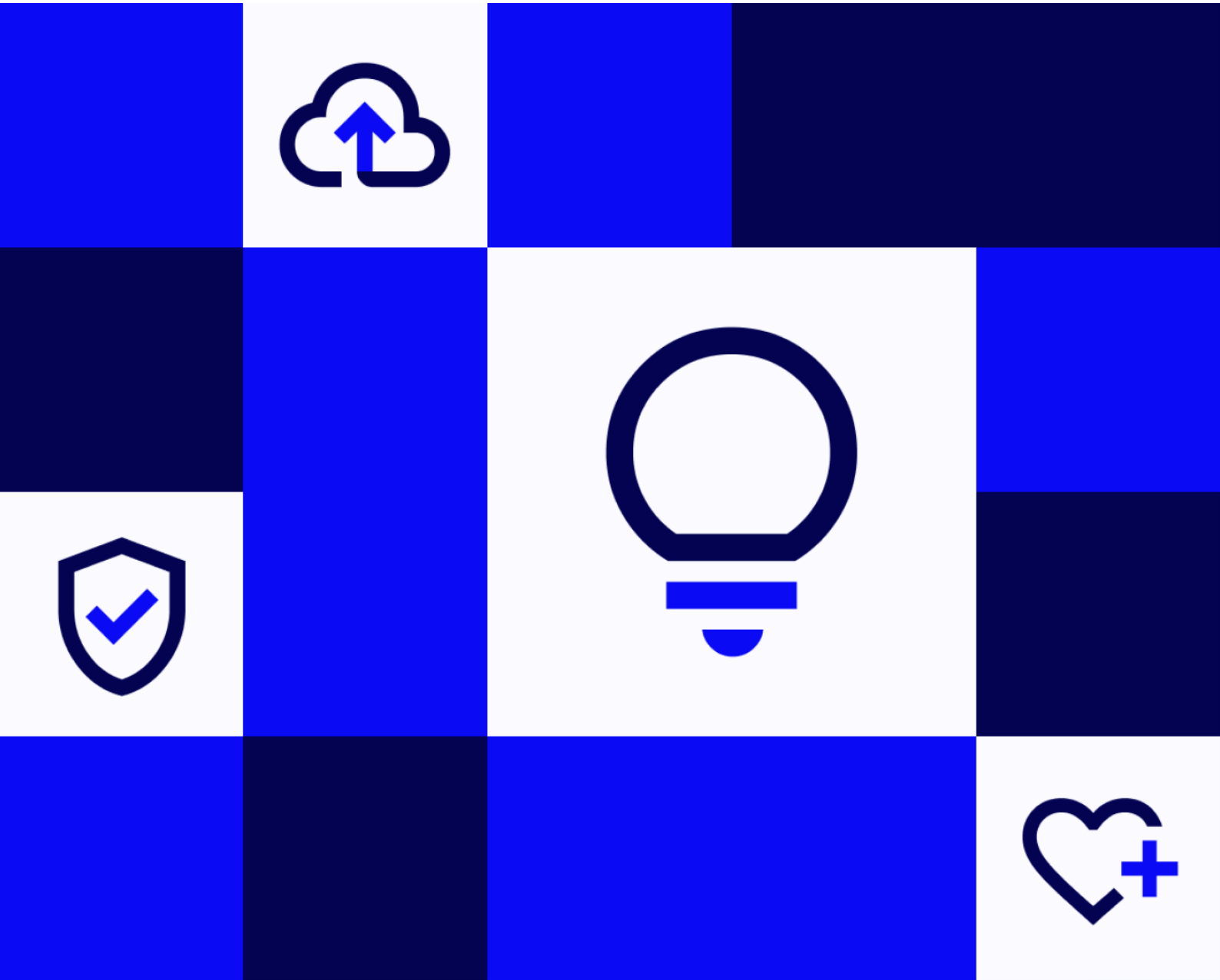
Conditions Spécifiques d'Utilisation des Services



Les présentes Conditions Spécifiques d'Utilisation (ci-après « **Conditions Spécifiques d'Utilisation** » ou « **CSU** ») ont pour objet de définir les conditions spécifiquement applicables aux différents services proposés par la Société Cryptolog International, SAS , sise 5-7, rue du Faubourg Poissonnière, 75009 Paris, RCS de Paris n° 439 129 164 (ci-après « **Universign** »).

DEFINITIONS

Sauf mention contraire, les termes en lettres majuscules ont la signification attribuée au présent article et peuvent être employés au singulier comme au pluriel, en fonction du contexte.

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.

Autorité de Préservation (AP) : désigne l'autorité en charge de la conservation des Signatures Électroniques, qui s'opère notamment via contrôles réalisés sur ces éléments et des méthodes d'extension de la fiabilité des Signatures au-delà de leur période de validité technologique.

Autorité de Validation (AV) : désigne l'autorité en charge de la validation des Signatures et Cachets au titre de la Politique de Validation.

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.

Cachet Électronique : désigne le procédé permettant de garantir l'intégrité d'un Document scellé et d'identifier l'origine de ce Document au moyen du Certificat utilisé pour son scellement.

Certificat Électronique ou Certificat : désigne un Document Électronique délivré par l'Autorité de Certification comportant l'identité du titulaire du Certificat et une clé cryptographique dite publique, utilisée, lors de la vérification de Signature ou du Cachet Électronique, pour contrôler que le Signataire ou l'émetteur est bien le titulaire du Certificat.

Certificat qualifié : désigne un Certificat répondant aux exigences de l'article 28 ou 38 du Règlement Européen n°910/2014 du 23 juillet 2014.

Client : désigne une personne physique ou morale (i) ayant souscrit aux Conditions Générales de Vente – Saas, ou (ii) ayant signé un accord commercial séparé avec Universign.

Compte d'Utilisateur ou Compte : désigne les ressources informatiques attribuées à l'Utilisateur par Universign et qui lui permettent d'accéder au Service.

Conditions Générales d'Utilisation (CGU) : désigne les conditions générales d'utilisation applicables à l'ensemble des Services fournis par Universign. Elles sont disponibles sur le Site Internet.

Conditions Spécifiques d'Utilisation (CSU) : désigne les conditions spécifiques d'utilisation du Service qu'elles encadrent. Elles sont disponibles sur le Site Internet.

Conservation : désigne le service associé consistant en la mise en œuvre de procédures et de technologies permettant d'étendre la fiabilité des Signatures Électroniques ou Cachet Électronique pendant une période déterminée.

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.

Document Électronique ou Document : désigne l'ensemble de données structurées pouvant faire l'objet de traitement informatique par le Service.

Documentation : désigne la documentation fonctionnelle et technique fournie par Universign dans le cadre de l'utilisation des Services.

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 Politique de Certification.

Horodatage : désigne un procédé permettant d'attester, au moyen de Contremarques de Temps, qu'un Document a existé à un moment donné.

Personnes Autorisées : 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 du Porteur.

Personne Tierce : désigne toute personne, physique ou morale, souhaitant, pour ses propres besoins, se baser sur un Certificat ou une Contremarque de Temps émis par une Autorité de Certification ou vérifier la validité de ces Certificats ou Contremarques de Temps.

Plateforme : désigne l'infrastructure technique composée de l'ensemble des matériels, progiciels, système d'exploitation, base de données et environnement gérés par Universign ou ses sous-traitants sur laquelle sera effectuée l'exploitation du Progiciel. Elle permet la fourniture de Service en mode SaaS. Elle est directement accessible à distance via le réseau Internet directement sur le Site Internet ou au moyen d'un smartphone ou d'une tablette tactile.

Politique de Certification (PC) : désigne l'ensemble de règles, identifié par un numéro (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations.

Politique de Préservation (PP) : désigne l'ensemble des règles auxquelles l'AP se conforme pour la mise en œuvre du Service de Conservation.

Politique de Validation (PV) : désigne l'ensemble des règles auxquelles l'AV se conforme pour la mise en œuvre du Service de validation de Signature et de Cachet.

Politique d'Horodatage ou PH désigne l'ensemble des règles auxquelles l'AH se conforme pour la mise en œuvre du Service d'horodatage

Porteur : désigne la personne, physique ou morale, identifiée dans le Certificat ayant sous son contrôle la clé privée correspondant à la clé publique.

Rapport de Validation : désigne le document qui est émis par Universign suite à l'analyse de la Signature ou du Cachet d'un document signé ou cacheté.

Règlement eIDAS : désigne le règlement n° 910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS »

SaaS (Software as a Service) : désigne le mode d'accès au Service. Cet accès est réalisé à distance via le réseau Internet par une connexion à la Plateforme mutualisée et hébergée sur les serveurs d'Universign et de ses sous-traitants.

Scellement Électronique ou Scellement : désigne un procédé permettant de garantir l'intégrité du Document scellé et d'identifier l'origine de ce Document au moyen du Certificat utilisé pour son scellement.

Service(s) : désigne e ou les service(s) de Signature Électronique, de cachet électronique ou d'horodatage, ainsi que les services associés qu'Universign s'engage à fournir à l'Utilisateur en mode SaaS.

Signataire : désigne la personne physique souhaitant conclure ou ayant conclu une Transaction avec le Client au moyen du Service.

Signature Électronique ou Signature : désigne un procédé permettant de garantir l'intégrité du Document signé et de manifester le consentement du Signataire qu'il identifie.

Site Internet : désigne le site Internet www.universign.com

Stockage : désigne le service associé au Service de Signature Électronique Universign consistant en la possibilité de stocker sur la Plateforme les Documents signés au moyen du Service.

Transaction : désigne le processus entre le Client pouvant intégrer un tiers au cours duquel est signé ou horodaté un Document Électronique proposé par le Client au moyen du Service.

Utilisateur : désigne un utilisateur des Services qui peut être selon les cas un Client, ses collaborateurs ou sous-traitants ainsi qu'un tiers Signataire amené à utiliser les Services dans le cadre de leur mise à disposition par un Client.

ARTICLE 1 – OBJET

Les présentes Conditions d'Utilisation Spécifiques associées aux Conditions Générales d'Utilisation définissent les conditions applicables aux Services.

ARTICLE 2 – DOCUMENTS CONTRACTUELS

Les CSU forment un tout indivisible avec les CGU. Elles prévalent en toute hypothèse sur les éventuelles conditions générales d'achat du Client.

Universign se réserve le droit de modifier les présentes CSU à tout moment et sans préavis.

Les CSU applicables ainsi que les versions antérieures sont accessibles en permanence sur le Site Internet, et ce dans un format permettant leur impression et/ou téléchargement par l'Utilisateur.

ARTICLE 3 – 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.

3.1. 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'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.

3.2. Utilisation du Service

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

3.3. Description du Service

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.

3.4. 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 de Temps.

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

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

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.

3.5. Obligation de l'Utilisateur

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

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 Internet.

En dehors des cas prévus par la Politique d'Horodatage, les Contremarques de Temps peuvent être vérifiée pendant cinq (5) 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.

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

3.6. Conservation des Données

Conformément à la Politique d'Horodatage et à la réglementation applicable, Universign conserve les journaux d'évènements relatifs au fonctionnement du Service pendant une durée de six (6) ans.

3.7. Politiques et normes

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

1.3.6.1.4.1.15819.5.1.1	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 Internet. Elles sont auditées par un organisme accrédité.

ARTICLE 4 – SERVICE 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.

4.1. – 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 ;
- D'un Certificat de personne morale associé à des clés cryptographiques conformes à l'une des Politique de Certification mentionnée aux présentes.

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.

4.2. – 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.

4.3. – 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 Electronique au sens de la réglementation européenne.

4.4. Catégories de cachet Électroniques

4.4.1. 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.

4.4.2 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.

4.5. 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.

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

4.6. – 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.

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

4.7. Conservation des Données

Universign conserve les journaux d'évènements relatifs au fonctionnement du Service pendant une durée de quinze (15) ans à compter de la date du scellement.

4.8. 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-l
1.3.6.1.4.1.15819.7.1.3	ETSI EN 319-411	Déclaration des PC de l'Autorité de Certification
1.3.6.1.4.1.15819.5.1.3.7	ETSI EN 319 411-2	PC pour les certificats de personnes morales, niveau QCP-l-QSCD

Ces politiques sont publiées sur le Site Internet. Elles sont auditées par un organisme accrédité.

ARTICLE 5 – SERVICE DE CLES CRYPTOGRAPHIQUES

5.1. – Accès au service

L'accès au Service nécessite de disposer :

- 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.

5.2. – Utilisation du Service

Pour la création de Signature Electronique, 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.

5.3. – 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.

5.4. – 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.

5.5. – 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.

5.6. – Responsabilités

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

5.7. – 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.

5.8. – 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 Internet.

ARTICLE 6 – 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.

6.1. Dispositions applicables au Signataire

6.1.1. 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).

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

6.1.2. 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.

6.1.3. Description 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.

6.1.4. 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 signature et la signature pour ordre sont prohibées.

6.2. Dispositions applicables au Client

6.2.1. Accès au Service

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

6.2.2. Description 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.

6.2.3. 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'entrainer l'inopposabilité de la Signature Électronique et/ou la nullité de l'acte sur lequel elle est apposée.

6.3. Niveaux de Signature Électroniques

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.

6.3.1. Signature Electronique de niveau 1

Dans le cadre de la mise en œuvre de la Signature de niveau 1, Universign ne peut garantir l'identité du Signataire ou ses habilitations. 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.

6.3.2. Signature Electronique 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.

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.

6.3.3. Signature Electronique 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.

6.4. 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.

6.5. Stockage des documents

Sauf avis contraire du Client, Universign stocke 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 sous-traitant spécialisé.

Dans le cas où le Stockage est réalisé par Universign et sauf accord contraire entre Universign et le Client, les Documents sont stockés à compter de leur dépôt jusqu'à la survenance de l'un des évènements ci-après :

- Quinze (15) ans après la date de dépôt du Document ;
- La clôture du Compte d'Utilisateur ;
- Deux (2) mois après la fin d'un Contrat sauf si une période de réversibilité le prolonge.

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.

6.6 Obligations des Utilisateurs

6.6.1. Obligation 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 porte 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.

6.6.2. – 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, etc.) ;
- Assurer la confidentialité de son Identifiant et du ou des code(s) confidentiel(s) qui lui sont adressés.

6.7. Limite de Responsabilités

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.

6.8. Politiques et normes

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

1.3.6.1.4.1.15819.5.1.3.3	ETSI EN 319 411-1	PC pour les certificats de personnes physiques niveau LCP
1.3.6.1.4.1.15819.5.1.3.1	ETSI EN 319-411-2	PC pour les certificats de personnes physiques, niveau QCP-n
1.3.6.1.4.1.15819.5.1.3.8	ETSI EN 319-411-2	PC pour les certificats de personne physiques niveau QCP-n où l'identité a été vérifiée à l'aide d'un PVID

1.3.6.1.4.1.15819.5.1.3.9	E T S I E N 3 1 9 - 4 1 1 - 2	PC pour les certificats de personne physiques niveau QCP-n-QSCD où l'identité a été vérifiée à l'aide d'un PVID
1.3.6.1.4.1.15819.7.1.3	ETSI EN 319-411	Déclaration des PC de l'Autorité de Certification
1.3.6.1.4.1.15819.5.1.3.6	E T S I E N 3 1 9 - 4 1 1 - 2	PC pour les certificats de personnes physiques, niveau QCP-n-QSCD

Ces politiques sont publiées sur le Site de publication. Elles sont auditées par un organisme accrédité.

6.9 Fichier de preuve

Pour les signatures, Universign fournira aux Utilisateurs les Données extraites de ses journaux d'évènements participant à établir la preuve des opérations constitutives d'une Signature Électronique, sous réserve de la production de l'un ou l'autre des éléments justificatifs adéquats.

Ces Données seront transmises sous la forme d'un fichier attestant de l'authenticité de ces Données et scellé au moyen d'un Certificat Électronique au nom d'Universign.

La demande d'accès à ses Données sera formalisée selon les conditions prévues en Annexe « Conditions d'accès au fichier de preuve » du Contrat.

Ledit fichier sera transmis dans les meilleurs délais, à compter de la réception du justificatif idoine.

Après la résiliation ou l'expiration du présent Contrat et ce, quels qu'en soient les motifs, les Fichiers de Preuve judiciaire seront stockés pendant une durée de 15 ans à compter de la date de la Transaction objet du (i) litige, (ii) du contrôle ou de (iii) la réquisition judiciaire.

Article 7 – SERVICE DE CONSERVATION

Le Service de Conservation permet d'étendre la fiabilité des Documents ayant fait l'objet d'une Signature Électronique ou d'un Cachet Électronique au-delà de leur période de validité technologique et ce, conformément à la Politique de Préservation qui décrit plus précisément la mise en œuvre et l'organisation du Service.

7.1. Accès au Service

L'accès au Service est une option intégrée au service de Signature Electronique fourni par Universign.

Il nécessite de disposer d'un équipement informatique adapté pour accéder au Service et :
- d'un Compte d'Utilisateur ou ;
- d'un compte attribué par un Client dans le cadre de son organisation lorsque le Service est utilisé via les API.

Le Service est fourni par défaut à l'ensemble des Clients Stockant les Documents signés électroniquement avec une solution Universign.

Il peut être désactivé à la demande du Client.

7.2. Utilisation du Service

Lorsque les Documents signés électroniquement sont stockés chez Universign, cette dernière effectue via sa solution un traitement permettant la fiabilité des Signatures qu'ils contiennent au-delà de leur période de validité technologique.

Le Service intègre alors dans le Document signé électroniquement l'ensemble des éléments décrits dans la Politique de Préservation.

7.3. Limites d'Utilisation

Le Service ne constitue pas un service d'archivage électronique notamment au regard de la norme NF Z42-013.

7.4. Garanties et limites de garanties

Universign garantit en outre la fourniture d'un Service conforme à la Politique de Préservation.

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 Services ainsi que les dispositions de la Politique de Préservation répondent à ses exigences propres.

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

7.5. Stockage des Documents

Il appartient à l'Utilisateur de prendre toute disposition de manière à stocker les Documents ayant fait l'objet d'une Conservation, ces Documents ne faisant pas l'objet s'un stockage par le Service.

7.6. Conservation des Données

Universign conserve les journaux d'évènements relatifs au fonctionnement du Service de Conservation pendant une durée de quinze (15) ans.

7.7. Limite de Responsabilités

Universign ne contrôle pas le contenu des Documents traités dans le cadre des Services, aussi sa responsabilité ne saurait donc être engagée relativement à la valeur et/ou la validité du contenu desdits Documents ou le défaut de ces derniers.

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 dont la fiabilité a été étendue au-delà de la période de validité technologique.

7.8. Politiques et normes

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

1.3.6.1.4.1.15819.5.8.1	ETSI TS 119 511	PP pour la préservation par extension des documents signés
1.3.6.1.4.1.15819.7.4.1	ETSI TS 119 511	DPP pour la préservation par extension des documents signés
1.3.6.1.4.1.15819.5.8.2		Profil de Préservation
1.3.6.1.4.1.15819.5.8.3		Politiques des Preuves de Préservation

Ces politiques sont publiées sur le Site de publication. Elles sont auditées par un organisme accrédité.

Article 8 – SERVICES DE VALIDATION DE SIGNATURE ET CACHET ELECTRONIQUE

Le Service de validation de Signature et Cachet permet à un Utilisateur de valider une Signature ou un Cachet opéré antérieurement.

8.1. Accès au Service

L'Utilisateur 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 Compte d'Utilisateur Universign.

8.2. Description du Service

Le processus de validation d'une Signature dans un Document signé ou d'un Cachet dans un Document cacheté repose sur les étapes suivantes :

Etape 1 : Import du Document signé ou cacheté

L'Utilisateur via son Compte d'Utilisateur, importe un Document déjà signé ou cacheté afin d'en vérifier leur validité.

Etape 2 : Vérification du Document signé ou cacheté

Pour chaque Signature ou Cachet contenu dans un document signé ou cacheté, le Service vérifie que :
-Le Certificat sur lequel repose la signature était, au moment de la Signature, un Certificat conforme aux dispositions du Règlement eIDAS;
- Le Certificat utilisé a été délivré par un prestataire de services de confiance qualifié et était valide au moment de la Signature ou du Scellement ;
- Les données de validation de la Signature ou du Cachet correspondent aux données communiquées à l'Utilisateur ;
- L'ensemble unique de données représentant le signataire dans le Certificat est correctement fourni à l'Utilisateur ;
- La Signature ou le Cachet, s'ils sont qualifiés, ont été créés par un dispositif de création de Signature ou de Cachet Electronique qualifié ;
-L'intégrité des données signées ou scellées n'a pas été compromise ;

Etape 3 : Emission et envoi du Rapport de Validation

À la suite de l'analyse d'un Document signé ou cacheté, Universign procède à l'émission d'un Rapport de Validation qui est ensuite mis à disposition de l'Utilisateur via l'API une seule fois.

8.3. Garanties et limites de garanties

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

Universign garantit en outre la fourniture d'un Service conforme à la Politique de Validation.

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 Validation répondent à ses exigences propres.

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

8.4. Stockage des Rapports de validation

Universign stocke de manière à en préserver l'intégrité, uniquement les Rapports de Validation générés au moyen du Service.

Les Documents cachetés ou signés importés pour les besoins du Services sont supprimés des serveurs une fois l'étape d'analyse de l'élément complété.

Universign se réserve le droit de stocker les Rapports de Validation signés auprès d'un sous-traitant spécialisé.

Les Rapports de Validation et les journaux d'évènements sont stockés pendant sept (7) ans à compter de leur émission conformément à la réglementation applicable.

Toutefois, il est précisé qu'il appartient à l'Utilisateur de prendre toute disposition de manière à conserver le Rapport de Validation qui lui est transmis après l'analyse, ce dernier ne pouvant plus être communiqué ultérieurement par Universign.

8.5. Obligations des Utilisateurs

L'Utilisateur s'engage également à vérifier que le Document signé ou cacheté soumis à validation dans le cadre du Service est bien celui transmis à Universign.

Le Service ne réalise aucun archivage des Documents signés ou cachetés soumis à validation, ce dernier restant de la responsabilité des Utilisateurs.

8.6. Limite de Responsabilités

Universign ne contrôle pas le contenu des Documents signés ou cachetés soumis à validation dans le cadre du Service, 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.

Universign ne peut être tenue pour responsable d'un usage inapproprié du Service.

8.7. Politiques et normes

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

1.3.6.1.4.1.15819.5.7.1	ETSI TS 119 441	Service de validation
	ETSI EN 319 102-1	Algorithme de validation
	ETSI TS 119 102-2	Format du rapport de validation
1.3.6.1.4.1.15819.7.3.1	ETSI TS 119 441	DPV Service de Validation de signature
1.3.6.1.4.1.15819.5.7.2.1		PV pour les signatures et cachets qualifiés
1.3.6.1.4.1.15819.5.7.2.2		PV pour tout type de signatures ou cachets (qualifiés ou non)

Ces politiques sont publiées sur le Site Internet. Elles sont auditées par un organisme accrédité.

8.8. Rapport de validation

Après l'analyse du Document signé ou cacheté que l'Utilisateur a souhaité valider dans le cadre du Service, un Rapport de Validation est émis par Universign.
Il contient pour chaque Signature / Cachet présent dans le Document, les informations ci-après :

- le statut global de la validation de chaque Signature / Cachet ;
- l'identifiant de la Signature / Cachet (sous la forme d'un hash) ;
- les contraintes appliquées pendant la validation avec un statut (indiquant le succès de la vérification effectuée ou l'éventuelle erreur rencontrée) ;
- la date et heure de la validation.

Le Rapport de Validation sera transmis sous la forme d'un fichier attestant de l'authenticité des données qu'il contient et scellé au moyen d'un Certificat Électronique au nom d'Universign.

ANNEXE 1 : CONDITIONS D'ACCES AU FICHIER DE PREUVE

1. NOTIONS

1.1. Fichier de preuve d'une transaction

Les éléments collectés par Universign lors d'une Transaction réalisée au moyen du service de Signature électronique sont consignés dans un fichier dit « fichier de preuve ».

Ces éléments participent à démontrer la fiabilité du processus de signature du document objet de la Transaction.

Le fichier de preuve contient notamment les données nominatives relatives au(x) Signataire(s) et créateur de Collecte, l'empreinte numérique des documents signés, l'adresse électronique des Signataires, l'adresse électronique du créateur de Collecte, les numéros de téléphone sur lesquels des codes confidentiels permettant l'authentification ont été adressés, ainsi que les adresses de connexion (IP) des Signataires (i.e. : adresses IP des terminaux à partir desquelles le signataire a accédé au document).

Le fichier de preuve est scellé au moyen d'un cachet électronique dont le certificat a été émis au nom d'*Universign Evidence Service*. Il est horodaté électroniquement dans un délai bref à compter de la Transaction, puis conservé de manière à en garantir l'intégrité.

Avec la transmission de ce fichier, Universign atteste de la réalisation des opérations relatives à la Signature qui y sont consignées.

1.2. Origine des données du fichier de preuve

Le fichier de preuve est constitué de données collectées directement et indirectement auprès des Signataires.

Les données collectées de manière indirecte ont pour origine le créateur de la collecte de signature.

Les autres données sont collectées par Universign directement auprès du Signataire. La preuve des connexions, des enregistrements informatiques et d'autres éléments d'Identification (tel que le numéro de téléphone utilisé pour l'authentification du signataire) est établie autant que de besoin à l'appui des journaux de connexion tenus par Universign.

1.3. Données de connexion

Ces données sont générées ou traitées par le Service Universign lors de la mise en œuvre du procédé de Signature. Les données de connexion ont pour caractéristiques d'être intrinsèquement liées à la Transaction mais n'en constitue pas le contenu. Il s'agit de données purement descriptives qui contiennent les éléments techniques nécessaires au bon fonctionnement du service de Signature.

Ces données sont également soumises à la règlementation relative à la protection des données personnelles.

1.4. Preuve

Le fichier de preuve participe à démontrer l'existence d'un acte juridique.

D'une part, l'acte juridique se prouve par un écrit qui, s'il est établi sur un support électronique, doit permettre d'identifier la personne dont il émane et être établi et conservé dans des conditions de nature à en garantir l'intégrité.

D'autre part, en ce qui concerne l'acte sous seing privé, la seule obligation formelle à laquelle il est soumis est sa signature par les parties.

Dès lors, le fichier de preuve d'une Transaction tel qu'il est prévu par Universign apporte des éléments concourants à la preuve :

- De l'acte juridique ;
- De l'obligation formelle qu'est la signature électronique d'un acte auquel elle se rapporte.

2. CONDITIONS D'ACCES AU FICHIER DE PREUVE

2.1. Evènements permettant l'accès au fichier de preuve

✓ **Litige**

Le litige ouvrant droit à un accès au fichier de preuve est un différend, qui implique une ou plusieurs des parties à la Transaction ou Parties Utilisatrices. Il a nécessairement pour objet la validité de l'acte juridique du seul point de vue formel.

La survenance d'un litige est nécessairement antérieure à l'engagement d'une procédure judiciaire.
Le litige couvre, notamment, le règlement amiable du différend, la médiation et la conciliation qu'ils soient conventionnels ou judicaires.

✓ **Procédure judiciaire**

Dans le cadre d'une procédure judiciaire, une action a été engagée par l'une ou l'autre des parties à la Transaction ou par une Personne Tierce devant une juridiction compétente pour connaître du conflit qui les oppose.

✓ **Demande ou contrôle d'une autorité administrative**

Une demande impérative émanant d'une autorité de tutelle ou de contrôle ouvre le droit d'accès au(x) fichier(s) de preuve sans que soit nécessaire l'information préalable des Signataires concernées par la Transaction ou les Transactions contrôlées.

✓ **Réquisition judiciaire**

Certaines autorités publiques sont légalement autorisées à se faire communiquer, sous certaines conditions et dans le cadre de leurs missions particulières, des informations issues du fichier de preuve détenu par Universign sans information préalable d'aucune des personnes concernées par la Transaction.

2.2. Personnes autorisées à accéder au fichier de preuve

Les Personnes autorisées à accéder aux fichiers de preuve diffèrent selon l'évènement ouvrant droit à cet accès.

✓ <u>En cas de litige ou de procédure judiciaire :</u>
- Le ou les utilisateur(s) Signataire(s) ;
- Le ou les utilisateur(s) collecteur(s) ;
- La ou les Partie(s) Utilisatrice(s).

✓ <u>Dans le cadre d'une demande impérative émanant d'une autorité de tutelle ou de contrôle :</u>
- L'autorité habilitée ;
- Le ou les utilisateur(s) collecteur(s) ;
- La ou les Partie(s) Utilisatrices.

✓ <u>Dans la cadre d'un audit interne du Client :</u>
- Le ou les utilisateur(s) collecteur(s).

✓ <u>Dans le cadre de réquisition judicaire :</u>
- L'autorité habilitée :
- Le procureur de la République ;
- Le juge d'instruction ;
- L'officier de police judiciaire autorisé par le Procureur de la République.

2.3. Demande d'accès au fichier de preuve

La demande d'accès au fichier de preuve doit être adressée à Universign par la Personne autorisée. Elle est écrite et signée par la Personne autorisée.

Universign exige du demandeur qu'il complète et adresse un formulaire spécifique de demande d'accès au fichier de preuve. Un exemplaire original du formulaire doit être transmis à Universign par courrier postal.

Lorsque la demande émane d'une autorité publique, le demandeur justifie de ses habilitations.

La demande mentionne le motif de l'accès : litige, contrôle administratif, procédure ou réquisition judiciaires. Elle est en accompagnée du justificatif idoine dont la liste figure dans le formulaire de demande d'accès au fichier de preuve.

2.4. Durée

Le fichier de preuve sera transmis dans un délai de trois (3) jours ouvrés, à compter de la réception du justificatif idoine. La demande d'accès au fichier de preuve est possible pendant quinze (15) ans à compter de la date de la Transaction objet de la demande d'accès au fichier de preuve. A l'issue de ce délai, les fichiers de preuve sont automatiquement supprimés.