



CONDITIONS SPECIFIQUES D'UTILISATION DES SERVICES

Universign

1. Conditions Spécifiques d'Utilisation du service de signature électronique

Les présentes Conditions Spécifique d'Utilisation (CSU) ont pour objet de définir les conditions d'accès au Service de Signature Électronique et son utilisation. Elles complètent les CGU des services Universign, sur lesquelles elles prévalent et les Politiques de Certification.

Avant toute utilisation du Service, l'Utilisateur reconnaît :

- avoir pris connaissance des présentes CSU ;
- disposer de la capacité juridique et des habilitations pour s'engager au titre des présentes CSU
- accepter sans réserve les présentes CSU.

L'acceptation de l'Utilisateur est matérialisée en cliquant sur la case à cocher sur le site lors de la création d'un compte d'Utilisateur ou préalablement à la signature.

Les CSU sont mises à sa disposition par Universign sur son Site. Elles peuvent être téléchargées au format PDF.

> DÉFINITIONS

- **Autorité de Certification (AC)** : désigne l'autorité en charge de la création, la délivrance, la gestion et la révocation des Certificats au titre de la Politique de Certification.
- **Certificat Électronique ou Certificat** : désigne le fichier électronique délivré par l'Autorité de Certification comportant les éléments d'identification de son Porteur et une clé cryptographique permettant la vérification de la Signature Électronique pour lequel il est utilisé.
- **Certificat qualifié** : désigne un Certificat répondant aux exigences de l'article 28 ou 38 du Règlement Européen n°910/2014 du 23 juillet 2014
- **Politique de Certification (PC)** : désigne l'ensemble des règles auxquelles l'AC se conforme pour la mise en œuvre du Service de certification.
- **Porteur** : désigne la personne, physique ou morale, identifiée dans le Certificat ayant sous son contrôle la clé privée correspondant à la clé publique
- **Service** : désigne l'ensemble des prestations et solutions logicielles qu'Universign s'engage à fournir à l'Utilisateur dans le cadre des présentes.

> Article 1 – SERVICE DE SIGNATURE ÉLECTRONIQUE

Le Service de Signature Electronique permet au Signataire de disposer d'une solution de création de Signature Electronique et au Client de la recueillir.

DISPOSITIONS APPLICABLES AU SIGNATAIRE

Article 1.1. – ACCÈS AU SERVICE

Le Signataire peut bénéficier du Service proposé à la condition de disposer :

- d'un équipement informatique adapté pour accéder au Service ;
- d'une adresse e-mail valide et personnelle (. dont il contrôle l'accès) ;
- d'un moyen d'authentification personnel accepté par Universign (ex : un numéro de téléphone portable personnellement attribué)

VERSION	DIFFUSION : <i>RESTREINT</i>	PAGE
02/20		1 / 14

Les Signatures Électroniques de niveau 2 et 3 nécessitent l'émission d'un Certificat dont le Porteur est le Signataire.

Article 1.2. – CRÉATION D'UN COMPTE UNIVERSIGN

L'accès au Service et son utilisation nécessitent la création d'un Compte d'Utilisateur.

Par exception, la Signature Électronique de niveau 1 ne nécessite pas de création de Compte d'Utilisateur au bénéfice du Signataire.

Article 1.3. – UTILISATION DU SERVICE

Le processus de Signature Électronique des Documents repose sur les étapes suivantes :

- Etape 1 : Mise à disposition du Document

Le Client, via son Compte d'Utilisateur, met le Document à signer et, le cas échéant y ajoute un Document à lire, à disposition du Signataire.

- Etape 2 : Invitation à signer

Le Signataire est invité à signer le Document via le Service.

Le cas échéant, un e-mail contenant un hyperlien permettant l'accès au Service est adressé au Signataire.

- Etape 3 : Accès au Document

Le Signataire est dirigé vers une interface affichant le Document à signer. Il est invité à prendre connaissance de l'intégralité du Document.

- Etape 4 : Consentement au Document et aux CSU/CGU

Le Signataire déclare avoir pris connaissance du Document et, lorsque la Signature est requise, approuver son contenu. Le Signataire déclare également accepter les présentes CSU complétées des CGU reconnaissant ainsi la validité et l'opposabilité de la Signature Électronique.

L'acceptation du Signataire est matérialisée en cliquant sur la case à cocher correspondant à ces déclarations.

- Etape 5 : Signature – Authentification

Le Signataire clique sur le bouton « signer » pour activer la Signature. Pour assurer la fiabilité de la Signature, le Signataire reçoit un code confidentiel adressé sur le numéro téléphone qu'il a déclaré à Universign ou au Client. Dès réception du code d'authentification, le Signataire s'authentifie en saisissant ce code afin de créer la Signature Électronique du Document.

Le Signataire est informé et accepte que les conditions de recueil de sa Signature Électronique sont satisfaisantes pour produire des effets juridiques et que sa Signature Électronique pourra lui être valablement opposée.

Article 1.4. – LIMITES D'UTILISATION

Le Signataire s'engage à réaliser lui-même et conformément aux CGU et CSU les étapes qui constituent la Signature Électronique. La délégation de ces opérations, la délégation de de signature et la signature pour ordre sont prohibées.

DISPOSITIONS APPLICABLES AU CLIENT

Article 1.5. – ACCÈS AU SERVICE

L'accès au Service et son utilisation par le Client nécessitent la création d'un Compte d'Utilisateur.

VERSION	DIFFUSION : <i>RESTREINT</i>	PAGE
02/20		2 / 14

Article 1.6. – UTILISATION DU SERVICE

Le Client s'engage à fournir à Universign des informations exactes pour l'utilisation du Service.

Le processus de mise à la Signature Électronique de Documents repose sur les étapes suivantes :

Etape 1 : Mise à disposition du Document

Le Client via son Compte d'Utilisateur met le Document à signer et le cas échéant, à lire, à disposition du Signataire.

Etape 2 : Invitation à signer

Le Client complète les données relatives au Signataire requises par le Service.

Etape 3 : Accès au Document signé

L'accès au Document signé valant original est accessible via le compte d'Utilisateur du Client.

Article 1.7. – LIMITES D'UTILISATION

Le Client s'engage à ne pas détourner les fonctionnalités du Service ou les moyens d'authentification du Signataire, notamment en renseignant des informations relatives au Signataire qu'il sait erronées ou en ne permettant au Signataire de visualiser correctement le Document à signer ou saisissant lui-même le code confidentiel adressé au Signataire.

Toute utilisation du Service non conforme aux CGU et CSU est susceptible d'entraîner l'inopposabilité de la Signature Électronique et/ou la nullité de l'acte sur lequel elle est apposée.

> Article 2 – NIVEAUX DE SIGNATURE ÉLECTRONIQUE

Le Service permet la mise en œuvre de trois niveaux de Signature Électronique dont les effets juridiques sont reconnus par la réglementation applicable sur le territoire de l'Union Européenne.

2.1. SIGNATURE ÉLECTRONIQUE DE NIVEAU 1

Dans le cadre de la mise en œuvre de la Signature de niveau 1, l'identification du Signataire incombe au Client au moyen de processus organisationnels et techniques qui lui sont propres et qu'il met en œuvre sous sa seule responsabilité.

Universign authentifie le Signataire au moyen du numéro de téléphone du Signataire déclaré à Universign (par le Signataire lui-même ou par le Client), le cas échéant.

La Signature Électronique de niveau 1 ne nécessite pas la création d'un compte Universign de la part du Signataire.

Dans le cadre de l'utilisation de cette Signature, Universign ne peut garantir l'identité du Signataire, les seuls éléments fournis étant ceux communiqués par le Client.

Les données d'identification qui figurent sur la Signature Électronique sont celles transmises par le Client à Universign.

2.2 SIGNATURE ÉLECTRONIQUE DE NIVEAU 2

Dans le cadre de la mise en œuvre de la Signature Électronique de niveau 2, le contrôle de l'identification du Signataire est réalisé à distance au moyen de la copie numérique de sa pièce d'identité adressée à Universign.

Universign authentifie le Signataire au moyen du numéro de téléphone du Signataire déclaré à Universign (par le Signataire lui-même ou par le Client), le cas échéant.

VERSION	DIFFUSION : <i>RESTREINT</i>	PAGE
02/20		3 / 14

Dans le cadre de l'utilisation de cette Signature, Universign ne peut garantir l'identité du Signataire. En conséquence, il incombe au Client de s'assurer par ses propres moyens et sous sa seule responsabilité de l'identité du Signataire.

Universign vérifie la cohérence entre données d'identification déclarées et le justificatif d'identité dont la copie lui a été transmise.

La Signature Électronique de niveau 2 est réalisée au moyen de Certificats conformes aux exigences de la norme ETSI EN 319 411-1.

2.3. SIGNATURE ÉLECTRONIQUE DE NIVEAU 3

Dans le cadre de la mise en œuvre de la Signature Électronique de niveau 3, Universign vérifie l'identité du Signataire en sa présence et au moyen d'un justificatif d'identité.

Universign authentifie le Signataire au moyen du numéro de téléphone du Signataire déclaré à Universign (par le Signataire lui-même ou par le Client), le cas échéant.

La Signature Électronique de niveau 3 est réalisée au moyen de Certificats qualifiés et conformes aux exigences de la norme ETSI EN 319 411-2.

> **Article 3- STOCKAGE DES DOCUMENTS**

Universign stocke, à la demande du Client, de manière à en préserver l'intégrité, les Documents signés au moyen du Service. Le stockage permet au Client la consultation en ligne des Documents signés, leur conservation, leur restitution et/ou leur destruction.

La fonction du service de conservation électronique est de garantir, pour la durée du stockage, l'intégrité des documents signés et l'extension de la fiabilité des Signatures Électroniques au-delà de leur période de validité technologique.

Universign se réserve le droit de stocker les Documents signés auprès d'un partenaire commercial spécialisé.

Les Documents sont stockés à compter de leur dépôt et jusqu'à la fermeture du Compte d'Utilisateur du Client.

Il appartient à l'Utilisateur de prendre toute disposition de manière à conserver les Documents qui ne sont plus ou pas stockés par le Service de manière pérenne et intègre.

> **Article 4 – OBLIGATIONS DES UTILISATEURS**

Article 4.1. – OBLIGATIONS DU CLIENT

Le Client s'engage à ce :

- que le contenu des Documents soit licite et ne permette pas d'effectuer des actes illicites ou contraires aux lois et réglementations applicables ;
- que le contenu des Documents ne portent pas atteinte à la vie privée des personnes et/ou aux dispositions relatives à la protection des données à caractère personnel et/ou au droit de la concurrence, et/ou au droit de la consommation ;
- le cas échéant, si le Client agit en qualité de commerçant ou de professionnel, qu'il respecte les obligations lui incombant au regard de son statut, notamment en termes de mentions obligatoires et de transmission des Documents signés.

L'utilisation du Service en dehors de ces garanties engage la seule responsabilité du Client.

VERSION	DIFFUSION : <i>RESTREINT</i>	PAGE
02/20		4 / 14

Article 4.2. – OBLIGATIONS DU SIGNATAIRE

Le Signataire s'engage à :

- fournir à Universign des informations exactes pour l'utilisation du Service, notamment ses données d'identification et d'authentification (nom, prénom, adresse e-mail, numéro de téléphone, ...).
- assurer la confidentialité de son Identifiant et du ou des code(s) confidentiel(s) qui lui sont adressés

> **Article 5 – LIMITES DE RESPONSABILITÉ**

Universign ne contrôle pas le contenu des Documents, aussi sa responsabilité ne saurait donc être engagée relativement à la valeur et/ou la validité du contenu des Documents ou le défaut de celles-ci.

La responsabilité d'Universign ne saurait être engagée des conséquences par les décisions qui pourraient être prises ou des actions qui pourraient être entreprises à partir de ces Documents (qu'ils soient signés ou non).

Universign ne peut être tenue pour responsable d'un usage inapproprié du Service au regard de la réglementation applicable aux Documents.

> **Article 6 – GARANTIES ET LIMITES DE GARANTIES**

Dans le cadre de la mise en œuvre de la Signature Électronique de niveau 3, Universign garantit l'utilisation d'un Certificat qualifié dont la délivrance est subordonnée à la vérification de l'identité du Signataire par des moyens appropriés et conformes au droit français.

Sous réserve du respect par les Utilisateurs des CGU et des CSU applicables, Universign garantit l'opposabilité, au sens de la réglementation européenne, des Signatures Électroniques créées au moyen du Service.

Universign ne vérifie en aucun cas que le Service corresponde aux régimes juridiques applicables aux Documents. En conséquence, la fourniture du Service ne saurait dispenser les Utilisateurs d'une analyse et de vérifications concernant les exigences légales et/ou réglementaires applicables.

> **Article 7 – CONSERVATION DES DONNÉES**

Les données des journaux d'évènements relatifs au Service sont conservées pendant 15 ans à compter de leur émission. Elles sont susceptibles d'être transmises aux autorités administratives et judiciaires en cas de contrôle ainsi qu'aux parties intéressées en cas de contentieux portant sur la validité de la Signature.

2. Conditions Spécifiques d'Utilisation du service d'horodatage

Les présentes Conditions Spécifiques d'Utilisation (CSU) ont pour objet de définir les conditions d'accès au Service d'Horodatage Universign et son utilisation. Elles complètent les CGU des services Universign sur lesquelles elles prévalent et la Politique d'Horodatage.

Avant toute utilisation du Service, l'Utilisateur reconnaît :

- avoir pris connaissance des présentes CSU ;
- disposer de la capacité juridique et des habilitations pour s'engager au titre des présentes CSU
- accepter sans réserve les présentes CSU.

L'acceptation de l'Utilisateur est matérialisée en cliquant sur la case à cocher sur le site lors de la création d'un compte d'Utilisateur.

Les CSU sont mises à sa disposition par Universign sur son site internet. Elles peuvent être téléchargées au format PDF.

> DÉFINITIONS

- **Autorité d'Horodatage (AH)** : désigne l'autorité en charge de l'émission des Contremarques de temps au titre de la Politique d'Horodatage.
- **Cachet Electronique** : désigne un procédé permettant de garantir l'origine et l'intégrité du Document sur lequel il est apposé.
- **Contremarque de temps**: désigne une structure qui lie un Document à un instant particulier, établissant ainsi la preuve qu'il existait à cet instant-là.
- **Horodatage** : désigne un procédé permettant d'attester, au moyen de Contremarques de temps, qu'un Document a existé à un moment donné.
- **Politique de Certification (PC)** : désigne l'ensemble des règles auxquelles l'AC se conforme pour la mise en œuvre du service de certification.
- **Politique d'Horodatage (PH)** : désigne l'ensemble des règles auxquelles l'AH se conforme pour la mise en œuvre du Service d'horodatage
- **Service** : désigne l'ensemble des prestations et solutions logicielles qu'Universign s'engage à fournir à l'Utilisateur dans le cadre des présentes.

> Article 1 – SERVICE D'HORODATAGE

Le Service permet d'horodater des Documents au moyen de Contremarques de temps émises selon la Politique d'Horodatage qui décrit plus précisément la mise en œuvre et l'organisation du Service.

Article 1.1. – ACCÈS AU SERVICE

L'accès au Service nécessite de disposer :

- d'équipements logiciels et matériels adaptés pour accéder au Service ;
- d'un Compte d'Utilisateur.

L'utilisation du Service au moyen de l'API nécessite la configuration du système d'information de l'Utilisateur selon les prescriptions de la Documentation.

VERSION	DIFFUSION : <i>RESTREINT</i>	PAGE
02/20		6 / 14

Article 1.2. – UTILISATION DU SERVICE

L'Utilisateur adresse au Service le Document à horodater, par le biais de l'API, conformément à la Documentation.

Le Service adresse en réponse à la requête de l'Utilisateur une Contremarque de temps dont les éléments constitutifs sont décrits dans la Politique d'Horodatage.

Article 1.3. – LIMITES D'UTILISATION

Le Service ne doit pas être utilisé pour établir la preuve qu'un courrier électronique a bien été transmis à un destinataire ou reçu par lui.

Le Service ne constitue pas un service d'envoi recommandé électronique.

Le Service ne doit pas être utilisé avec pour objectif d'identifier l'auteur ou l'origine du Document.

> Article 2 – GARANTIES ET LIMITES DE GARANTIES

Sous réserve du respect par l'Utilisateur des CGU et des CSU applicables, Universign garantit l'opposabilité, au sens de la réglementation européenne, des Contremarques de temps créées au moyen du Service.

L'Horodatage réalisé au moyen du Service bénéficie d'une présomption d'exactitude de la date et de l'heure contenues dans la Contremarque de temps et d'intégrité du Document auquel se rapporte cette Contremarque.

Le Service d'Horodatage est synchronisé avec le temps universel coordonné afin que la précision des Contremarques de temps soit d'une (1) seconde.

Les Contremarques sont scellées au moyen d'un Cachet Électronique.

En cas d'évènement affectant la sécurité du Service et qui pourraient avoir une conséquence sur les Contremarques, une information appropriée sera mise à la disposition des Utilisateurs via le Site de publication.

Les informations nécessaires à la mise en œuvre de la procédure de vérification des Contremarques de temps décrite dans la Politique d'Horodatage sont disponibles sur le Site de publication.

Universign ne garantit pas l'adéquation du Service aux besoins de l'Utilisateur. Il appartient à l'Utilisateur de vérifier cette adéquation, notamment en s'assurant que les dispositions de la Politique d'Horodatage répondent à ses exigences propres.

> Article 3 – OBLIGATIONS DE L'UTILISATEUR

L'Utilisateur s'engage à vérifier la validité des Contremarques dès leur réception selon la procédure de vérification décrite dans la Politique d'Horodatage.

En dehors des cas prévus par la Politique d'Horodatage, les Contremarques de temps peuvent être vérifiées pendant cinq ans à compter de leur émission.

L'Utilisateur s'engage également à vérifier que le Document horodaté est bien celui transmis à Universign pour Horodatage.

Le Service ne réalise aucun archivage des Contremarques de temps émises.

> **Article 4 – RESPONSABILITÉS**

L'Utilisateur s'engage à fournir à Universign des informations exactes pour l'utilisation du Service.

L'archivage des Contremarques de temps relève de la seule responsabilité de l'Utilisateur.

> **Article 5 – CONSERVATION DES DONNÉES**

Conformément à la Politique d'Horodatage et à la réglementation applicable, Universign conserve les données relatives au fonctionnement du service pendant six (6) ans.

> **Article 6 – POLITIQUE ET NORMES**

Universign s'engage à se conformer aux politiques et aux normes mentionnées dans le tableau suivant.

1.3.6.1.4.1.15819.5.1.1	ETSI EN 319 411-1	PC de l'Autorité d'Horodatage
1.3.6.1.4.1.15819.5.2.2	ETSI EN 319 421	Politique d'Horodatage

Ces Politiques sont publiées sur le Site de publication. Elles sont auditées selon la norme EN 319 403 par un organisme accrédité.

3. Conditions Spécifiques d'Utilisation du service de cachet électronique

Les présentes Conditions Spécifique d'Utilisation (CSU) ont pour objet de définir les conditions d'accès au Service de Cachet Électronique et son utilisation. Elles complètent les CGU des services Universign, sur lesquelles elles prévalent et les Politiques de Certification.

Avant toute utilisation du Service, l'Utilisateur reconnaît :

- avoir pris connaissance des présentes CSU ;
- disposer de la capacité juridique et des habilitations pour s'engager au titre des présentes CSU
- accepter sans réserve les présentes CSU.

L'acceptation de l'Utilisateur est matérialisée en cliquant sur la case à cocher sur le site lors de la création d'un compte d'Utilisateur.

Les CSU sont mises à sa disposition par Universign sur son Site. Elles peuvent être téléchargées au format PDF.

> DÉFINITIONS

- **Autorité de Certification (AC)** : désigne l'autorité en charge de la création, la délivrance, la gestion et la révocation des Certificats au titre de la Politique de Certification.
- **Cachet Electronique** : Désigne un procédé permettant de garantir l'origine et l'intégrité du Document sur lequel il est apposé.
- **Certificat Électronique ou Certificat** : désigne le fichier électronique délivré par l'Autorité de Certification comportant les éléments d'identification de son Porteur et une clé cryptographique permettant la vérification du Cachet Électronique pour lequel il est utilisé.
- **Certificat qualifié** : désigne un Certificat répondant aux exigences de l'article 28 ou 38 du Règlement Européen n°910/2014 du 23 juillet 2014
- **Politique de Certification (PC)** : désigne l'ensemble des règles auxquelles l'AC se conforme pour la mise en œuvre du service de certification.
- **Porteur** : désigne la personne, physique ou morale, identifiée dans le Certificat ayant sous son contrôle la clé privée correspondant à la clé publique
- **Service** : désigne l'ensemble des prestations et solutions logicielles qu'Universign s'engage à fournir à l'Utilisateur dans le cadre des présentes.

> Article 1 – SERVICE DE CACHET ÉLECTRONIQUE

Le Service permet de sceller des Documents au format PDF au moyen de Certificats et de leur clé cryptographique associée.

Article 1.1. – ACCÈS AU SERVICE

L'accès au Service nécessitent de disposer :

- d'équipements logiciels et matériels adaptés pour accéder au Service ;
- un Compte d'Utilisateur ;
- d'un Certificat de personne morale associé à des clés cryptographiques conformes à l'une des Politique de Certification mentionnée aux présentes.

VERSION		PAGE
02/20	DIFFUSION : <i>RESTREINT</i>	9 / 14

L'accès au Service au moyen de l'API nécessite la configuration du système d'information de l'Utilisateur selon les prescriptions de la Documentation.

La Documentation est fournie par Universign sur demande de l'Utilisateur après la création de son Compte.

Article 1.2. – UTILISATION DU SERVICE

L'Utilisateur adresse au Service le Document à sceller, par le biais de l'API, conformément à la Documentation.

Le Service adresse en réponse à la requête de l'Utilisateur le Document sur lequel a été apposé un Cachet Électronique.

Article 1.3. – LIMITES D'UTILISATION

Le Service permet d'apposer un Cachet Électronique sur un Document. Il ne doit pas être utilisé pour établir la preuve du consentement du Porteur du Certificat utilisé pour le Cachet Électronique. Le Cachet Électronique ne constitue pas une signature électronique au sens de la réglementation européenne.

> Article 2 – CATÉGORIES DE CACHET ÉLECTRONIQUE

Le Service permet la mise en œuvre de deux catégories de Cachet Électronique dont les effets juridiques sont reconnus par la réglementation applicable sur le territoire de l'Union Européenne.

2.1. CACHET ELECTRONIQUE DE NIVEAU 1

Les Cachets Électroniques de catégorie 1 sont créés au moyen de Certificats conformes aux exigences de la norme ETSI EN 319 411-1 qui prévoit notamment la possibilité de vérifier à distance les données d'identification du Porteur.

2.2 CACHET ELECTRONIQUE DE NIVEAU 2

Les Cachets Électroniques de catégorie 2 sont créés au moyen de Certificats qualifiés et conformes aux exigences de la norme ETSI EN 319 411-2 qui prévoit notamment la vérification des justificatifs du Porteur en la présence de son représentant expressément autorisé.

> Article 3 – GARANTIES ET LIMITES DE GARANTIES

Sous réserve du respect par l'Utilisateur des CGU et des CSU applicables, Universign garantit l'opposabilité, au sens de la réglementation européenne, des Cachets Électroniques créés au moyen du Service.

Universign ne garantit pas l'adéquation du Service aux besoins de l'Utilisateur. Il appartient à l'Utilisateur de vérifier cette adéquation, notamment en s'assurant que les dispositions de la Politique de Certification répondent à ses exigences propres.

> Article 4 – OBLIGATIONS DE L'UTILISATEUR

L'Utilisateur s'engage également à vérifier que le Document scellé est bien celui transmis à Universign pour la création d'un Cachet Électronique.

Le Service ne réalise aucun archivage des Documents scellés.

VERSION		PAGE
02/20	DIFFUSION : <i>RESTREINT</i>	10 / 14

> **Article 5 – RESPONSABILITÉS**

L'Utilisateur s'engage à fournir à Universign des informations exactes pour l'utilisation du Service.

L'archivage des Documents scellés relève de la seule responsabilité de l'Utilisateur.

> **Article 6 – POLITIQUES ET NORMES**

Universign s'engage à se conformer aux politiques et aux normes mentionnées dans le tableau suivant.

1.3.6.1.4.1.15819.5.1.3.4	ETSI EN 319 411-1	PC pour les certificats de personnes morales, niveau LCP
1.3.6.1.4.1.15819.5.1.3.5	ETSI EN 319-411-2	PC pour les certificats de personnes morales, niveau QCP-I

Ces Politiques sont publiées sur le Site de publication. Elles sont auditées selon la norme EN 319 403 par un organisme accrédité.

4. Conditions Spécifiques d'Utilisation du service de gestion des clés cryptographiques

Les présentes Conditions Spécifiques d'Utilisation (CSU) ont pour objet de définir les conditions d'utilisation du Service de gestion des Clés cryptographiques. Elles complètent les CGU des services Universign, sur lesquelles elles prévalent et les Politiques de Certification. Avant toute utilisation du Service, l'Utilisateur reconnaît :

- avoir pris connaissance des présentes CSU ;
- avoir consenti aux CSU du service de Signature Électronique et ou aux CSU du service de Cachet Électronique
- disposer de la capacité juridique et des habilitations pour s'engager au titre des présentes CSU accepter sans réserve les présentes CSU.

L'acceptation de l'Utilisateur est matérialisée en cliquant sur la case à cocher sur le site lors de la création d'un compte d'Utilisateur ou préalablement à la signature. Les CSU sont mises à sa disposition par Universign sur son Site. Elles peuvent être téléchargées au format PDF.

> DÉFINITIONS

- **Bi-clé** : désigne un couple de clés cryptographiques composé d'une clé privée et d'une clé publique associées à un Certificat émis par l'Autorité de Certification.
- **Dossier d'enregistrement** : désigne le dossier à l'appui duquel est réalisée la demande de Certificat contenant les informations et documents justificatifs requis par la PC.
- **Personnes Autorisées** : désigne les personnes expressément autorisées par le Porteur à utiliser la clé privée associée au Certificat de Cachet Électronique émis à son nom.
- **Responsable du Certificat** : désigne la personne physique responsable du cycle de vie du Certificat de Cachet Électronique. Il s'agit d'un représentant légal du Porteur ou d'une personne dument mandatée à cet effet par un représentant légal de Porteur.
- **Service de certification** : désigne le service Universign d'émission de Certificat.

> Article 1 – SERVICE DE GESTION DES CLÉS CRYPTOGRAPHIQUES

Le Service de Gestion des clés cryptographiques permet au Porteur de générer une Bi-clé associée à un Certificat et de l'utiliser à distance pour signer ou sceller des Documents au moyen d'une Signature Électronique ou d'un Cachet Électronique.

Article 1.1. – ACCÈS AU SERVICE

L'accès au Service et son utilisation nécessitent :

- la création d'un Compte d'Utilisateur
- un moyen d'authentification personnel accepté par Universign (ex : un numéro de téléphone portable personnellement attribué)
- la souscription au Service de Certification.

Les conditions d'émission, de gestion et de révocation des Certificats sont prévues par la Politique de Certification.

VERSION		PAGE
02/20	DIFFUSION : <i>RESTREINT</i>	12 / 14

Article 1.2. – UTILISATION DU SERVICE

Pour la création de Signature électronique, la Bi-clé associée au Certificat est activée à distance après authentification du Porteur au moyen d'un code confidentiel adressé sur le numéro de téléphone déclaré auprès d'Universign.

Pour la création de Cachet Électronique, la Bi-clé associée au Certificat est activée à distance après authentification du Porteur ou d'une Personne autorisée au moyen d'un identifiant unique.

Les utilisations par les Personnes Autorisées de la Bi-clé sont réputées être celles du Porteur.

Article 1.3. – LIMITES D'UTILISATION

Universign ne garantit pas l'adéquation du Service aux besoins de l'Utilisateur. Il appartient à l'Utilisateur de vérifier cette adéquation.

> **Article 2 – OBLIGATIONS DE L'UTILISATEUR**

L'Utilisateur s'engage à assurer la sécurité de ses moyens d'authentification de manière à éviter l'utilisation de la Bi-Clé par des tiers non autorisés.

Il s'engage notamment à prendre les mesures nécessaires à garantir la confidentialité des moyens d'activation transmis par Universign et à mettre en œuvre les mesures permettant de garder la Bi-Clé sous le contrôle exclusif des Personnes Autorisées.

> **Article 3 – OBLIGATIONS D'UNIVERSIGN**

Universign s'engage à générer et à activer la Bi-clé du Porteur dans un dispositif cryptographique avec des algorithmes compatibles avec les exigences de la PC correspondant au Certificat.

Le Service de gestion des clés cryptographiques permet au Porteur de garder la Bi-Clé sous son contrôle exclusif pour créer des Signatures Électroniques.

Le Service de gestion des clés cryptographiques permet au Porteur et aux Personnes Autorisées de garder la Bi-Clé sous leur contrôle pour créer des Cachets Électroniques.

Universign assure la protection de la clé privée de la Bi-Clé afin de garantir son intégrité et sa confidentialité.

Universign s'assure par des moyens appropriés que la Bi-Clé ne pourra plus être utilisée après l'expiration ou la révocation du Certificat.

À l'exception des garanties expressément prévues par l'Accord, Universign exclut toute autre garantie expresse ou implicite notamment toute garantie implicite d'adéquation à un usage spécifique, de satisfaction d'exigence du Porteur.

> **Article 4 – RESPONSABILITÉ**

L'Utilisateur engage sa seule responsabilité dans le cas où des conséquences dommageables causées à des tiers résulteraient d'un manquement du Porteur ou des Personnes Autorisées aux conditions de protection de la clé privée de la Bi-Clé et/ou de ses moyens d'authentification.

> **Article 5 – PROPRIÉTÉ INTELLECTUELLE**

Une licence d'utilisation de la Bi-clé est consentie au Porteur ainsi qu'aux Personnes autorisées pour la fourniture du Services de Signature et/ou de Cachet Électronique.

> **Article 6 – CONSERVATION DES DONNÉES**

Universign conserve les données relatives au contrôle des données d'identification de l'Utilisateur et les journaux d'événements liés à l'utilisation de la Bi-clé sont conservés dans des conditions conformes à la politique de protection des données personnelles disponible sur le Site de Publication.

VERSION		PAGE
02/20	DIFFUSION : <i>RESTREINT</i>	14 / 14