Worldline

DIGITAL PAYMENTS
FOR A TRUSTED WORLD

CONDITIONS GENERALES DES SERVICES DES AC EN LIGNE

AUTEUR(S)	:	F. LESECQ
N° DE DOCUMENT	:	WLS-OTU-F022
VERSION	:	2.5
STATUT	:	FINAL
Classification	:	Public
SOURCE	:	WORLDLINE
DATE DU DOCUMENT	:	22 JUILLET 2021
NOMBRE DE PAGES	:	12

PROPRIETAIRE	:	COMITE MEDIACERT

1 Contenu

Liste des modifications

Versions	Date	Description	Auteur(s)
1.0	24/10/2014	Version publique initiale	J.J. Milhem
2.0	05/07/2017	Réécriture pour prise en compte des contraintes réglementaires eIDAS	F. Da Silva
2.1	18/09/2018	Corrélation avec l'intégration de la PC-DPC à la structure documentaire du TSP MediaCert. Pas de modification(s) réalisée(s) hormis la mise en forme du présent document	F. Da Silva
2.2	18/09/2018	Ajout d'une AC au périmètre de la PC-DPC ce qui implique la mise à niveau des présentes CGS. Ces CGS deviennent alors les CGS des « AC en ligne »	F. Da Silva
2.3	16/07/2019	Ajout des obligations des porteurs de certificats dans le document.	F. Poulain
2.4	31/03/2020	Prise en compte des remarques post-audit : - Ajout du moyen technique permettant le recueil du consentement explicite requis de l'utilisateur aux Conditions Générales de service et la PC DPC - Ajout du moyen technique permettant le recueil du consentement explicite requis de génération d'un certificat au nom de l'utilisateur Revue générale du document pour conformité avec les CGA mises à jour.	F.Lesecq
2.5	22/07/2021	Mise à jour de la charte graphique Modification des informations d'entreprise Mise à jour du scope des Autorités de Certification 2021	H. Yete F.Lesecq

2 Introduction

2.1 Présentation du document

Le présent document définit les dispositions essentielles définies dans la [PC-DPC] concernant la délivrance de certificats par les Autorités de Certification dites « en ligne » à la demande de l'Abonné, conformément à la réglementation [eIDAS] et plus particulièrement à [ETSI EN 319 411-1]. Les AC en ligne opérées par TSP Mediacert, lui-même créé par Worldline France, sont les Autorités de Certification suivantes dénommées :

- « Mediacert OTU LCP CA 2021» ;
- « Mediacert OTU LCP CA S2 2021» ;
- « Mediacert OTU CA 2021 » ;
- « Mediacert OTU CA S2 2021 » ;
- « Mediacert ORG CA 2021 » ;
- « Mediacert ORG CA S2 2021 » ;
- « Mediacert ORG NCP CA 2021 » ;
- « Mediacert ORG NCP CA S2 2021 » ;
- « Mediacert PERM CA 2021 » ;
- « Mediacert PERM CA S2 2021 » ;

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

- [OTU LCP] pour les AC « Mediacert OTU LCP CA 2021» et « Mediacert OTU LCP CA S2 2021»;

- [OTU] pour les AC « Mediacert OTU CA 2021 » et « Mediacert OTU CA S2 2021 » ;
- [ORG] pour les « Mediacert ORG CA 2021 » , « Mediacert ORG CA S2 2021 » , « Mediacert ORG NCP CA 2021 » et « Mediacert ORG NCP CA S2 2021 » ;
- [PERM] pour les AC « Mediacert PERM CA 2021 » et « Mediacert PERM CA S2 2021 ».

Il est toutefois précisé, qu'en raison de son caractère synthétique, ce document ne substitue pas à la [PC-DPC] référencée au chapitre 1.3.

Il convient de rappeler que la délivrance de certificats par ces AC repose sur la mise en place d'une relation contractuelle préalable entre une organisation, laquelle est alors désignée comme Abonnée, et Worldline France. L'organisation, désormais Abonnée, s'inscrit alors aux services délivrés par le TSP Mediacert de Worldline France pour obtenir la délivrance, au choix, de :

- certificats de signature à usage unique, émis au nom de la personne physique qui l'aura mandaté à cet effet, en vue de pouvoir signer un ou plusieurs documents sous forme électronique ; et/ou

- certificats d'organisation, émis au nom d'organisations qui dépendent de l'Abonné ou au nom d'organisations qui lui donnent expressément mandat à cet effet, en vue de pouvoir sceller un ou des documents sous forme électronique et/ou

- certificats permanents, émis au nom d'une personne physique qui sera identifiée comme Abonné au sein du TSP, en vue de pouvoir signer des documents sous forme électronique.

Les futurs Titulaires de certificats se doivent d'accepter explicitement au moyen d'un dispositif technique qui leur a été explicité par l'Abonné (matérialiser par un clic de bouton ou une case à cocher par exemple) la délivrance de certificat en leur nom avant toute émission de certificat.
Suite à l'émission de certificats délivrés par les AC en ligne, les Titulaires doivent, avant toute utilisation de leurs certificats, prendre connaissance des conditions d'utilisation qui sont exprimées dans les présentes Conditions Générales des Services et dans la [PC-DPC].

En effet, avant toute utilisation d'un certificat émis par l'une de ces AC, l'utilisateur se doit de lire la [PC-DPC] disponible sur le site web du TSP Mediacert à l'adresse suivante : https://www.mediacert.com.

2.2 Acronymes

Les acronymes utilisés dans le présent document sont les suivants :

Acronyme	Description
AC	Autorité de Certification
CGA	Conditions Générales d'Abonnement
CGS	Conditions Générales des Services
CGV	Conditions Générales de Vente
IGC	Infrastructure à Gestion de Clés
LCP	*Lightweight Certificate Policy*
NCP	*Normalized Certificate Policy*
OID	*Object Identifier*
ORG	*ORGanization : Cachet électronique*
OTU	*One Time Usage : Certificat de signature courte durée*
PC-DPC	Politique de Certification / Déclaration des Pratiques de Certification
PERM	PERManent : Certificat de signature longue durée

2.3 Références

La structure de ce document est conforme à l'annexe A2 – « *The PDS structure* » de la spécification technique [ETSI EN 319 411-1].

2.3.1 Réglementation

Référence	Description
[CNIL]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
[eIDAS]	REGLEMENT (UE) N°910 DU PARLEMENT EUROPEEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

2.3.2 Réglementation technique

Référence	Description
[ETSI EN 319 411-1]	ETSI EN 319 411-1 v1.3.1 (2021-05) Electronic Signature and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements

2.3.3 Documentation interne

Référence	Description
[CGA]	Conditions Générales d'Abonnement Autorités de Certification en ligne Référence : WLS-OTU-F008
[CGV]	Conditions Générales de Vente et de Prestations de Services Worldline France Référence : 212007
[PC-DPC]	Politique de Certification / Déclaration des Pratiques de Certification Autorités de Certification en ligne Référence : WLM-OTU-F002 OID : 1.2.250.1.111.20.5.5

3 Conditions Générales des Services

<table>
<tr><th>Type d'information</th><th>Description</th></tr>
<tr><td>Point de contact</td><td>Comité Mediacert
Worldline France
23 rue de la Pointe
Zone Industrielle A
59113 Seclin
France
dl-mediacert-tsp@worldline.com</td></tr>
<tr><td>Type de certificat, procédure de validation et usage</td><td>Les AC en ligne produisent cinq (5) gammes de certificats :
<table>
<tr><th>Scope</th><th>Gamme de certificat</th><th>Conformité et niveau de sécurité ciblé</th><th>OID</th></tr>
<tr><td rowspan="2">Mediacert PERM CA 2021</td><td>Certificats à usage permanent S1</td><td>[ETSI EN 319 411-1] niveau LCP</td><td>1.2.250.1.111.20.5.5.3</td></tr>
<tr><td>Certificats à usage permanent S2</td><td>[ETSI EN 319 411-1] niveau LCP</td><td>1.2.250.1.111.20.5.5.7</td></tr>
<tr><td rowspan="2">Mediacert OTU CA 2021</td><td>Certificats à usage unique « renforcé » S1</td><td>[ETSI EN 319 411-1] niveau LCP</td><td>1.2.250.1.111.20.5.5.1</td></tr>
<tr><td>Certificats à usage unique « renforcé » S2</td><td>[ETSI EN 319 411-1] niveau LCP</td><td>1.2.250.1.111.20.5.5.5</td></tr>
<tr><td rowspan="2">Mediacert OTU LCP CA 2021</td><td>Certificats à usage unique « standard » S1</td><td>[ETSI EN 319 411-1] niveau LCP</td><td>1.2.250.1.111.20.5.5.4</td></tr>
<tr><td>Certificats à usage unique « standard » S2</td><td>[ETSI EN 319 411-1] niveau LCP</td><td>1.2.250.1.111.20.5.5.8</td></tr>
<tr><td rowspan="2">Mediacert ORG CA 2021</td><td>Certificats d'Organisation S1</td><td>[ETSI EN 319 411-1] niveau LCP</td><td>1.2.250.1.111.20.5.5.2</td></tr>
<tr><td>Certificats d'Organisation S2</td><td>[ETSI EN 319 411-1] niveau LCP</td><td>1.2.250.1.111.20.5.5.6</td></tr>
<tr><td rowspan="2">Mediacert ORG NCP CA 2021</td><td>Certificats d'Organisation S1</td><td>[ETSI EN 319 411-1] niveau NCP</td><td>1.2.250.1.111.20.5.5.9</td></tr>
<tr><td>Certificats d'Organisation S2</td><td>[ETSI EN 319 411-1] niveau NCP</td><td>1.2.250.1.111.20.5.5.10</td></tr>
</table></td></tr>
</table>

Type d'information	Description
	<table><tr><td></td><td></td><td></td><td></td></tr></table> Un certificat à usage unique est produit dynamiquement sur requête de l'Abonné pour le compte d'une personne physique (Titulaire) qui veut pouvoir signer des documents sous forme électronique. La [PC-DPC] précise par ailleurs que : • [OTU LCP] les contrôles de l'identité du futur Titulaire pourront se faire de manière automatisés permettant de vérifier l'identité déclarée du Titulaire ; • [OTU] les contrôles de l'identité du futur Titulaire devront être réalisés par des opérateurs afin de pouvoir vérifier l'identité du Titulaire de manière physique. Le certificat d'organisation ou Cachet électronique est produit par l'AC à la demande de l'Abonné pour le compte d'une organisation pour laquelle l'Abonné est habilité à demander un scellement de documents. Les certificats de test peuvent être générés conformément à la [PC-DPC] et sont délivrés à des fins : • techniques ; • de démonstration ; • de recette des modifications apportées sur le système d'information de production ; à la demande : • d'un Abonné ; • de Worldline France ; pour le compte : • d'une personne physique (Titulaire) ; • d'une organisation ; • de Worldline France. Récupération du certificat : • Lors de l'envoi du contrat signé en PDF, le signataire peut récupérer son certificat en double cliquant sur sa signature. • Ainsi la fenêtre « Signature Validation Status » s'ouvre, et le signataire doit cliquer sur « Signature Properties… » • Enfin cliquer sur « Show Certificate » Le certificat apparait. Ces certificats de test ne peuvent être utilisés dans d'autres contextes. Un ensemble d'actions et de moyens est mis en place, lors de la procédure

<table>
<tr><th>Type d'information</th><th>Description</th></tr>
<tr><td></td><td>d'enregistrement, afin d'identifier les demandeurs et futurs Titulaires de certificats et valider les informations présentes au sein des certificats émis (cf. chapitre 3.2 de la [PC-DPC]).

Les conditions d'acceptations des Certificats sont les suivantes :

<table>
<tr><th>Type de certificat</th><th>Conditions d'acceptation</th></tr>
<tr><td>Certificat à usage unique</td><td>L'acceptation explicite des données contenues au sein du Certificat par le futur Titulaire se fait en amont de l'émission de celui-ci.</td></tr>
<tr><td>Certificat d'Organisation</td><td>L'acceptation explicite des données contenues au sein du Certificat soit par le représentant légal ou statutaire de l'Abonné qui a fait la demande, soit par l'individu habilité identifié dans le Certificat se fait dans les dix (10) jours ouvrés consécutifs à la génération dudit Certificat par e-mail. Une fois cette période arrivée à échéance, le Certificat est réputé conforme.</td></tr>
<tr><td>Certificat Permanent</td><td>L'acceptation explicite des données contenues au sein du Certificat par le Titulaire du Certificat, Abonné au service du TSP, qui a fait la demande dans les dix (10) jours ouvrés consécutifs à la génération dudit Certificat par e-mail. Une fois cette période arrivée à échéance, le Certificat est réputé conforme.</td></tr>
</table>
</td></tr>
<tr><td>Limites d'usage des certificats</td><td>Les certificats produits ne sont utilisables que dans le cadre de procédure de souscription ou de transmission dématérialisée, afin de :

• signer électroniquement un document statique électronique au format PDF avec un certificat à usage unique ou un certificat permanent ;

• sceller électroniquement un document statique électronique au format PDF avec un certificat organisation (cachet électronique).

Les données archivées sont définies au chapitre 5.5.1 de la [PC-DPC].

La période de conservation de ces données est dépendante de la donnée en question et de sa finalité.
La durée de conservation des archives des dossiers d'enregistrement pour un certificat à usage unique est de huit (8) ans. La durée de conservation des archives des dossiers d'enregistrement pour un certificat d'organisation est de dix (10) ans. Ceci en cohérence avec les obligations qui pèsent sur les prestataires de service de certification.
Plus de détails définis au chapitre 5.5.2 de la [PC-DPC].</td></tr>
<tr><td>Obligations des porteurs de certificats</td><td>Les porteurs de certificat ont pour obligation de :

• protéger les moyens d'accès aux clés privées et aux certificats ;

• n'utiliser leurs certificats que pour les usages prévus et définis dans la [PC-DPC] associée ;

• révoquer ou demander la révocation de leur certificat en cas de compromission ou de suspicion de compromission si celui-ci n'est pas</td></tr>
</table>

Type d'information	Description
	expiré; • révoquer ou demander la révocation de leur certificat en cas de compromission ou de suspicion de compromission des moyens d'accès si celui-ci n'est pas expiré; • révoquer ou demander la révocation de leur certificat si celui contient des informations devenues obsolètes si celui-ci n'est pas expiré; • Ne plus utiliser sa clef privée en cas de compromission ou suspicion de compromission ; • vérifier et respecter les obligations qui leur incombent décrites dans le présent document et dans la [PC-DPC] et, dans le cas de certificats à usage unique, dans le contrat noué avec leur mandataire, ici désigné comme étant l'Abonné. Avant d'accorder sa confiance au dit certificat, le porteur de certificat doit impérativement vérifier sa validité auprès du TSP Mediacert en consultant les Listes des Certificats Révoqués appropriées les plus récentes, ainsi qu'en vérifiant sa validité intrinsèque, en particulier sa date d'expiration et sa signature, et la validité du certificat. A défaut de remplir cette obligation, le porteur de certificat assume seul tous les risques de ses actions non conformes aux exigences de la [PCDPC], le TSP Mediacert ne garantissant, dès lors, plus aucune valeur juridique aux certificats qu'il a émis et qui pourraient avoir été révoqués ou qui ne seraient pas valides. De plus, le futur titulaire à l'obligation de communiquer des informations et des justificatifs, demandés par l'Abonné, qu'il certifie exacts et à jour lors de la demande de certificat. Les obligations qui incombent au futur titulaire sont par ailleurs définies dans le contrat conclu avec son mandataire, ici désigné comme étant l'Abonné. Les obligations spécifiques de **l'Abonné**, qui s'ajoutent à celles énumérées ci-dessus, sont définies au chapitre 9.6.3 de la [PC-DPC] ainsi que dans les [CGA] qu'il a signé avec Worldline France.
Obligations des utilisateurs de certificats	Les utilisateurs de certificats générés par les AC en ligne ont pour obligation s'ils veulent pouvoir bénéficier desdits certificats de : • prendre connaissance des conditions générales de service et de les accepter de manière explicite de même qu'accepter la délivrance de certificat en leurs noms ; • vérifier et respecter les obligations qui leur incombent et qui figurent dans la [PC-DPC] et dans les présentes Conditions Générales des Services. Ces obligations devront également lui avoir été décrites par l'Abonné pour les Certificats à usage unique dans le contrat qui le lie à lui. Ce contrat expose le fonctionnement d'une signature sous forme électronique, les implications de ce choix, les modalités pour y procéder avec les recueils des consentements nécessaires en conformité avec celles figurant dans le propre Contrat d'Abonnement de l'Organisation; • vérifier et respecter l'usage pour lequel un certificat a été émis ;

Type d'information	Description
	• vérifier la validité du certificat (expiration, révocation, intégrité) et celle de chaque certificat de la chaîne de certification.
Exigences de vérification du statut des certificats par les utilisateurs	Dans le cadre d'utilisation d'un certificat à usage unique fourni par l'une des AC en ligne, la [PC-DPC] ne formule, compte tenu du caractère atomique de l'opération de signature, aucune exigence concernant l'obligation de vérification de la révocation du certificat. Dans le cadre d'utilisation d'un certificat d'organisation fourni par l'AC, l'utilisateur se doit de vérifier le statut du certificat auquel il compte se fier avant de l'utiliser. Pour cela, il peut utiliser les différents services d'information mis à sa disposition par l'AC. En plus du statut, l'utilisateur se doit de vérifier la validité du certificat en question et de la chaîne de certification correspondante.
Limites de garanties et de responsabilités	Les AC en ligne s'engagent à émettre des certificats en conformité avec la PC-DPC, ainsi qu'avec l'état de l'art et de la technique. Le TSP Mediacert garantit via ses services : • l'authentification de l'Abonné avec son certificat par l'Autorité d'Enregistrement ; • la génération de certificat(s) conformément à la demande de l'Abonné, préalablement authentifié et vérifiée ; • la mise à disposition 7j/7 24h/24 de fonctions d'informations sur l'état des certificats émis, suite à la demande de l'Abonné, par les AC conformément au présent document ; • le contrôle exclusif de la clé privée du certificat par le Dispositif Porteur de Certificats et la destruction de cette même clé à l'issue d'une session unique d'utilisation dans le cas d'un certificat à usage unique. Aucune autre garantie n'est assurée. La responsabilité du TSP Mediacert ne peut être engagée qu'en cas de non-respect prouvé de ses obligations. Le TSP Mediacert ne pourra être tenue responsable dans le cas d'une faute sur le périmètre d'une entité Abonnée, notamment en cas : • d'utilisation d'un certificat expiré ; • d'utilisation d'un certificat révoqué ; • d'utilisation d'un certificat dans le cadre d'une application autre que celles décrites dans la rubrique « *Limites d'usage des certificats* » du présent document. Les AC ne sont d'une façon générale pas responsables des documents et informations transmises par l'Abonné et ne garantissent pas leur exactitude ni les conséquences de faits, actions, négligences ou omissions dommageables de l'Abonné, de son représentant ou du Titulaire. L'Abonné s'interdit de prendre un engagement au nom et pour le compte des AC auxquelles elle ne saurait en aucun cas se substituer.

Type d'information	Description
Références applicables	Les références applicables sont définies au chapitre 2.3 du présent document. La documentation des AC en ligne est disponible sur son site web à l'adresse suivante : https://www.mediacert.com.
Politique de confidentialité	Worldline France prend toutes les mesures nécessaires pour assurer la confidentialité des données professionnelles (cf. chapitre 9.3 de la [PC-DPC]) et personnelles (cf. chapitre 9.4 de la [PC-DPC]) conformément à la législation française en vigueur sur le territoire français.
Politique d'indemnisation	La délivrance de certificats par les AC concernées par le présent document est opérée dans le cadre de services de plus haut niveau tels que notamment de souscription électronique. Le contrat cadre signé entre l'Abonné et Worldline France ou ses filiales, ou son mandataire dument habilité, précise les conditions d'indemnisation en cas de dommage. En l'absence de contrat cadre, les [CGV] de Worldline France s'appliqueront.
Loi applicable	Les IGC en ligne dans toutes leurs composantes et y compris documentaires sont régies par la législation et la réglementation en vigueur sur le territoire français qui lui est applicable, bien que leurs activités qui découlent de la [PC-DPC] puissent avoir des effets juridiques en dehors du territoire français. Le contrat cadre signé entre le client et Worldline France ou ses filiales, ou son mandataire dument habilité, précise les dispositions concernant la résolution de conflits. En l'absence de contrat cadre, les [CGV] de Worldline France s'appliqueront. Le contact habilité pour toute remarque, demande d'informations complémentaires, réclamation ou remise de dossier de litige concernant la [PC-DPC] est défini dans la rubrique *« Point de contact »* du présent document.
Audits de l'AC	Worldline France procède régulièrement à un audit externe de certification à la norme [ETSI EN 319 411-1] des IGC en ligne par un organisme indépendant et accrédité.