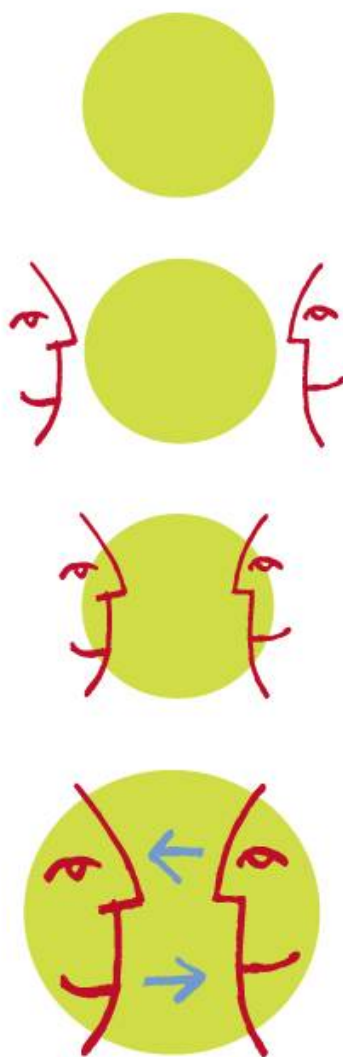


# La Politique de Gestion des Preuves « K.WEBSIGN<sup>®</sup> »

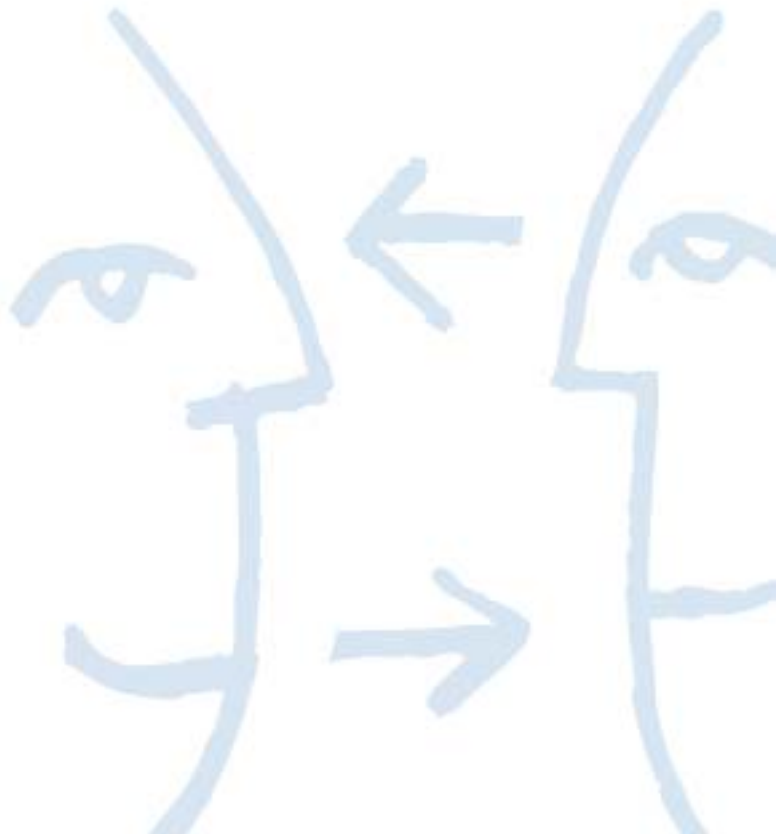


**KEYNECTIS**

[www.keynectis.com](http://www.keynectis.com)

## SOMMAIRE

1	QUEL EST LE ROLE DE LA POLITIQUE DE GESTION DES PREUVES ? _____	3
2	COMMENT FONCTIONNE LE SERVICE K.WEBSIGN® ? _____	3
3	QUELS SONT LES USAGES ET APPLICATIONS CONCERNES PAR LA POLITIQUE DE GESTION DES PREUVES « K.WEBSIGN® » ? _____	4
4	QU'EST-CE QU'UN FICHER DE PREUVE ? _____	4
5	QUELLE EST LA VALEUR JURIDIQUE DES ECRITS SUR SUPPORT ELECTRONIQUE SIGNES ? ___	5



## 1 QUEL EST LE ROLE DE LA POLITIQUE DE GESTION DES PREUVES ?

La Politique de Gestion des Preuves associée au Service K.Websign<sup>®</sup>, ci-après dénommée « PGP K.Websign<sup>®</sup> », de la société KEYNECTIS a pour objet de décrire les règles suivies pour constituer et conserver les preuves relatives aux échanges électroniques réalisés entre plusieurs parties, afin d'être en mesure de démontrer la réalité et l'intégrité des échanges de données électroniques intervenus entre ces parties.

La PGP K.Websign<sup>®</sup> formalise et énonce ainsi les modalités techniques de la constitution et de la gestion dans le temps de la preuve d'un écrit sur support électronique (contrat, souscription d'abonnement, bon de commande ou tout autre type de document sous forme électronique) sur lequel a été apposé une signature électronique au moyen d'un certificat électronique, et ce uniquement dans le cadre du service K.Websign<sup>®</sup> proposé par KEYNECTIS pour le compte de ses clients (ci-après « Organisme client »).

En fonction du domaine d'activité de l'Organisme client, du type de document sous forme électronique qu'il souhaite échanger et signer avec ses propres clients, partenaires ou toute autre personne (ci-après « les Utilisateurs »), ainsi que de ses besoins de preuve spécifiques, l'Organisme client devra compléter la PGP K.Websign<sup>®</sup> par un document propre à ses besoins, ses procédures et spécificités techniques et fonctionnelles de son application informatique utilisant le Service K.Websign<sup>®</sup>.

Il est à cet égard précisé que KEYNECTIS au travers de son service K.Websign<sup>®</sup> n'intervient pas sur le contenu des échanges de données sous forme électronique signées entre l'Organisme Client et les Utilisateurs.

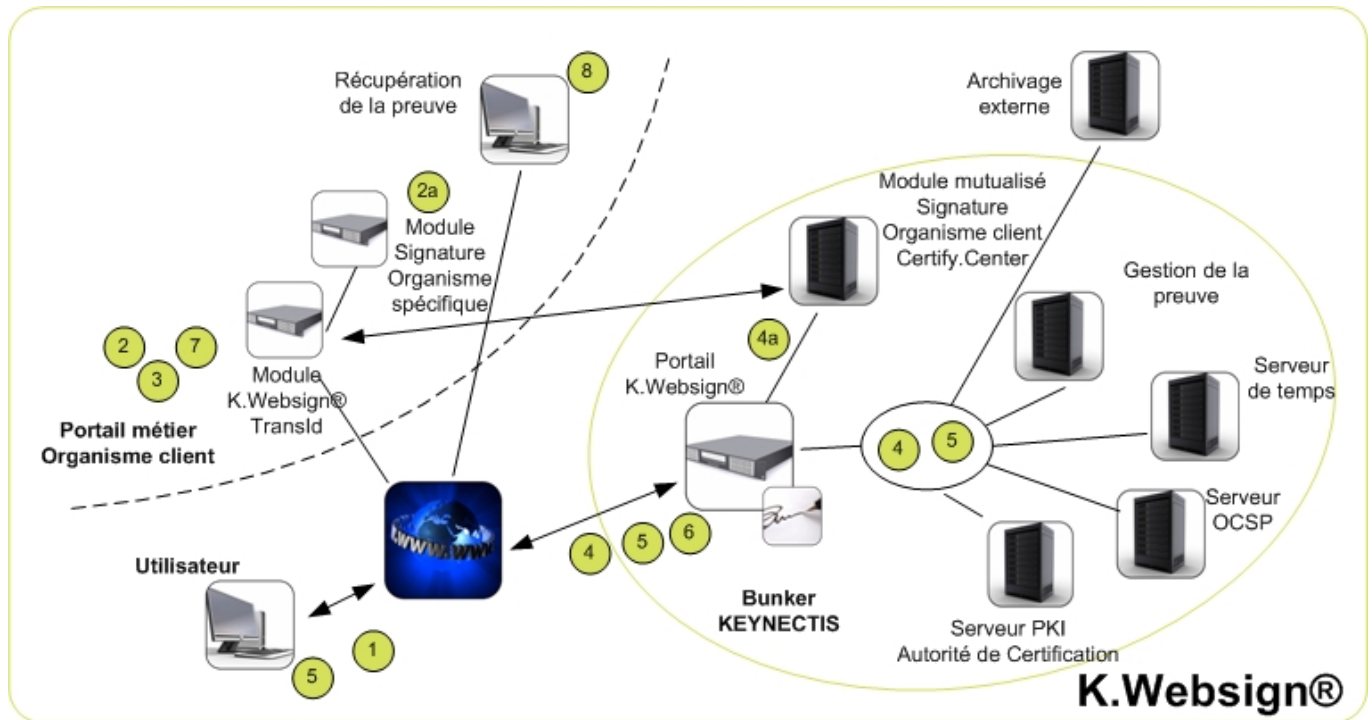
## 2 COMMENT FONCTIONNE LE SERVICE K.WEBSIGN<sup>®</sup> ?

Le Service K.Websign<sup>®</sup> de KEYNECTIS repose notamment sur les éléments suivants :

- mise à disposition le cas échéant d'un Service de certification électronique ayant pour objet l'émission (i) de Certificats à usage unique et d'une durée limitée pour signature de documents sous forme électronique entre l'Organisme Client et ses propres clients/partenaires/fournisseurs ou toutes autres personnes en relation avec l'Organisme Client (ci-après « Utilisateur »), (ii) du Certificat de l'Organisme client pour signature des données électroniques présentées à l'Utilisateur et (iii) des Certificats (chiffrement, intégrité) associés au transport des données électroniques entre le site web de l'Organisme client et la Plateforme K.Websign<sup>®</sup>;
- mise à disposition de l'Organisme client d'une Application logicielle (ci-après « Application K.Websign<sup>®</sup> ») dont l'objet est (i) de permettre à l'Organisme client de proposer à ses Utilisateurs un service de conclusion en ligne de contrat ou de validation de tout autre document sous forme électronique au moyen d'une Signature électronique (ci-après « Transaction électronique ») associée à un certificat (clé privée) à usage unique d'une durée limitée émis pour chaque Transaction et (ii) de constituer un Fichier de preuve non modifiable et horodaté contenant la trace du déroulement et des contrôles relatifs à la Transaction réalisée en ligne ;
- mise à disposition d'un Service d'Archivage pour conservation du Fichier de preuve créé par l'Application K.Websign<sup>®</sup>.

A compter de la version 2 de la Plateforme K.Websign, la fonctionnalité additionnelle de signature électronique embarquée dans un document sous format PDF permettant d'intégrer dans le document la signature électronique des signataires peut être utilisée dans le cadre du Service K.Websign. Dans ce cas, les Certificats de signature utilisés sont émis par l'Autorité de certification de KEYNECTIS ayant été référencée par Adobe<sup>®</sup>. Il est précisé que cette fonctionnalité additionnelle de signature électronique embarquée dans un document sous format PDF est associée à un service de validation OSCP du certificat signataire et à un service d'horodatage de la signature lors de la signature du document.

## Processus de la constitution de la preuve



### 3 QUELS SONT LES USAGES ET APPLICATIONS CONCERNES PAR LA POLITIQUE DE GESTION DES PREUVES « K.WEBSIGN® » ?

L'Organisme client peut utiliser le service K.Websign® pour toutes applications métier ou pour tout type de document sous forme électronique de son choix.

Il formalise et communique à KEYNECTIS les spécificités techniques et fonctionnelles propres à son application métier utilisant le Service K.Websign®.

Il détermine notamment à cet égard les procédures d'identification des Utilisateurs lors de la génération du Certificat électronique applicable à ses applications métiers utilisant le Service K.Websign®.

KEYNECTIS intervient lors de la création technique du fichier de preuve associé à la transaction électronique réalisée entre l'Organisme client et l'Utilisateur pour ainsi permettre à chacune des parties de conserver les éléments relatifs à cette transaction (informations signées, horodatées et archivées).

Il est précisé que le Certificat électronique associé à la signature électronique apposée sur l'acte validé et accepté par le Client et l'Utilisateur est conforme à la norme technique applicable en matière de certification électronique mais ne répond pas à l'ensemble des exigences d'un certificat qualifié telles prévues par le Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique. En conséquence, la présomption légale de fiabilité du procédé de signature électronique prévue par le Code civil n'est pas applicable.

### 4 QU'EST-CE QU'UN FICHIER DE PREUVE ?

Un fichier de preuve désigne l'ensemble des éléments créés lors de la réalisation de la Transaction entre l'Organisme Client et l'Utilisateur, puis conservé pendant un délai conforme aux exigences légales ou indiqué par

l'Organisme Client, permettant ainsi d'assurer la traçabilité de la réalisation de la Transaction conclue conformément au Service K.Websign®.

## **5 QUELLE EST LA VALEUR JURIDIQUE DES ECRITS SUR SUPPORT ELECTRONIQUE SIGNES ?**

S'adaptant à l'utilisation croissante d'Internet, le Code civil dans sa partie relative à la preuve des écrits, a été modifié par la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

Dorénavant, l'article 1316-1 du Code civil reconnaît que *"l'écrit sur support électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont l'écrit émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité"*.

D'autre part, l'article 1316-4 du Code civil reconnaît que la signature électronique a la même valeur juridique que la signature manuscrite, sous réserve que le procédé de signature électronique soit fiable.

Plus récemment, la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) complétée par l'ordonnance no 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique a encadré légalement les formalités de conclusion, de validité ou des effets de certains contrats en vue de permettre l'accomplissement de celles-ci par voie électronique.

En matière de preuve des écrits sur support électronique, le droit positif a mis en évidence l'importance de la traçabilité des échanges sous forme électronique, l'identification des signataires et le cas échéant leur acceptation préalable à l'utilisation de ces modes de communication et d'échanges de consentements ainsi que la fiabilité technique des procédés utilisés.

