offerte ou non de rétractation ;
- 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/.

10.3. **Vérification des Demandes de Création de Certificat.** L'Abonné a l'obligation de vérifier l'exactitude et la complétude des informations fournies à l'AE dans le message électronique signé (requête) ou dans le formulaire papier destiné à l'Autorité d'Enregistrement et qui est nécessaire à l'émission soit du Certificat à usage unique soit d'Organisation par les AC.

10.4. **Pratiques non-discriminatoires.** L'Abonné 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.

10.5. **Respect des obligations par le(s) Titulaire(s) de Certificats à usage unique.** L'Abonné s'engage en outre à faire respecter par les Titulaires les dispositions qui leur sont applicables et qui découlent de son Contrat d'Abonnement.

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

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

10.6. **Information de l'AE par l'Abonné**

Certificats de Cachet électronique ou d'Organisation

L'Abonné se doit :

- d'informer l'Autorité d'Enregistrement dans le cas où les données du Certificat ne seraient plus valables du fait d'un changement au sein de l'Organisation. A cet égard, l'Abonné doit notifier sans délai à l'AE, par lettre recommandée avec accusé de réception :
    - tout changement dans l'identité de la personne assurant la fonction de représentant d'Abonné ou de représentant adjoint d'Abonné, ainsi que la date d'effet de ce changement, accompagné des pièces justificatives ;
    - tout changement dans les informations communiquées à l'AE, ainsi que la date d'effet de ces changements.
- de communiquer dans les meilleurs délais à l'Autorité d'Enregistrement tout évènement pouvant porter atteinte à la fiabilité des moyens d'authentification auprès de celle-ci. A cet égard, les changements (prénom, nom, adresse e-mail) doivent être notifiés à l'AE ;
- d'informer l'Autorité d'Enregistrement dans le cas où l'Organisation n'existerait plus. A cet égard, l'Abonné doit notifier sans délai à l'AE, par lettre recommandée avec accusé de réception, les changements (prénom, nom, adresse e-mail, identifiant de l'Organisation) affectant l'ensemble des Certificats de l'Organisation, accompagnés des pièces justificatives ;
- d'informer l'Autorité d'Enregistrement dans le cas où des informations concernant l'Organisation, ne figurant pas dans le Certificat d'Organisation et n'ayant pas d'impact sur sa validité, sont amenées à être modifiées. A cet égard,

l'Abonné doit notifier dans les meilleurs délais l'AE, par lettre simple, les changements d'informations.

Certificats Permanents

L'Abonné se doit :

- de communiquer dans les meilleurs délais à l'Autorité d'Enregistrement tout changement d'information de contact (adresse, adresse e-mail);
- d'informer l'Autorité d'Enregistrement dans le cas où les données du Certificat ne seraient plus valables du fait d'un changement de nom d'usage.

Certificats à usage unique

L'Abonné se doit de :

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

11. ENGAGEMENTS DE WORLDLINE

11.1. Worldline s'engage à mettre en œuvre les moyens (techniques et humains) nécessaires à la fourniture des Services. Le niveau de service mis en œuvre est celui fixé dans le contrat référencé dans le Contrat d'Abonnement joint aux présentes Conditions Générales.

11.2. Worldline, au travers du TSP Mediacert, 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'Abonné.

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

11.4. Worldline, au travers du TSP Mediacert, s'engage à authentifier toute requête de l'Abonné portant sur une demande de Certificat et s'engage à conserver notamment la preuve de cette requête.

11.5. Worldline, en sa qualité de TSP Mediacert, conserve l'ensemble des données nécessaires aux AC définies au chapitre 5.5.2 *« Période de conservation des archives »* de la PC-DPC, notamment :

- les dossiers d'enregistrement :
    - huit (8) ans pour les dossiers concernant les certificats à usage unique ;
    - dix (10) ans pour les dossiers concernant les certificats d'Organisation ou permanents.
- les journaux d'activité des services : dix (10) ans.

11.6. Worldline, en sa qualité de TSP Mediacert, a un devoir de conseil vis-à-vis de l'Abonné afin que ce dernier puisse choisir de façon éclairée, la solution technique de Signature électronique adaptée au type de parcours de signature qu'il a déterminé. L'intervention du TSP Mediacert se limite, dans le cadre d'une obligation de moyens, à une prestation technique qui permet à l'Abonné ou ses ayant droit de bénéficier des Services de Signature électronique et/ou de Cachet électronique sur des Documents conformément à la PC-DPC applicable. Worldline n'a aucune action sur le contenu des Documents sujets à aux services fournis par le TSP MediaCert, hormis l'insertion de Signatures électroniques et / ou de Cachet 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.

12. INTERRUPTION DE SERVICE

L'Abonné reconnaît que Worldline, en sa qualité de TSP Mediacert, peut être amené à interrompre le Service, en tout ou partie, afin d'en assurer la maintenance ou effectuer des améliorations. Le TSP Mediacert informe dans les meilleurs délais l'Abonné 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.

13. 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.

14. CONDITIONS FINANCIERES

Le TSP MediaCert ne commercialise pas les Certificats seuls, mais uniquement en complément de services de plus haut niveau fournis par lui-même ou par des sociétés de son groupe. Ces services sont précisés dans le contrat référencé dans le Contrat d'Abonnement associé aux présentes conditions générales.

Ce contrat détaille l'ensemble des conditions financières.

15. RESPONSABILITE DE L'ABONNÉ ET GARANTIE PAR CELUI-CI

Responsabilités

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

15.2. Dans l'hypothèse où Worldline, en sa qualité de TSP MediaCert n'est pas destinataire des justificatifs recueillis par l'Abonné en ce compris ceux collectés par les Rattachés conventionnels, à l'appui de l'identification des Titulaires, le TSP MediaCert réalise une campagne d'échantillonnage des signatures à usage unique réalisées sur requête de l'Abonné afin de vérifier la bonne application par l'Abonné, en ce compris ses Rattachés conventionnels, de la Procédure d'Identification validée conjointement entre les parties. L'échantillonnage doit permettre de vérifier que le contrôle d'identité a bien été effectué et nécessite que les preuves de ce contrôle aient été conservées pour une durée minimum de huit (8) ans par l'Abonné, en ce compris ses Rattachés conventionnels. Cette campagne d'échantillonnage aura lieu au moins une (1) fois par an. En cas d'écarts avec ladite procédure, l'Abonné s'engage à établir un plan d'action avec Worldline pour résorber lesdits écarts. La non-application de ce plan d'action ou le constat d'écarts lors de la campagne d'échantillonnage suivante pourront conduire à une désactivation du service de Signature électronique utilisant des Certificats à usage unique pour l'Abonné en ce compris ses ayant droit selon les dispositions évoquées dans la PC-DPC.

Garanties

15.3. L'Abonné garantit Worldline, en sa qualité de TSP MediaCert, 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'Abonné, ses ayant droit ou un Titulaire de l'une quelconque des dispositions du Contrat d'Abonnement, en ce compris les documents y afférents.

15.4. L'Abonné, en ce compris ses rattachés conventionnels, garantit le TSP MediaCert 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.

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

16. RESPONSABILITE DE WORLDLINE ET GARANTIE PAR CELLE-CI

Responsabilités

16.1. Worldline fournit une prestation technique en faisant bénéficier l'Abonné des Services de Signature électronique et/ou Cachet électronique du TSP MediaCert.

16.2. L'Abonné reconnait que le TSP MediaCert n'a pas d'action sur le contenu des Documents émis par celui-ci, hormis l'insertion par les AC du TSP MediaCert de Signatures ou de cachets électroniques sur lesdits Documents et ne saurait en conséquence être tenue pour responsable des contenus et informations qu'ils contiennent .

16.3. La responsabilité de Worldline est limitée aux dommages matériels directs à l'exclusion de tout dommage indirect. 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 Service dont les références sont précisées dans le Contrat d'Abonnement au service de Signature électronique et/ou Cachet électronique (réf. *« WLF-OTU-F005 »*) joint aux présentes Conditions Générales.

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

16.5. Worldline ne pourra voir sa responsabilité engagée en cas d'interruption, totale ou partielle, du Service conformément à l'article 12 ci-dessus.

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

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

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

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

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

16.10. **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 Contrat d'Abonné, de plein droit et sans formalité judiciaire, sans que l'Abonné ne puisse prétendre à aucune indemnité.

Garanties

16.11. Worldline, en sa qualité de TSP MediaCert, garantit à l'Abonné 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;

16.12. Worldline ne peut se substituer à l'Abonné dans le choix du niveau de service souscrit en lien aux régimes juridiques applicables aux Documents métier pour lesquels l'Abonné a décidé de recourir à de la Signature électronique et/ou du Cachet électronique.

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

16.14. Le 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.

16.15. Le TSP MediaCert garantit via ses services :

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

17. MODIFICATION DES DOCUMENTS ET CONDITIONS CONTRACTUELLES

Evolutions documentaires du fait de contraintes externes

17.1. **Conditions Générales d'Abonnement.** Les Conditions Générales d'Abonnement ayant vocation à évoluer pour tenir compte de contraintes légales, techniques, ou commerciales feront l'objet de mises à jour.

Le 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.

Le TSP MediaCert notifiera, via un communiqué par e-mail signé, les mises à jour opérées sur les Conditions Générales d'Abonnement au plus tôt.

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

17.2. **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.

17.3. Toute notification entre les parties sera valablement faite auprès de l'Abonné, à son adresse e-mail renseignée dans son dossier d'enregistrement ou à toute autre adresse que les parties se communiqueraient ultérieurement par simple courrier ordinaire ou par courriel.

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

17.5. 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.mediacert.com/

17.6. L'Abonné en ce compris ses ayant droit est informé qu'il a la possibilité de sauvegarder et/ou d'imprimer les Conditions Générales d'Abonnement applicables.

17.7. **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'Abonné par tout moyen, au moins un (1) mois avant leur entrée en vigueur.

17.8. **Autres évolutions.** Si des évolutions s'avérant nécessaires dans le cadre du service devaient avoir une incidence sur l'économie du contrat référencé au Contrat d'Abonnement, l'Abonné 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'Abonné sera réputé avoir accepté lesdites modifications.

18. DUREE

Le Contrat d'Abonnement prend effet à compter de sa date de signature par l'Abonné pour une durée indéterminée, sans toutefois dépasser la durée du contrat de service de plus haut niveau référencé dans le Contrat d'Abonnement.

19. RESILIATION

19.1. Le Contrat d'Abonné pourra être résilié, de plein droit et sans formalité judiciaire, par lettre recommandée avec avis de réception (LRAR), par l'Abonné ou l'Autorité de Certification :

- pour convenance, suivant le respect du préavis stipulé au Contrat référencé dans le Contrat d'Abonnement ;
- 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 (1ère présentation) restée sans effet ;
- en cas de force majeure, dans les conditions décrites à l'article 16.10 du présent document ;
- de plein droit, en cas de résiliation du Contrat de Services auquel le présent Contrat d'Abonnement est lié.

19.2. En cas de résiliation du Contrat d'Abonnement et à la date d'effet de la résiliation, l'accès au service de l'Abonné en ce compris ses ayant droits, sera coupé et les Certificats de Cachet électroniques éventuellement émis seront immédiatement révoqués sans que l'Abonné ne puisse faire valoir un quelconque droit à indemnisation.

19.3. L'Abonné s'interdit de faire une demande de création de Certificat auprès de l'Autorité d'Enregistrement à la date d'effet de la Résiliation.

20. PROPRIETE INTELLECTUELLE

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

21. PROTECTION DES DONNEES PERSONNELLES

21.1. **Les Certificats de Cachet électronique ou d'Organisation ou de Certificats Permanents.** Les données personnelles recueillies dans le cadre du présent Contrat d'Abonnement sont obligatoires pour le traitement du dossier d'enregistrement. Elles sont destinées, de même que celles qui pourront être recueillies ultérieurement, aux AC qui, sont autorisées par l'Abonné, dûment habilité à cet effet, à les conserver en mémoire informatique, à les utiliser, ainsi qu'à les communiquer aux mêmes fins et sous les mêmes protections, aux personnes morales de Worldline ou à des tiers habilités pour des besoins de gestion des Certificats de Cachet électronique et de Certificats Permanents.

21.2. **Certificats à usage unique.** Dans le cadre des certificats à usage unique, il est rappelé que l'Abonné veillera à obtenir l'acceptation expresse des futurs Titulaires, avant de transmettre les données personnelles de ces futurs Titulaires à l'Autorité d'Enregistrement, 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'AE auprès de l'Abonné fassent l'objet d'un traitement informatique aux seules fins de :

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

Il est en effet précisé que toute opposition à la conservation de données à caractère personnel empêchera la délivrance de ce type de Certificat. En effet, en acceptant la fourniture du Certificat pour procéder à une Signature électronique, le Titulaire accepte que l'AC via l'AE, conserve, à la demande de l'AE, les données à caractère personnel pendant la durée nécessaire à l'exercice des finalités des traitements opérés dans le cadre de la fourniture et la gestion du Certificat à usage unique.

21.3. L'Abonné en ce compris les représentants d'Abonnés ou d'Organisations ainsi que les Titulaires disposent d'un droit d'accès, de rectification, de suppression et d'opposition relatifs à leurs données personnelles communiquées qu'ils peuvent exercer auprès de Worldline à l'adresse indiquée ci-dessous :

Comité MediaCert
Worldline
23, rue de la Pointe
Zone Industrielle A
59113 Seclin
France
dl-mediacert-tsp@worldline.com

21.4. 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.

21.5. Worldline a mis en œuvre et respecte des procédures de protection des données personnelles pour garantir la sécurité des données transmises par :

Paraphe Abonné

- l'Abonné en ce compris l'ensemble de ses rattachés conventionnels ;

- les Titulaires, personnes physiques, à l'Abonné, en ce compris l'ensemble de ses rattachés conventionnels, lequel les communique à Worldline dans le cadre du présent contrat aux fins de les identifier et les authentifier.

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

21.6. Les Titulaires doivent garantir sur l'honneur à l'Abonné, en ce compris ses rattachés conventionnels, 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.

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

21.8. Les Titulaires doivent être informés des éléments tracés pour le compte de l'Abonné 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).

21.9. 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.

21.10. 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.

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

21.12. 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.

22. DOCUMENTS CONTRACTUELS

22.1. Le Contrat d'Abonnement est constitué des documents, qui forment un ensemble indissociable, énumérés ci-dessous :

- le contrat d'adhésion au service de Signature électronique et/ou Cachet électronique ;

- les présentes Conditions Générales d'Abonnement au service de Signature électronique et/ou Cachet électronique ;

- la « *Politique d'identification OTU et modalités de recueil du consentement* » dans le cas de la souscription au service de Signature électronique OTU ;

- la Politique de Certification – Déclaration des Pratiques de Certification disponible en ligne à l'adresse définie en Article 1.

Par ailleurs, il s'inscrit dans le processus d'attribution de la qualité d'Abonné comme défini à l'article 2.1 du présent document.-.

22.2. L'ensemble des documents susvisés constituent le cadre technique dans lequel s'effectuera le service de Signature électronique à l'Abonné. Il est complété des dispositions du contrat de service de plus haut niveau précisant notamment l'article 14 des présentes portant sur les conditions financières, l'article 18 portant sur la durée, l'article 16 portant sur la Responsabilité de Worldline.

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

23. LOI APPLICABLE

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

Le TSP MediaCert, offrant les services objet des présentes, dans toutes ses composantes et y compris documentaires est régie par la législation et la réglementation en vigueur sur le territoire français qui lui est applicable, bien que ses activités qui découlent de la 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 22.1 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, notamment sur l'interprétation du Contrat d'Abonnement ou de la commune intention des parties.

24. 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.

Paraphe Abonné