



**KEYNECTIS**

## ▪ POLITIQUE DE GESTION DE PREUVES

**K**•Websign®

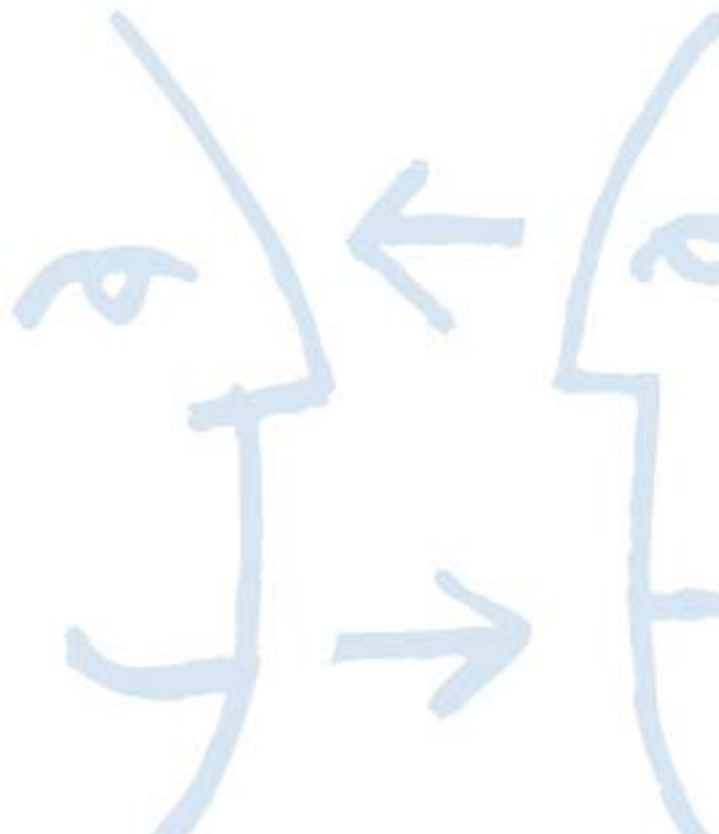
© 2006-2009 KEYNECTIS. Tous droits réservés.

<b>Date :</b>	30 Octobre 2009
<b>Référence :</b>	PGP/KEY/K.Websign
<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

## HISTORIQUE DES MODIFICATIONS

Historique du document :				
Date	Version	Rédacteur	Objet	Statut
01/12/2005	0.1	MQ	Rédaction	Projet
20/12/2005	0.2	MQ	Prise en compte des remarques DM/EM	Projet
20/12/2005	0.3	MQ	Document complété	Projet
20/12/2005	0.4	DM/EM	Document complété	Projet
20/01/2006	0.7	EM	Chapitre 3	Projet
25/01/2006	0.8	EM	Revue générale	Projet.
01/02/2006	0.9	DM	Relecture interne	Projet
27/02/2006	1.0	DM	Relectures externes	Diffusable
03/04/2006	1.1	MQ/DM	Document complété	Diffusable
12/10/2006	1.2	MQ	Document complété et actualisé	Projet
20/10/2006	1.3	MQ	Intégration remarques DM	Projet
23/10/2006	2	MQ	Mise en forme pour diffusion	Diffusable
05/03/2009	3	DM/MQ	Ajout de l'horodatage RFC3161, intégration remarques MQ et modification du siège social de KEYNECTIS	Diffusable
30/10/2009	4	DM/MQ/EM	Ajout de la fonctionnalité « Signature électronique embarquée » dans les documents format PDF	Diffusable





## SOMMAIRE

<b>AVERTISSEMENT</b>	<b>5</b>
<b>1 INTRODUCTION</b>	<b>6</b>
1.1 Présentation générale de la politique de gestion de preuves.....	6
1.2 Identification de la politique de gestion des preuves.....	6
1.3 Les entités de la constitution et de la gestion des preuves.....	6
1.3.1 L'Organisme client.....	7
1.3.2 L'Autorité de Certification.....	7
1.3.3 L'Utilisateur.....	7
1.3.4 Le fournisseur du Service K.Websign®.....	7
1.3.5 Le tiers horodateur : l'Autorité d'horodatage.....	7
1.3.6 Le tiers archiveur.....	7
1.4 Usages et applications concernés par la politique de gestion de preuves.....	8
1.5 Gestion de la politique de gestion de preuves.....	8
1.5.1 Entité gérant la Politique de gestion de preuve.....	8
1.5.2 Point de contact.....	8
1.6 Acronymes et définitions.....	8
1.6.1 Liste des acronymes.....	8
1.6.2 Définitions.....	9
<b>2 CONSTITUTION DES PREUVES</b>	<b>14</b>
2.1 Processus de la constitution de la preuve.....	14
2.2 Les obligations des acteurs de la constitution de la preuve.....	17
2.2.1 Les obligations de l'Organisme client.....	17
2.2.2 Les obligations de l'Utilisateur.....	18
2.2.3 Les obligations des Autorités de Certification.....	18
2.2.4 Les obligations du fournisseur de l'Application K.Websign®.....	18
2.2.5 Le tiers Horodateur / l'Autorité d'horodatage.....	18
2.2.6 Le tiers archiveur.....	18
2.3 Eléments constitutifs de la preuve : le Fichier de preuve.....	19
<b>3 GESTION DES ELEMENTS CONSTITUANT LE FICHER DE PREUVE</b>	<b>20</b>
3.1 Identification et authentification.....	20
3.2 Intégrité des éléments constituant le fichier de preuve.....	20
3.2.1 Données métier signées.....	20
3.2.2 Original.....	20
3.2.3 Accusé réception.....	20
3.2.4 Fichier de preuve.....	20
3.2.5 Intégrité des échanges, des procédures et identité des acteurs techniques.....	20
3.2.6 Lien entre « date de signature, identité utilisateur, identité Organisme client et document métier » ..	21
3.3 Disponibilité et consultation du Fichier de preuve.....	21
3.4 Lisibilité et pérennité.....	21
3.5 Cohérence temporelle.....	21
<b>4 UTILISATION DU FICHER DE PREUVE</b>	<b>22</b>
4.1 Restitution du Fichier de preuve.....	22
4.2 Visualisation du contenu du Fichier de preuve.....	22
4.3 Vérification de la signature du fichier de preuve (Intégrité).....	22
<b>5 MESURES DE SECURITE NON TECHNIQUES DES OPERATIONS</b>	<b>23</b>
5.1 Pour le Service de certification électronique.....	23
5.2 Pour le fournisseur de l'Application K.Websign®.....	23
5.2.1 Mesures de sécurité physique.....	23



5.2.1.1	Situation géographique.....	23
5.2.1.2	Accès physique.....	23
5.2.1.3	Energie et air conditionné.....	23
5.2.1.4	Exposition aux liquides.....	23
5.2.1.5	Prévention et protection incendie.....	23
5.2.1.6	Sauvegardes hors site.....	23
5.2.2	Mesures de sécurité procédurales.....	23
5.2.3	Procédures de constitution des données d'audit.....	24
5.2.3.1	Type d'événements enregistrés.....	24
5.2.3.2	Processus de journalisation.....	25
5.2.3.3	Procédures de sauvegardes des journaux d'événements.....	25
5.2.3.4	Evaluation des vulnérabilités.....	25
5.2.4	Archivage des données d'exploitation.....	25
<b>5.3</b>	<b>Pour l'Organisme client.....</b>	<b>25</b>
<b>5.4</b>	<b>Pour le tiers archiveur.....</b>	<b>25</b>
<b>5.5</b>	<b>Pour le tiers horodateur.....</b>	<b>25</b>
<b>6</b>	<b>MESURES DE SECURITE TECHNIQUES ET LOGIQUES.....</b>	<b>26</b>
<b>6.1</b>	<b>Pour le Service de certification électronique.....</b>	<b>26</b>
<b>6.2</b>	<b>Pour l'Utilisateur.....</b>	<b>26</b>
<b>6.3</b>	<b>Pour l'Organisme client.....</b>	<b>26</b>
<b>6.4</b>	<b>Pour le fournisseur de l'Application K.Websign.....</b>	<b>26</b>
6.4.1	Mesures de sécurité de l'outil de signature mis à disposition de l'Organisme client.....	27
6.4.2	Mesures de sécurité de l'outil de signature mis à disposition de l'Utilisateur.....	27
6.4.3	Mesures de sécurité des systèmes informatiques.....	27
6.4.4	Mesures de sécurité du système durant son cycle de vie.....	27
6.4.4.1	Mesures de sécurité liées au développement des systèmes.....	27
6.4.4.2	Gestion de la sécurité.....	27
6.4.5	Mesures de sécurité réseau.....	27
<b>6.5</b>	<b>Pour le tiers archiveur.....</b>	<b>28</b>
<b>6.6</b>	<b>Pour le tiers horodateur.....</b>	<b>28</b>
<b>7</b>	<b>AUDIT DE CONFORMITE ET AUTRES EVALUATIONS.....</b>	<b>29</b>
7.1	Fréquences et / ou circonstances des évaluations.....	29
7.2	Identités / qualifications des évaluateurs.....	29
7.3	Relations entre évaluateurs et entités évaluées.....	29
7.4	Sujets couverts par les évaluations.....	29
7.5	Actions prises suite aux conclusions des évaluations.....	29
7.6	Communication des résultats.....	29
<b>8</b>	<b>DISPOSITIONS DE PORTEE GENERALE.....</b>	<b>30</b>
<b>8.1</b>	<b>Barèmes des prix.....</b>	<b>30</b>
<b>8.2</b>	<b>Responsabilité financière.....</b>	<b>30</b>
<b>8.3</b>	<b>Loi applicable et juridictions compétentes.....</b>	<b>30</b>
<b>8.4</b>	<b>Droits de propriété intellectuelle.....</b>	<b>30</b>
<b>8.5</b>	<b>Protection des données à caractère personnel.....</b>	<b>30</b>
<b>8.6</b>	<b>Durée et fin anticipée de validité de la politique de gestion des preuves.....</b>	<b>30</b>
8.6.1	Durée de validité.....	30
8.6.2	Effets de la fin de validité et clauses restant applicables.....	30
<b>8.7</b>	<b>Administration de la politique de gestion des preuves.....</b>	<b>30</b>
8.7.1	Délai de préavis.....	31
8.7.2	Forme de diffusion des avis.....	31
8.7.3	Modifications nécessitant l'adoption d'une nouvelle politique.....	31
<b>8.8</b>	<b>Limite de responsabilité.....</b>	<b>31</b>

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

## AVERTISSEMENT

La présente politique de gestion de preuves est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de KEYNECTIS.

La reproduction, la représentation (hormis la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement de manière expresse par KEYNECTIS ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'Article L.122-5, d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (Article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les Articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

L'utilisation de la présente politique de gestion de preuves peut être concédée par des accords de licence à toutes entités privées ou publiques qui souhaiteraient l'utiliser dans le cadre de leurs propres services de gestion de preuves.



 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

## 1 INTRODUCTION

### 1.1 Présentation générale de la politique de gestion de preuves

Ce document constitue la politique de gestion de preuves associée au Service K.Websign® de la société KEYNECTIS, utilisé par ses clients (ci-après « Organisme client »).

L'objet de la présente politique de gestion des preuves est de décrire les règles suivies et les procédés utilisés par KEYNECTIS pour constituer et conserver les preuves relatives aux échanges électroniques réalisés entre plusieurs parties (dont l'organisme client), afin d'être en mesure de démontrer ultérieurement l'existence et l'intégrité des échanges de données électroniques intervenus entre ces parties.

Le Service K.Websign® 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 le cas échéant de(s) certificats de l'Organisme client (Signature de certification) mis en œuvre pour création de la signature incluse dans le document PDF 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® ;
- mise à disposition de l'Organisme client d'une Application logicielle (ci-après « Application K.Websign® ») 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®.

En fonction de l'application métier, du type de document sous forme électronique devant être signé et de ses besoins de preuve spécifiques, l'Organisme client devra compléter cette présente politique de gestion de preuves par un document propre à son application métier utilisant le Service K.Websign®.

L'Organisme client formalisera et communiquera à KEYNECTIS les spécificités techniques et fonctionnelles propres à son application métier utilisant le Service K.Websign® (choix du Protocole de consentement, nom de l'application métier, de l'AC...).

Il est à cet égard précisé que KEYNECTIS dans le cadre de la réalisation de ses prestations de service K.Websign® n'intervient pas sur le contenu des données, leur format et/ou sur le choix du type de document sous forme électronique signé entre l'Organisme Client et les Utilisateurs.

### 1.2 Identification de la politique de gestion des preuves

La présente politique de gestion de preuves est identifiée par l'OID 1.3.6.1.4.1.22234.2.4.6.1.4. Le numéro d'OID de cette PGP est indiqué à titre de gestion documentaire pour la société KEYNECTIS.

La politique de gestion des preuves correspondant à l'OID ci-dessus indiqué est ci-après désignée sous le nom de « PGP K.Websign® ».

### 1.3 Les entités de la constitution et de la gestion des preuves

Le Service K.Websign® comprend les fonctions principales suivantes :

- mise à disposition d'un Service de certification électronique pour la délivrance de Certificats électroniques dont l'un d'eux est notamment associé à la Signature de données électroniques échangées et validées par l'Organisme client et les Utilisateurs ;
- mise à disposition d'un outil logiciel de signature électronique ;

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

- réception et enregistrement des éléments validés et signés par l'Organisme client et l'Utilisateur ;
- création, horodatage et archivage du Fichier de preuve relatif à chaque Transaction.

Les entités intervenant dans la constitution du Fichier de preuve sont décrites ci-après.

### **1.3.1 L'Organisme client**

L'Organisme client est l'entité qui met en œuvre et exploite un portail web applicatif pour les besoins de son application métier sur lequel l'Utilisateur se connecte afin de réaliser une Transaction au moyen de l'Application K.Websign®. Il génère, notamment à partir des informations transmises par l'Utilisateur conformément au Protocole de consentement défini par l'Organisme client, le document électronique (ci-après « Données métier signées ») qui sera proposé à l'Utilisateur pour signature.

Si le document électronique est au format PDF et que l'Organisme client souhaite mettre en œuvre les mécanismes de signature embarquée au sein du document PDF, le document devra inclure des champs de signatures prédéfinis qui seront utilisés par l'Application K.Websign.

### **1.3.2 L'Autorité de Certification**

L'Autorité de Certification est l'entité qui est en charge de l'émission et de la gestion des Certificats électroniques utilisés par l'Organisme client et les Utilisateurs dans le cadre du Service K.Websign®. En fonction des différentes étapes du processus de constitution du Fichier de preuve, les Certificats électroniques ont un usage de signature, de chiffrement ou d'intégrité, étant précisé qu'un Certificat est associé à un usage particulier.

L'Autorité de Certification peut être indifféremment, en fonction des Applications web et de la préférence de l'Organisme Client, soit l'Organisme client, soit KEYNECTIS, soit toute autre entité sous réserve que le Service de certification utilisé soit exploité techniquement par KEYNECTIS. Quelque soit l'entité choisie, l'identité de l'Autorité de certification et la Politique de certification applicable seront mentionnées dans le Certificat utilisé dans le cadre du Service K.Websign®.

Si l'Organisme Client souhaite mettre en œuvre les mécanismes de signature embarquée au sein du document PDF, l'Autorité de certification devra faire partie d'une des hiérarchies de confiance particulières gérées par KEYNECTIS sous approbation de la société Adobe® Inc.

### **1.3.3 L'Utilisateur**

L'Utilisateur est une personne physique qui se connecte sur le portail web applicatif de l'Organisme client et qui réalise avec ce dernier une Transaction. Au cours de cette Transaction, et afin de manifester son consentement aux Données métier signées, l'Utilisateur signe le document présenté par l'Organisme client, et ce au moyen du Service K.Websign®.

### **1.3.4 Le fournisseur du Service K.Websign®**

Le fournisseur du Service K.Websign® est l'entité qui exploite et héberge l'Application K.Websign® utilisée par l'Organisme Client et les Utilisateurs de son portail web applicatif. En l'espèce, le fournisseur de l'Application K.Websign® est la société KEYNECTIS.

KEYNECTIS met en œuvre les applications logicielles nécessaires à la génération du Fichier de preuve et est en charge de l'hébergement de l'applicatif de signature utilisé par l'Utilisateur pour signer les Données métier conformément au Protocole de consentement établi par l'Organisme client.

### **1.3.5 Le tiers horodateur : l'Autorité d'horodatage**

Le tiers horodateur est l'entité qui délivre la Contremarque de temps associée au Fichier de preuve. Cette Contremarque de temps a pour objet de positionner dans le temps la réalisation et l'acceptation de la Transaction par l'intermédiaire du Service K.Websign. Dans le cadre des présentes, KEYNECTIS est le tiers horodateur pour la génération des Contremarques de temps.

### **1.3.6 Le tiers archiveur**

Le tiers archiveur est l'entité qui conserve le Fichier de preuve créé et transmis par KEYNECTIS de manière à prolonger la garantie d'intégrité, d'imputabilité et d'intelligibilité (sous réserve du format du document sous forme électronique choisi par l'Organisme client) pendant la période de temps définie par l'Organisme client. Dans le cadre des présentes, KEYNECTIS a fait appel au tiers archiveur « CDC Arkhinéo » pour la réalisation du Service d'archivage.

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

## 1.4 Usages et applications concernés par la politique de gestion de preuves

La présente Politique de Gestion de Preuves s'applique aux Transactions réalisées entre l'Organisme client et ses Utilisateurs par l'intermédiaire du Service K.Websign®. KEYNECTIS conserve ainsi les éléments relatifs à la Transaction (informations signées et archivées) afin de constituer des Preuves.

L'Organisme client peut utiliser le Service K.Websign® pour toutes applications métier de son choix, étant précisé qu'il est le seul à apprécier l'adéquation du Service K.Websign® à ses besoins et qu'il définit le Protocole de consentement (incluant les procédures d'identification des Utilisateurs lors de la génération du Certificat électronique) applicable à ses applications métiers utilisant le Service K.Websign®.

Il est également 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 X 509 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.

## 1.5 Gestion de la politique de gestion de preuves

### 1.5.1 Entité gérant la Politique de gestion de preuve

L'entité en charge de l'administration et de la gestion de la politique de gestion de preuve est l'Autorité Administrative (AA) de la Politique de Gestion de preuve au sein de la société KEYNECTIS. L'AA est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente Politique de gestion de preuve.

A cette fin, elle met en œuvre et coordonne une organisation dédiée, qui statue à échéance régulière, sur la nécessité d'apporter des modifications à la Politique de gestion de preuve.

Toute évolution de la politique de gestion des preuves effectuée par la société KEYNECTIS le sera dans le cas d'évolution de l'Application K.Websign®.

### 1.5.2 Point de contact

L'AA est l'entité à contacter pour toutes questions concernant la présente Politique de gestion de preuve K.Websign®.

Le représentant habilité de cette AA est :  
Monsieur Jean-Yves Faurois  
Directeur Qualité & Sécurité de KEYNECTIS  
KEYNECTIS – 11 13 rue René Jacques - Issy les Moulineaux 92131 Cedex  
Téléphone : (33) (0)1.55. 44.22.00  
Fax : (33) (0)1.55.64.22.01

## 1.6 Acronymes et définitions

### 1.6.1 Liste des acronymes

AC	Autorité de certification
AE	Autorité d'enregistrement
AH	Autorité d'Horodatage
CRL ou LCR	Certificate Revocation List (Liste des Certificats Révoqués)
ICP	Infrastructure à Clés Publiques
LCR ou CRL	Liste des Certificats Révoqués ou (Certificate Revocation List)
PC	Politique de certification
PDF	Portable Document Format
PH	Politique d'Horodatage
PGP	Politique de Gestion de Preuves
WISIWYS	What You Sign Is What You See : vous signez ce que vous voyez.

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

## 1.6.2 Définitions

Les termes qui suivent auront la signification suivante lorsqu'ils sont utilisés dans la présente Politique de gestion de preuve avec une majuscule.

**Adobe Approved Trust List ou AATL :** désigne le programme Adobe mettant à disposition un ensemble de fonctions de signature électronique au sein du format PDF permettant à toute personne recevant un document d'en vérifier l'intégrité et d'identifier son auteur de façon certaine avec les produits Adobe Acrobat et Reader à partir de la release 9. Les certificats utilisés doivent être conformes aux exigences des politiques de certification approuvées par le département de sécurité de la société Adobe et de KEYNECTIS.

**Adobe Certified Document Services ou CDS :** désigne le programme Adobe mettant à disposition un ensemble de fonctions de signature électronique au sein du format PDF permettant à toute personne recevant un document d'en vérifier l'intégrité et d'identifier son auteur de façon certaine avec les produits Adobe Reader ou Acrobat. Les certificats utilisés doivent être conformes aux exigences des politiques de certification approuvées par le département de sécurité de la société Adobe et de KEYNECTIS.

**Application K.Websign® :** désigne l'ensemble cohérent d'informations et de programmes informatiques de KEYNECTIS hébergé sur les matériels de KEYNECTIS mis à disposition du Client et ayant pour objet de fournir un service de génération et d'archivage de fichiers de preuve associées à des Transactions réalisées en ligne entre l'Organisme client et l'Utilisateur.

**Application web :** désigne un ensemble d'applications informatiques de l'Organisme client susceptible de faire appel au Service K.Websign® proposé et hébergé par KEYNECTIS. Plus particulièrement, ce terme désigne l'ensemble cohérent d'informations et de programmes informatiques de l'Organisme client ayant pour objet de mettre à disposition de l'Utilisateur un service de Transactions conformément au Protocole de consentement défini par l'Organisme client et à la Politique de gestion de preuve K.Websign®.

**Autorité de Certification (ou AC) :** désigne l'une des composantes de l'Infrastructure de Clés Publiques (ICP) générant et émettant des Certificats sur demande des Autorités d'enregistrement, et ce en application des règles et des pratiques déterminées par elle dans sa Politique de Certification et la Déclaration des Pratiques de Certification associée.

**Autorité d'horodatage (AH) :** désigne une entité qui a en charge l'application d'au moins une politique d'horodatage en s'appuyant sur une ou plusieurs Unités d'Horodatage. L'AH délivre des contremarques de temps avec une précision donnée et à partir de source de temps choisies.

**Autorité d'Enregistrement (ou AE) :** désigne l'une des composantes de l'ICP, approuvée par une AC pour enregistrer les demandes de Certificats, les valider ou les rejeter. Cette entité applique des procédures d'identification des demandeurs de Certificat conformément aux règles définies dans la Politique de Certification complétées par celles mises en place par le Client dans le cadre de ses pratiques commerciales.

**Binary Large Object (BLOB) :** désigne un ensemble formaté de données qui contient les éléments propres à une Transaction entre l'Organisme client et un Utilisateur ainsi que les données de sécurité y afférents.

**Biclé :** désigne un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptologie basée sur des algorithmes asymétriques. Deux types de biclés interviennent dans l'ICP :

- Les biclés de signature dont la clé privée est utilisée à des fins de signature et/ou d'authentification et la clé publique à des fins de vérification,
- Les biclés de confidentialité, dont la clé privée est utilisée par une application à des fins de déchiffrement de données ou informations et la clé publique à des fins de chiffrement de ces mêmes informations.

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

**Certificat électronique** ou **Certificat** : désigne un fichier électronique attestant que la clé publique appartient à l'entité qu'il identifie. Il est délivré par une autorité de confiance : l'Autorité de certification qui en signant le certificat valide le lien entre l'entité et le bi-clé. Un certificat contient des informations telles que :

- l'identité du porteur de certificat,
- la clé publique du porteur de certificat,
- la durée de vie du certificat,
- l'identité de l'autorité de certification qui l'a émis,
- la signature de l'AC qui l'a émis.

Un format standard de certificat est normalisé dans la recommandation X509 v3.

Dans le cadre des présentes et sans précision complémentaire, le terme Certificat désigne l'ensemble des certificats électroniques utilisés dans le cadre du Service K.Websign® à savoir :

- les **certificats KWS** lesquels peuvent être affectés à la fois à la signature par l'Organisme client des Données métier et à la fois à la sécurisation des échanges de données entre le serveur de l'Organisme client et l'Application K.Websign® ;
- les **certificats KWA** lesquels sont affectés à la signature par l'Utilisateur des Données métier signées présentées par l'Organisme Client et qui ont pour caractéristique principale d'avoir une existence éphémère permettant leur génération « à la volée » pour le compte de l'Utilisateur identifié.

**Champ de signature** : désigne une zone particulière dans un document au format PDF dans laquelle pourront être positionnés les Eléments visuels constituant la représentation de la signature électronique dans le document.

**Contremarque de temps** : désigne la donnée qui lie une empreinte numérique à une date et une heure d'UH. Cette contremarque de temps est signée électroniquement par une unité d'horodatage (UH). Une contremarque de temps permet d'établir la preuve que l'empreinte numérique existe à la date et l'heure qui y figurent.

**CUF** : désigne une information contrôlable générée et communiquée par l'Organisme client à la Plateforme K.Websign® de façon sécurisée et saisie par l'Utilisateur pour être comparée à la valeur précédemment communiquée par l'Organisme client au niveau de la Plateforme K.Websign®.

**CUF\_ORG** : désigne une information contrôlable a posteriori, saisie par l'Utilisateur et transférée, sans contrôle de l'Application K.Websign®, dans l'accusé de réception par la Plateforme K.Websign® vers le site web de l'Organisme client.

**Déclaration des Pratiques de Certification (DPC)** : désigne l'énoncé des pratiques utilisées par une Autorité de Certification pour émettre des Certificats.

**Digital Signature (DIGSIG)** : désigne l'abréviation de Digital Signature pour un module particulier du logiciel Adobe® Live Cycle®.

**Document électronique** : désigne l'ensemble de données structurées pouvant faire l'objet de traitement informatique par les applications informatiques du Client K.Websign®.

**Données d'activation** : désigne les données ou actions associées à un Utilisateur permettant de mettre en œuvre sa clé privée. Dans le cas d'un Certificat KWA, ces données ou actions sont définies par le Protocole de consentement et la Politique de Gestion de Preuves.

**Données métier** : désigne un document électronique sous un format PDF ou XML créé par l'Organisme client.

**Données métier signées** : désigne les Données métier auxquelles a été apposée la signature électronique de l'Organisme client avec un Certificat de type KWS ou un Certificat de signature émis par une AC tierce. Ces données signées sont ensuite présentées à l'Utilisateur qui les signera électroniquement avec le Certificat KWA s'il y consent, créant ainsi l'Original.

**Eléments visuels de la signature** : désigne l'ensemble des informations sous format électronique (texte, fichier PDF, images) qui peuvent être combinées de façon à établir une représentation visuelle de la signature électronique dans le document signé. Ces éléments visuels seront intégrés dans le Champ de signature suivant la

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

configuration et les éléments prédéterminés par le Client à partir de la configuration de base proposée avec les outils de la société Adobe® Inc.

**Enveloppe Sécurisée** : désigne l'ensemble des éléments créés en suite de la réalisation de la Transaction entre l'Organisme Client et l'Utilisateur et lors de la fabrication d'un accusé réception par K.Websign®, condensé dans un BLOB signé et chiffré.

**Feuille de style** : désigne le fichier ou la partie de document web décrivant la manière d'afficher des éléments HTML individuels dans un navigateur web.

**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 et la preuve de la réalisation de la transaction conclue conformément aux procédures décrites dans la présente PGP.

**Hash ou Empreinte numérique** : désigne le résultat d'une fonction de hachage à sens unique appelé empreinte, c'est-à-dire d'une fonction calculant une empreinte d'un message de telle sorte qu'une modification même infime du message entraîne la modification de l'empreinte.

**Horodatage** : désigne l'ensemble des prestations nécessaires à la génération des contremarques de temps et à la gestion des unités d'horodatage.

**HTML (Hypertext Markup Language)** : désigne l'ensemble des éléments identifiés indiquant au navigateur web la manière d'afficher ces éléments et les informations d'une page web.

**Infrastructure à Clés Publiques (ICP)** : désigne un ensemble de moyens techniques, humains, organisationnels, documentaires et contractuels pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques. L'ICP gère le cycle de vie d'un certificat à savoir sa génération, sa distribution, sa gestion et son archivage.

**Intégrité** : désigne la propriété d'exactitude et de complétude des données. Dans le cadre des présentes, cette propriété est mise en œuvre soit au moyen de certificat électronique de signature ou d'intégrité pour les données stockées, soit au moyen de certificat électronique de contrôle d'accès (SSL) pour les données échangées.

**Liste de Certificats Révoqués (LCR)** : désigne la liste de certificats ayant fait l'objet d'une révocation avant la fin de sa période de validité.

**Module TransID** : désigne le logiciel qui permet de créer un identifiant TransNUM dans un BLOB ainsi que de signer et chiffrer un BLOB.

**Organisme Client** : désigne l'entité ayant contracté avec KEYNECTIS pour l'utilisation du service K.Websign®.

**Original** : désigne les Données métier signées auxquelles a été apposée une signature électronique de l'Utilisateur avec un Certificat KWA.

**PDF (Portable Document Format)** : désigne un format de fichier informatique créé par Adobe Systems et dont la spécificité est de préserver la mise en forme (polices d'écritures, images, objets graphiques...) telle que définie par son auteur, et ce quelles que soient l'application et la plate-forme utilisées pour lire ledit fichier PDF.

**Plateforme K.Websign®** : désigne l'ensemble matériels logiciels et règles d'exploitation mis en œuvre par KEYNECTIS pour délivrer le Service K.Websign® aux Organismes client.

**Politique de Certification (PC)** : désigne l'ensemble des règles énoncées et publiées par l'AC décrivant les caractéristiques générales des Certificats qu'elle délivre. Ce document décrit les obligations et responsabilités de l'AC, de l'AE, des Utilisateurs et de toutes les composantes de l'ICP intervenant dans l'ensemble du cycle de vie d'un Certificat.

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

**Politique d'horodatage (PH)** : désigne l'ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une communauté particulière et/ou une classe d'application avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les clients et les utilisateurs de contremarques de temps.

**Portail web métier** : désigne le serveur web mis en œuvre par l'organisme client et qui héberge une application de type transaction électronique avec des Utilisateurs connus de l'organisme client.

**Preuve électronique** : désigne l'ensemble des données électroniques lié à une transaction électronique réussie entre l'Organisme client et l'Utilisateur résultant de l'utilisation du Service K.Websign®.

**Protocole de consentement** : désigne le document dans lequel l'Organisme client précise l'ensemble des règles pour une Application web donnée utilisant le Service K.Websign® à savoir (i) la définition des actions à réaliser par l'Utilisateur pour signer le document proposé par l'Organisme client, (ii) les modalités de transfert de l'identification de l'Utilisateur par l'Organisme client vers l'Application K.Websign®, (iii) les modalités de contrôle par le Service K.Websign® des informations saisies par l'Utilisateur par comparaison aux informations fournies par le Client K.Websign® pour chaque Transaction, et (iv) le type de fichier soumis par l'Organisme client à signature (XML/PDF...). Trois types de protocoles sont applicables : (i) Protocole simple : simple ou double click, (ii) Protocole avec données vérifiables (appelé « CUF »), (iii) Protocole avec données à vérification ultérieure (appelé « CUFORG »).

**Service d'archivage** : désigne l'ensemble des prestations réalisées pour l'archivage de données électroniques consistant en la capture de l'information, sa conservation dans son format d'origine et sa restitution à la demande de la personne propriétaire de l'information.

**Service de certification électronique** : désigne l'ensemble des prestations réalisées par l'Autorité de Certification pour l'émission de Certificats en appliquant des procédures stipulées dans la Politique de Certification et dans ses engagements contractuels le cas échéant vis à vis de ses propres Utilisateurs.

**Service d'horodatage** : désigne l'ensemble des prestations réalisées pour la datation de données électroniques consistant en la fabrication d'une Contremarque de temps signée.

**Service K.Websign®** : désigne le service de KEYNECTIS mis à disposition de ses clients et constitué notamment de l'Application K.Websign® dont l'objet est de permettre à ses Clients à partir de leur Portail web de proposer à leurs propres clients, fournisseurs ou toute autre personne un service de signature de document sous forme électronique à partir d'une Signature électronique associée à un certificat à usage unique d'une durée limitée émis pour chaque Transaction et de constituer pour archivage électronique un Fichier de preuves relatif à la Transaction conclue en ligne.

**Service de validation OCSP** : désigne le service de KEYNECTIS (Online Certificate Status Protocole) mis à disposition de ses clients pour contrôler la validité des certificats utilisés lors des différentes opérations mettant en œuvre des certificats.

**Signature électronique** : désigne, aux termes de l'article 1316-4 du Code civil, « l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache » et a pour objet d'identifier la personne qui l'appose et de manifester le consentement du signataire aux obligations qui découlent de l'acte signé.

**Signature de certification (Adobe®)** : désigne un type de Signature électronique embarquée permettant de verrouiller et/ou de contrôler les modifications autorisées à un document PDF de type formulaire et permettant d'apposer d'autres signatures, dites Signature d'approbation, dans le document PDF.

**Signature (Adobe®)** : désigne un type de Signature électronique embarquée apposée au document PDF. Pour le cas où le document doit être signé par plusieurs personnes, la première signature est une Signature de certification.

**Signature électronique embarquée** : désigne une fonctionnalité additionnelle du Service K.Websign permettant d'intégrer la signature électronique de l'Utilisateur, et le cas échéant de l'Organisme Client, dans un document

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

sous format PDF. Dans ce cas, les Certificats de signature utilisés sont émis par l'Autorité de certification de KEYNECTIS ayant été référencée par Adobe® dans le cadre du programme « AATL » ou « CDS ». 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 d'horodatage de la signature lors de l'utilisation du certificat pour signature du document sous forme électronique. Cette fonctionnalité additionnelle est liée au choix du service de certification mis à disposition du Client par Keynectis et communiqué à Keynectis lors de la mise en production de l'application du Client utilisant le service K.Websign.

**Transaction électronique** : désigne l'échange électronique entre l'Organisme client et l'Utilisateur au cours duquel l'Organisme client propose pour signature un Document électronique à un Utilisateur qu'il a préalablement identifié, afin de manifester son consentement, l'ensemble constituant ainsi le document Original signé de l'Organisme client et l'Utilisateur.

**TransID** : désigne le module logiciel fourni par KEYNECTIS à l'Organisme client dans le cadre du Service K.Websign® pour générer une Enveloppe Sécurisée.

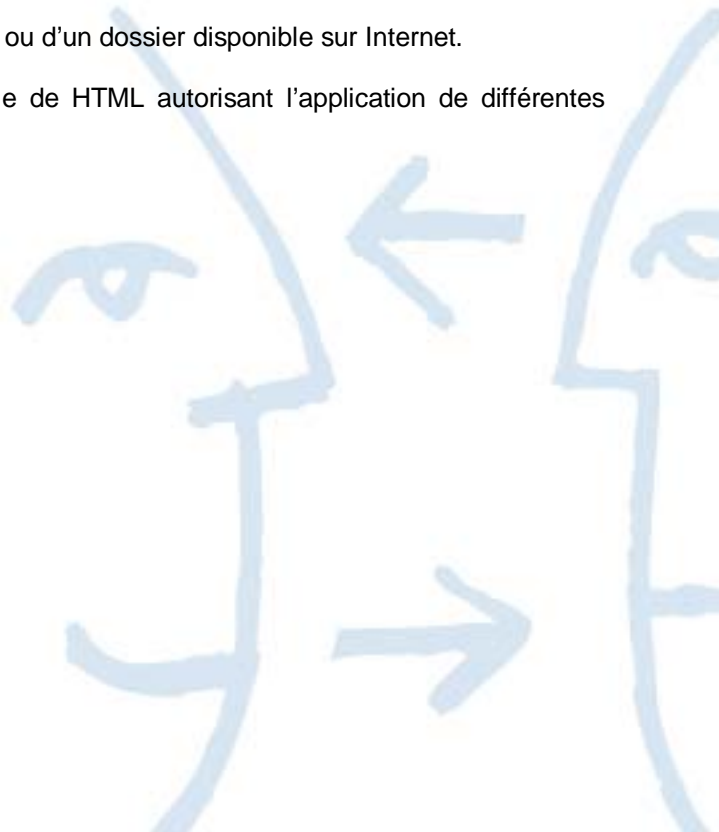
**TransNUM** : désigne un numéro de référence unique généré par l'Application web du Client K.Websign® permettant de lier un Document électronique sur lequel est apposée une signature électronique, à l'Utilisateur préalablement identifié par l'Application web. Cet identifiant est composé de l'identifiant de l'Application métier (fourni par KEYNECTIS), de l'identifiant du serveur de l'application métier, de l'identifiant de l'Organisme client, de la date, de l'heure et d'un index incrémental.

**Unité d'Horodatage (UH)** : désigne l'ensemble de matériels et de logiciels utilisés pour la création de contremarques de temps. L'UH est caractérisée par un identifiant délivré par une AC et une clé unique de signature de contremarques de temps. L'UH construit une date et une heure d'UH qu'elle utilise pour les contremarques de temps qu'elle signe.

**Utilisateur** : désigne une personne physique, connue du Client K.Websign®, identifiée dans le Certificat KWA, qui appose sa signature électronique sur le Document sous forme électronique proposé par l'Application web de l'Organisme Client par l'intermédiaire du Service K.Websign®.

**Uniform Resource Locator (URL)** : désigne l'adresse d'un site ou d'un dossier disponible sur Internet.

**XML (eXtensible Markup Language)** : désigne le sur-ensemble de HTML autorisant l'application de différentes définitions de type de document à une page.

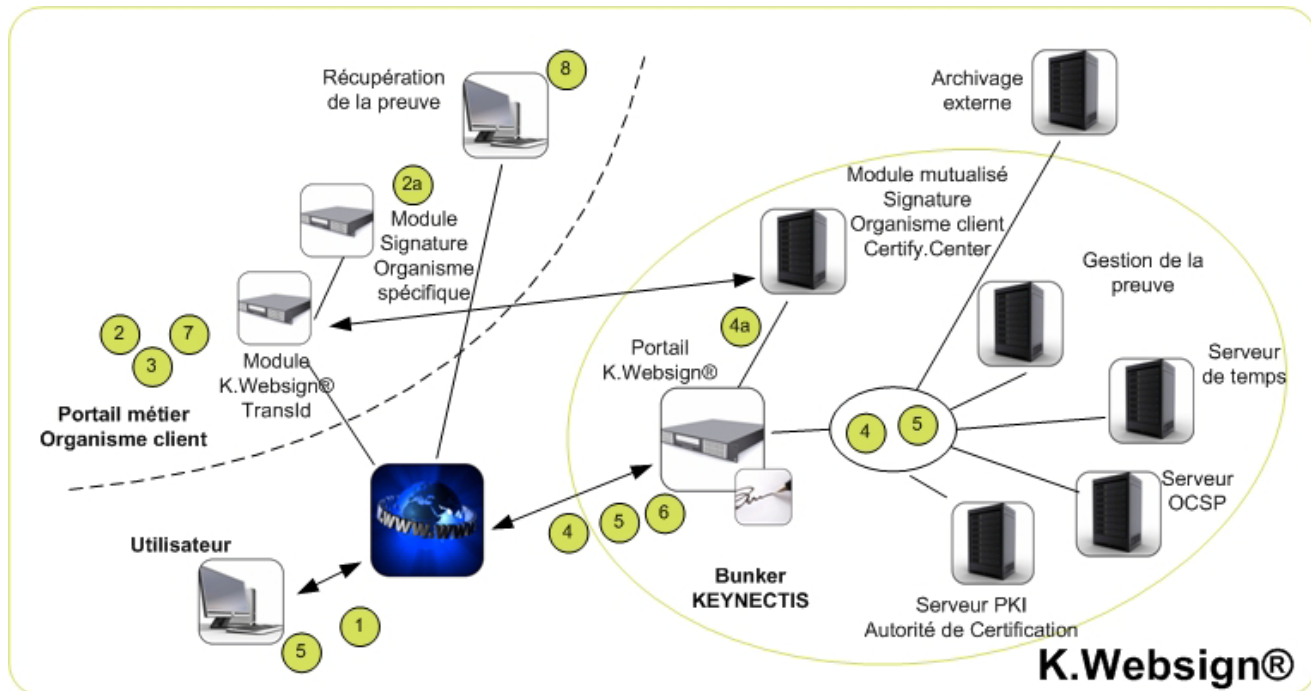


 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

## 2 CONSTITUTION DES PREUVES

Ce chapitre expose le processus de constitution de la preuve, l'identification des acteurs de la constitution de la preuve et leurs obligations au regard de la preuve à constituer ainsi que le contenu de la preuve de la Transaction électronique.

### 2.1 Processus de la constitution de la preuve



**1**  
L'Utilisateur se connecte au portail métier de l'Organisme client qui l'identifie et l'authentifie selon ses propres mécanismes sécuritaires (Login/psw, certificat électronique etc...) et qui lui propose de compléter le document, ci-après « données métier », requérant sa signature pour consentement.

L'identification de l'Utilisateur lors de cette étape est réalisée par l'Organisme client par les moyens de son choix et sous sa responsabilité.

**2**  
L'Application web de l'Organisme Client a pour fonction de constituer le document à partir des informations transmises et indiquées par l'Utilisateur afin de le présenter à l'Utilisateur pour signature si ce dernier y consent. Les modalités de validation du document électronique présenté à l'Utilisateur sont déterminées et mises en œuvre sous la responsabilité de l'Organisme client, notamment par exemple à travers la fourniture des formules adaptées saisies par l'Utilisateur à partir de son poste informatique (mention « Lu et Approuvé », indication de la date,...). C'est à cet ensemble de données que seront appliquées les signatures électroniques des différents intervenants.

**2a**  
Si l'Organisme client souhaite utiliser la fonctionnalité de Signature électronique embarquée dans le document au format PDF, il procédera à la création des Champs de signatures (1 à n) au sein du document. S'il souhaite apposer une première Signature électronique embarquée, il apposera une Signature de certification à l'aide de son certificat de signature Organisme client mis à disposition par KEYNECTIS. Pour le cas où le certificat utilisé est un certificat KWS CDS, l'Organisme client devra utiliser uniquement un logiciel de la société Adobe® tel que LiveCycle Digital Signature®, qui sera exploité par l'Organisme Client ou Keynectis (cf4a).

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

Afin d'assurer l'Intégrité de ces données (par exemple : contrat et mentions complétées par l'Utilisateur) l'Application web de l'Organisme client y appose une signature électronique au moyen d'un Certificat de type KWS-signature ou un certificat émis par une AC tierce. L'identité de l'Organisme client est ainsi certifiée par l'AC qui lui a délivré ce certificat électronique de signature (conformément à la Politique de Certification applicable) lequel contient son identité en tant qu'entité. Les Données métier (au format XML) sont donc signées avec un certificat garantissant l'identité de l'Organisme client en tant que société.

L'Application web de l'Organisme client a, à l'issue de cette étape, présenté à l'Utilisateur et selon les modalités définies par ses soins, l'ensemble des données non modifiables et signées par le certificat de l'Organisme client, ci-après les « Données métier signées ». L'application web a également la possibilité de présenter le Hash des Données métiers signées.

### 3

L'Organisme client ajoute aux Données métier signées :

- des informations sur la méthode de visualisation des Données métier (Feuille XSLT pour XML ou Pdf par exemple)
- des informations nécessaires à l'activation du Protocole de consentement défini par l'Organisme client.

Cet ensemble est ensuite transmis au module TransID, fourni par KEYNECTIS, lequel va :

- générer un numéro (TransNUM) de transaction unique dédié à cette transaction ;
- créer une Enveloppe électronique sécurisée (signée et chiffrée) au moyen du Certificat KWS-intégrité et du Certificat KWS-chiffrement (conformément à la Politique de certification applicable et dont les références sont indiquées dans le Certificat).

La création de cette Enveloppe signée permet à l'Organisme client de s'authentifier auprès de la plateforme K.Websign® lorsque cette Enveloppe sera transmise à l'Application K.Websign®. Elle garantit la non modification des données échangées entre l'Organisme client et la plateforme K.Websign® ainsi que la confidentialité des informations sur le réseau Internet.

Cette Enveloppe sécurisée (signée et chiffrée) est appelée BLOB (Binary Large Object) et est composée de caractères affichables (Base 64) transmissibles dans des pages Html. Il existe deux types de BLOB en fonction du sens du flux : (i) Flux Organisme client vers plateforme K.Websign®, le blob est dit de « requête » et (ii) Flux plateforme K.Websign® vers site web de l'Organisme client le BLOB est dit de « réponse ».

Le contenu du Blob « de requête » émis par l'Organisme client est le suivant :

- TransNUM,
- l'identifiant de l'Utilisateur conformément à la PC KWA applicable,
- l'adresse mail de l'Utilisateur conformément à la PC KWA applicable,
- le Protocole de consentement :
  - o La donnée vérifiable (CUF),
  - o La mise en œuvre de la zone de données à vérification ultérieure (CUFORG).
- la référence de l'autorité émettrice du Certificat KWA pour l'Utilisateur,
- l'adresse URL de retour en fin de transaction,
- le document signé par l'Application web de l'Organisme client et à faire signer par l'Utilisateur (Données métier signées).
- le type de document (XML, PDF...),
- la feuille de visualisation (XSLT) utilisée pour la présentation du document XML,
- des données métier (Tag) imposées dans le cadre de la mise en œuvre de la signature embarquée dans le document au format PDF permettant d'ajouter des Eléments de visualisation dans des champs de signatures précis.
- Des données métier (Tag) non imposées permettant d'enrichir le fichier de preuve

### 4 et 4a

L'Utilisateur est en session sécurisée « SSL » avec la plateforme K.Websign® pour l'application du Protocole de consentement défini et proposé par l'Organisme client.

L'Application K.Websign® reçoit l'Enveloppe sécurisée en provenance du site web de l'Organisme client et procède aux opérations suivantes :

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

1. Déchiffrement de l'Enveloppe
2. Vérification de l'intégrité du BLOB et de l'identité de l'Application web ayant créé ce BLOB
3. Récupération de la référence unique TransNUM et initialisation d'un fichier de preuve pour cette transaction
4. Stockage du BLOB dans le fichier de preuve
5. Vérification de la signature des Données métiers signées selon les règles de l'état de l'art (signature et CRL du certificat)
6. Calcul du Hash (empreinte numérique de ces Données métier signées obtenue au travers de l'algorithme SHA1) qui sera l'objet de la signature de l'Utilisateur
7. Dans le cas de la mise en œuvre de la Signature électronique embarquée, le portail K.Websign® fait appel au service Certify.center® de Keynectis pour apposer (sur la base du certificat de signature enveloppante de l'étape 2a) une Signature (4a)
8. Vérification de la signature électronique embarquée de certification dans le PDF
9. Envoi d'une page HTML appelée Page1 vers l'Utilisateur, étant précisé que cette page HTML de présentation est réalisée par l'Organisme client en respect de sa charte graphique et en a confié le stockage et l'opération à KEYNECTIS.

Cette page de présentation peut proposer :

- La mise en œuvre des processus simple click ou double click au travers d'une case à cocher avec un texte approprié aux obligations légales relatives au consentement de l'Utilisateur et de deux boutons d'action personnalisés (« signer » et « annuler »)
- Une zone de saisie pour l'Utilisateur lui permettant de transmettre une information vérifiable par KEYNECTIS (CUF)
- Une zone de saisie pour l'Utilisateur lui permettant de transmettre une information à vérification ultérieure (CUF\_ORG)
- La visualisation des données métiers signées (PDF) ou la visualisation du Hash des Données métiers signées (XML) afin d'assurer la fonction de WysiWys (what you see is what you sign)

En remplissant le formulaire proposé par l'Organisme client, l'Utilisateur est en mesure à ce stade, de donner son consentement ou d'abandonner l'action de consentement, en conformité avec les règles définies par l'Organisme client. L'acceptation de l'Utilisateur des données présentées par l'Organisme client se traduira par l'activation du moyen de signature électronique mis à son unique disposition au sein de la plateforme K.Websign®.

## 5

Le portail web K.Websign®, reçoit les réponses de l'Utilisateur au formulaire proposé à l'étape 4. Ces données sont sécurisées en intégrité et confidentialité par activation du protocole sécurisé SSL. Le portail K.Websign® procède à leur analyse et déclenche un des deux processus suivants:

- Cas 1 : l'Utilisateur choisit d'activer le bouton d'action «Abandonner». Dans ce cas, l'Application K.Websign® :
  - fabrique un accusé réception spécifique à l'abandon et le stocke dans le fichier de preuve
  - ferme et date le fichier de preuve, étant précisé que ce fichier de preuve n'est pas archivé
  - fabrique une Enveloppe sécurisée à destination de l'Organisme client contenant un BLOB de réponse
- Cas 2 : l'utilisateur choisit d'activer le bouton d'action « signer ». Dans ce cas, l'Application K.Websign® :
  - Applique les contrôles conformément au Protocole de consentement défini et ajoute le résultat du contrôle dans le Fichier de preuve;
  - Demande la génération des bicolé et Certificat KWA, valables uniquement pour cette transaction (TransNUM) en s'adressant à l'Autorité de Certification spécifiée uniquement pour l'Application web considérée
  - Signe au moyen de la clé privée et du certificat KWA associé les Données métier signées, créant ainsi le document signé des deux parties, ci-après « l'Original ».
    - i. Cette signature peut être au format Xades (dite signature enveloppante) et intègre une contremarque de temps émise par une AH de KEYNECTIS dont la PH est référencée dans la contremarque de temps elle-même (RFC 3161) ainsi que la chaîne complète de contrôle de confiance
    - ii. Cette signature peut être du type signature électronique embarquée dans le document sous format PDF avec association d'un Champ de signature au choix de l'Organisme client et contenant une contremarque de temps émise par une AH de KEYNECTIS dont la

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

PH est référencée dans la contremarque de temps elle-même (RFC 3161) ainsi que la chaîne complète de contrôle de confiance

- Vérifie le format de cette signature en appelant un module de contrôle externe (Serveur OCSP) ;
- Stocke l'Original dans le Fichier de preuve ;
- Détruit le biché généré précédemment ;
- Prépare les informations pour la création de l'accusé réception contenant :
  - le TransNUM,
  - l'identité de l'Utilisateur signataire,
  - le Hash du document signé par l'Utilisateur,
  - la valeur CUFORG saisie par l'Utilisateur,
  - les données d'informations communiquées par l'organisme (TAG),
  - la date et l'heure communiquées par le serveur de temps synchronisé par GPS.
- Signe l'accusé réception avec un certificat KWS de KEYNECTIS
- Ajoute l'accusé réception au Fichier de preuve.
- Ferme et scelle le Fichier de preuve au moyen d'une signature électronique dont la date et l'heure sont fournies par un système de datation interne assuré via un dispositif GPS. La forme de cette date et heure est de type contremarque de temps réalisée en respectant le document de recommandation RFC 3161. Cette contremarque de temps est réalisée conformément à la politique d'horodatage de KEYNECTIS publiée à l'URL suivante: <http://www.keynectis.com/fr/support-informations/pc.html>. La traçabilité de la date et l'heure liées au Fichier de preuve est assurée par les journaux d'activité et de suivi des modifications des serveurs de signature et les serveurs de temps utilisés par l'application K.Websign®. L'archivage du Fichier de preuve est alors réalisé localement dans la plateforme K.Websign®
- Gère des informations de suivi d'activité de l'Application web,
- Crée une Enveloppe sécurisée contenant l'accusé réception signé par KEYNECTIS et l'Original signé des parties
- Sauvegarde cette Enveloppe chiffrée pour des besoins de reprises en cas d'incident

## 6

Le portail K.Websign® envoie l'Enveloppe sécurisée sur le poste de l'Utilisateur qui le redirige vers le site web de l'Organisme manuellement ou automatiquement.

Cette action déclenche la tâche de fond d'archivage du Fichier de preuve vers le site d'archivage externe à travers le lien sécurisé (VPN) mis en place entre le site de KEYNECTIS et le site du tiers archiveur.

## 7

Le site web de l'Organisme client reçoit l'Enveloppe sécurisée, puis procède à son déchiffrement et informe l'Utilisateur de la complétude ou non du processus de consentement. Il peut procéder à la publication de l'Original auprès de l'Utilisateur. Si l'Organisme client utilise la fonction de signature électronique embarquée dans le document sous format PDF, ledit document, extrait de l'enveloppe sécurisée, est un original électronique autoportant qui peut être conservé par l'Organisme client ainsi que par l'Utilisateur.

Il est rappelé que le contrôle et la vérification des signatures électroniques embarquées du document PDF n'est réalisable que dans le cadre de l'utilisation des produits Adobe® (Reader ou Acrobat). L'usage d'autre visualisateur de document PDF par l'Utilisateur ne présentera que l'image visuelle de la signature électronique.

## 8

Toute personne désignée et habilitée par le Client peut à tout moment se connecter sur le site web du tiers archiveur et demander la restitution en ligne du Fichier de preuve (recherche sur l'identité du document par le TransNUM unique). KEYNECTIS fournit un utilitaire logiciel permettant la visualisation de ce Fichier de preuve.

## 2.2 Les obligations des acteurs de la constitution de la preuve

### 2.2.1 Les obligations de l'Organisme client

L'Organisme client a les obligations suivantes :

- Choix du moyen d'identification de l'Utilisateur,
- Information de l'Utilisateur et présentation des données objet du consentement, pour signature,

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

- Préparation du document électronique sous format PDF pour intégration des Champs de signature électronique et des Eléments visuels de signature électronique
- Signature des Données métiers (constitution des Données métier signées),
- Conservation des informations sécuritaires liées à la gestion de la signature par ses soins des Données métier conformément à la politique de certification de l'AC émettant les Certificats KWS et à la gestion des Enveloppes sécurisées,
- Définition et formalisation du Protocole de consentement proposé à l'Utilisateur,

### **2.2.2 Les obligations de l'Utilisateur**

L'Utilisateur a pour obligations :

- de se conformer aux procédures définies par l'Organisme client pour la signature des documents échangés avec l'Organisme client, notamment respecter le Protocole de consentement,
- de communiquer des informations exactes et à jour lors de l'établissement du document à signer.

### **2.2.3 Les obligations des Autorités de Certification**

Les Autorités de Certification ont pour obligations :

- d'émettre les Certificats utilisés dans le cadre du Service K.Websign® conformément aux dispositions de la Politique de certification applicable et référencée dans le Certificat,
- de définir les procédures d'enregistrement pour l'émission des Certificats ou de déléguer à une entité distincte la définition de ces procédures,
- de contrôler l'entité en charge de l'enregistrement et de la distribution des Certificats utilisés dans le cadre du Service K.Websign®.

### **2.2.4 Les obligations du fournisseur de l'Application K.Websign®**

Le fournisseur de l'Application K.Websign®, à savoir KEYNECTIS, a pour obligations :

- D'activer et d'exploiter sur sa plateforme de production K.Websign® les Applications web décrites dans le document de mise en production pour le compte de l'organisme Client, conformément à ses procédures métier ;
- De mettre en œuvre les éléments cryptographiques pour la réalisation des signatures au sein de son Centre de production.
- de générer et de détruire après usage pour signature des Données métier signées, la clé Utilisateur ;
- de générer le Fichier de preuve associé à la Transaction en cours ;
- de conserver les documents de mise en production associés au Protocole de consentement choisi par chaque Application web ;
- de contrôler et d'assurer la traçabilité des éléments techniques et organisationnels mis en œuvre pour l'exploitation de la plateforme K.Websign® (modifications apportées aux plateformes matériels et logiciels, changement de configuration, gestion des éléments sécuritaires etc.) ;
- de contrôler et de mettre en place des moyens de sécurité des flux échangés entre la plateforme K.Websign® et les différents acteurs (Utilisateur, Organisme client, tiers archiveur) ;
- de mettre à disposition des Organismes clients le Service K.Websign® conformément à ses engagements contractuels de qualité de service (disponibilité, maintenance planifiée) et à la présente Politique de gestion de preuve.

### **2.2.5 Le tiers Horodateur / l'Autorité d'horodatage**

Le tiers horodateur a l'obligation d'assurer l'émission et la conservation des Contremarques de temps (conformément à sa politique d'horodatage) demandées par la plateforme K.Websign lors de la fermeture de chaque fichier de preuve. Il fournit les moyens de valider la contremarque de temps générée après son émission.

### **2.2.6 Le tiers archiveur**

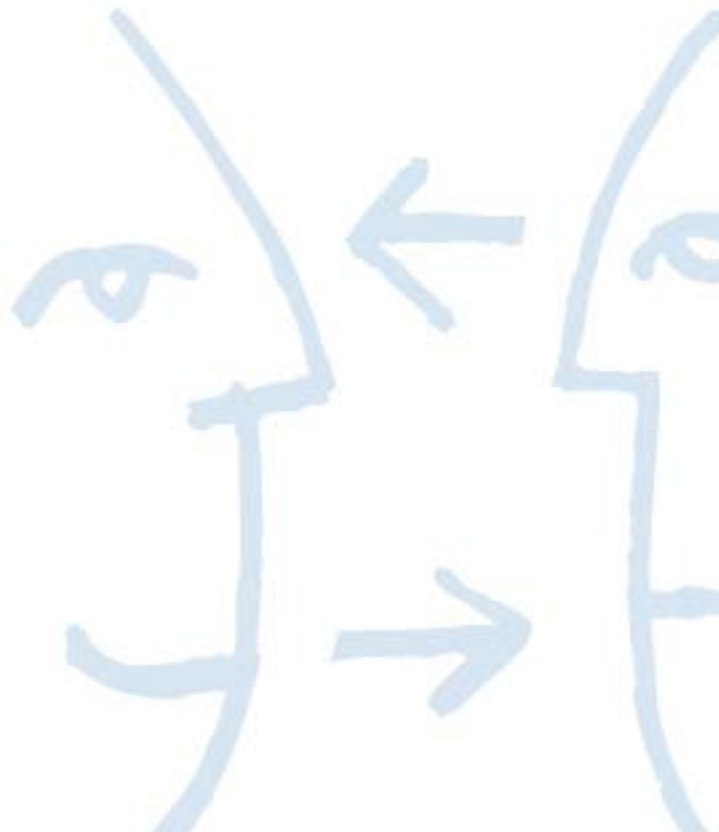
Le tiers archiveur met à disposition de l'Organisme Client l'ensemble de son infrastructure sécurisée permettant de conserver et de restituer pendant une période définie contractuellement les Fichiers de preuves générés par le Service K.Websign®, étant précisé que la plateforme K.Websign® n'est autorisée qu'à réaliser pour le compte des Organismes Clients et avec son accord expresse que (i) les opérations de dépôts des Fichiers de preuve au tiers archiveur à travers un lien sécurisé et (ii) les demandes d'impression d'un Fichier de preuve archivé pour le certifier conforme à l'Original.

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

### 2.3 Eléments constitutifs de la preuve : le Fichier de preuve

Le Fichier de preuve est constitué des éléments suivants (lesquels sont organisés dans un format XML signé) :

- l'ensemble de données (BLOB) envoyé par l'Organisme client à la plateforme K.Websign®
- le compte rendu de la vérification de la signature du BLOB et de l'identité de l'Application web appelante
- les Données métier signées
- le Certificat de signature utilisé par l'Organisme client pour signer les Données métier
- le compte rendu de la vérification de la signature des Données métier signées par la plateforme K.Websign®
- le TransNUM
- les éléments d'identités de l'Utilisateur
- les éléments du Protocole de consentement, CUF et CUFORG
- les dates d'initialisation et de fermeture du Fichier de preuve sur la base de temps fournie par le serveur de temps synchronisé sur GPS
- le Hash des Données métier signées
- le certificat électronique KWA utilisé lors de la signature par l'Utilisateur des Données métier signées
- l'Original signé des parties
- le compte rendu de la vérification par la plateforme K.Websign® de la signature de l'Original par l'Utilisateur
- l'accusé de réception signé par le Certificat de KEYNECTIS
- la signature du Fichier de preuve par un Certificat KEYNECTIS au format XADES et incluant une contremarque de temps signée par l'unité d'horodatage de KEYNECTIS.



 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

### 3 GESTION DES ELEMENTS CONSTITUANT LE FICHER DE PREUVE

#### 3.1 Identification et authentification

L'ensemble des identités contenues dans le Fichier de preuve est défini de la façon suivante :

- l'identité de l'Utilisateur et l'identité de l'Organisme client sont garanties par les Certificats et ce conformément aux Politiques de certification applicables et référencées dans le Certificat utilisé,
- l'identité de l'Application K.Websign® et l'identité du tiers archiveur sont garanties par KEYNECTIS.

L'identification de l'Utilisateur repose sur des procédures et données définies par l'Organisme client.

L'identité de chaque intervenant dans le processus de constitution de la preuve est vérifiée par des moyens techniques et sécuritaires adaptés (VPN, Certificats).

#### 3.2 Intégrité des éléments constituant le fichier de preuve

##### 3.2.1 Données métier signées

L'intégrité des Données métier signées qui font l'objet du consentement de l'Utilisateur est assurée par la signature de ces données par l'Organisme client au moyen d'un bicolé cryptographique associé au Certificat de type KWS ou au Certificat de signature délivré par une AC tierce. Cette intégrité est vérifiée de façon indépendante par la plateforme K.Websign® avant de proposer le déroulement du Protocole de consentement à l'Utilisateur.

##### 3.2.2 Original

La signature électronique apposée sous le contrôle de l'Utilisateur est appliquée aux Données métier signées c'est-à-dire aux Données métier et à la signature de l'Organisme client. L'Original contient donc la trace des actes de signature des parties prenantes.

##### 3.2.3 Accusé réception

L'intégrité de l'accusé de réception fabriqué par KEYNECTIS est assurée par la signature de l'Application K.Websign® avec une clé cryptographique associée à un certificat KWS émis par l'Autorité de Certification de KEYNECTIS qui publie PC, CRL et Certificat conformément à la politique de certification applicable et référencée dans le Certificat.

##### 3.2.4 Fichier de preuve

L'intégrité du Fichier de preuve fabriqué par KEYNECTIS est assurée par la signature de l'Application K.Websign® avec une clé cryptographique associée à un certificat KWS émis par l'Autorité de Certification KEYNECTIS qui publie PC, CRL et Certificat conformément à la politique de certification applicable et référencée dans le Certificat. Cette signature comprend une information de date et heure issue du serveur de temps de KEYNECTIS synchronisé par un signal GPS sous forme d'une contremarque de temps réalisée conformément à la politique d'horodatage suivante : <http://www.keynectis.com/fr/support-informations/pc.html>.

##### 3.2.5 Intégrité des échanges, des procédures et identité des acteurs techniques

L'Enveloppe sécurisée, utilisée entre l'Organisme métier et la plateforme K.Websign® permet de s'assurer de la non modification (intégrité) des données pendant le transport ainsi que la mutuelle reconnaissance des 2 extrémités en liaison. L'intégrité de l'Enveloppe, réalisée au moyen de la vérification de la signature de celle-ci, permet le contrôle de l'identité de l'émetteur. Le déchiffrement de l'Enveloppe permet d'assurer l'identité du récepteur.

Les procédures de mise en exploitation relatives :

- au Protocole de consentement et des Elements visuels de signature inclus dans le Champ de signature,
- aux Certificats d'Organisme client (lors de la mise en œuvre de la signature électronique de l'Organisme par la plateforme K.Websign® de KEYNECTIS),
- à la plateforme K.Websign® par KEYNECTIS,

assurent la traçabilité et l'intégrité de son implémentation.

Le mécanisme de « Virtual Private Network (VPN) » utilisé entre la plateforme K.Websign® et le tiers archiveur procure le même niveau d'intégrité et d'identité des acteurs.

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

Dans le cadre des échanges de flux entre la plateforme K.Websign® et le tiers archiveur, l'envoi des demandes d'archives (avec vérification de l'intégrité du Fichier de preuve au moment de son envoi) et la réception d'Accusé Réception Final permettent la gestion de l'état (archivable, en cours d'archivage et archivé) des Fichiers de preuve au sein de la plateforme K.Websign®. Des procédures de supervision de l'état des fichiers de preuve au sein de la plateforme K.Websign® permettent la gestion des reprises sur erreur d'archivage et la mise à jour de l'état (effacement données métier en conservant les opérations pour traçabilité) après l'opération d'archivage.

Le mécanisme de SSL (chiffrement au moyen d'un certificat serveur) mis en œuvre pendant la gestion du Protocole entre l'Utilisateur et la plateforme K.Websign® garantit l'intégrité des saisies de l'Utilisateur et l'identité de la plateforme K.Websign® pour l'Utilisateur.

L'Organisme Client peut demander à KEYNECTIS les informations de supervision et de traçabilité de la plateforme KWebsign® qui lui seront fournies selon les délais précisés dans le contrat de service conclu avec KEYNECTIS.

### **3.2.6 Lien entre « date de signature, identité utilisateur, identité Organisme client et document métier »**

L'autorité d'horodatage (AH) fournit une contremarque de temps lors de la fermeture du fichier de preuve, suivant la signature de l'Utilisateur qui s'effectue après celle de l'Organisme client. Cette action permet de s'assurer qu'à ce moment précis le document fichier de preuve existait avec ce contenu. Toute modification ultérieure de ce document entraînera la nullité de cette contremarque de temps. Le fichier de preuve contenant l'ensemble des éléments fournis par les différents acteurs (Identité et trace de saisie du protocole pour l'utilisateur, document et identité de l'organisme client) assure la liaison temporelle Utilisateur, Organisme Client, document objet du consentement.

Dans le cas de la signature électronique embarquée dans les documents PDF chaque signature contient sa propre contremarque de temps permettant d'apporter la garantie d'intégrité et d'identité du document et ce indépendamment du statut (expiré, révoqué, ou valide) des certificats électroniques utilisés.

## **3.3 Disponibilité et consultation du Fichier de preuve**

Un Fichier de preuve est constitué pour chaque Transaction réalisée par le biais de l'utilisation du Service K.Websign® et ce quelque soit le résultat de cette transaction (Complet, Erreur, Abandon).

Un module technique sécurisé procède à intervalle régulier à l'envoi des Fichiers de preuve résultant d'une transaction dont le résultat est complet vers le tiers archiveur choisi par l'Organisme client.

Les autres fichiers de preuve dont les résultats sont « erreur ou abandon » sont conservés dans la base de données de l'Application K.Websign®. KEYNECTIS est autorisée à les extraire de la base de données lors de ses opérations de maintenance technique ou évolution du Service K.Websign®.

Une fois archivé, le Fichier de preuve est accessible à toute personne ou application habilitée par l'Organisme Client auprès du tiers archiveur pendant la période requise (sauf indications contraires expressément formulé par l'Organisme client, la période d'archivage nominale est de 10 ans). Les archives ne sont jamais détruites et à la fin de la période de 10 ans, les archives sont restituées à l'Organisme client ou à sa demande expresse la durée de leur archivage peut être prolongée.

## **3.4 Lisibilité et pérennité**

Le Fichier de preuve est transmis à un tiers archiveur qui prolonge l'intégrité, la lisibilité et la disponibilité de cette donnée. KEYNECTIS ne prend pas d'engagement dans la conservation des Fichiers de preuve au sein de la base de données de l'Application K.Websign® mais assure la conservation technique des sauvegardes de cette base de données.

## **3.5 Cohérence temporelle**

L'ensemble des opérations techniques dont le résultat est de dater le Fichier de preuve est réalisé sur des serveurs séparés mais dont la synchronisation d'horloge est assurée par un réseau extérieur (GPS).

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

## 4 UTILISATION DU FICHER DE PREUVE

### 4.1 Restitution du Fichier de preuve


Toute personne ou une Application habilitée désigné par l'Organisme client peut accéder à tout moment au site du tiers archiveur pour procéder au téléchargement sur un poste informatique d'un Fichier de preuve dont l'intégrité est garantie par l'apposition de la signature de KEYNECTIS.

### 4.2 Visualisation du contenu du Fichier de preuve

Au moyen d'un outil logiciel (Feuille de style XSLT), l'Organisme client peut visualiser le contenu d'un Fichier de preuve.

L'outil logiciel fourni par KEYNECTIS permet la visualisation des Données métiers signées qui ont été présentées au consentement de l'Utilisateur sous réserve que l'Organisme Client ait fourni la Feuille de style utilisée lors de la fabrication de l'enveloppe sécurisée.

Exemple de visualisation du contenu d'un Fichier de preuve – vue de synthèse:



**SYNTHESE DE  
- FICHER DE PREUVE -**

**Fichier de preuve de la transaction : 1AXXT01-instal-verifJEE-2009.10.28\_18.4.48-124  
Attestation**

KEYNECTIS en qualité de Prestataire de service de gestion de preuves, atteste que le fichier de preuve référencé ci-dessus contient un document signé électroniquement à la date du: 28/10/2009 18:04:45.  
La signature électronique du document a été effectuée par l'utilisateur: MANENC Dominique dont l'adresse mail est: Dominique.manenc@keynectis.com  
Le fichier de preuve a bien été constitué à la même date.  
Le fichier de preuve a été signé par le serveur de signature de KEYNECTIS à la même date.

---

Les informations suivantes s'appliquent à ce fichier de preuve:  
Signature de contrat au format PDF

---

Le mode d'identification utilisé dans cette transaction était de type secret partagé entre les parties. Le code à usage unique utilisé était le suivant: 12345

---

Le portail K. Websign a reçu un Blob contenant les Données métier signées (original métier) provenant de l'application métier : 1AXXT01.  
La signature blob a été vérifiée par le serveur de validation de K. Websign.  
Cette signature est valide.

---

L'application Métier s'est engagée sur le contenu des Données Métier en le signant.  
La signature de l'original métier a été vérifiée par le serveur de validation de K. Websign.  
Cette signature est valide.

---

L'utilisateur s'est engagé par signature sur le contenu du document qui lui était présenté par l'application Métier.  
La signature du document a été vérifiée par le serveur de validation de K. Websign.  
Cette signature est valide.

---

Un accusé de réception synthétisant la transaction a été constitué par l'application K. Websign, puis soumis au serveur de signature de K. Websign.  
L'accusé de réception a bien été signé par KEYNECTIS.

---

La représentation informatique de l'original métier présenté est la suivante: Original Electronique au format PDF Autoportant  
Le nom de la balise permettant de visualiser l'original métier est :  
<docPDFb64>

### 4.3 Vérification de la signature du fichier de preuve (Intégrité)

Cette vérification peut être faite manuellement par l'Organisme client en utilisant l'outil logiciel fourni par KEYNECTIS appelé visualisateur à la date d'application des présentes en version 1.5.

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

## 5 MESURES DE SECURITE NON TECHNIQUES DES OPERATIONS

### 5.1 Pour le Service de certification électronique

L'ensemble des mesures applicables au Service de certification électronique utilisé pour la fourniture des différents certificats dans le cadre du Service K.Websign® est décrit dans les documents Politiques de certification et Déclaration des Pratiques de Certification de l'Autorité de Certification concernée.

### 5.2 Pour le fournisseur de l'Application K.Websign®

#### 5.2.1 Mesures de sécurité physique

##### 5.2.1.1 Situation géographique

Le site d'exploitation de l'Application K.Websign® est situé en région parisienne (FRANCE) dans les locaux de la société KEYNECTIS. La construction du site respecte les règlements et normes en vigueur et son installation tient compte des résultats de l'analyse de risques du métier d'opérateur de certification, par exemple au regard de certaines exigences spécifiques de type inondation, explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques,...) réalisée par KEYNECTIS.

##### 5.2.1.2 Accès physique

Afin de limiter l'accès aux Applications et aux informations de K.Websign® et afin d'assurer la disponibilité de la plateforme d'exploitation, KEYNECTIS a mis en place un périmètre de sécurité opéré pour ses besoins. La mise en œuvre de ce périmètre permet de respecter les principes de séparation des rôles de confiance telle que prévus pour l'exploitation de son site.

Les accès au site d'exploitation de la plateforme K.Websign® sont limités aux seules personnes nécessaires à la réalisation des services et selon leur besoin d'en connaître. Les accès sont nominatifs et leur traçabilité en termes d'accès est assurée. La sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion passifs et actifs. Tout évènement de sécurité fait l'objet d'un enregistrement et d'un traitement.

Le système d'informations supportant les Services de certification est installé au sein du périmètre de sécurité de KEYNECTIS.

##### 5.2.1.3 Energie et air conditionné

Afin d'assurer la disponibilité des systèmes informatiques de l'Application K.Websign®, des systèmes de génération et de protection des installations électriques ont été mis en œuvre par KEYNECTIS.

##### 5.2.1.4 Exposition aux liquides

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences du contrat de service K.Websign®.

##### 5.2.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences du contrat de service.

##### 5.2.1.6 Sauvegardes hors site

KEYNECTIS réalise des sauvegardes hors site permettant une reprise rapide des fonctions de l'Application K.Websign® suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces fonctions.

#### 5.2.2 Mesures de sécurité procédurales

Les mesures de sécurité procédurales portent sur les points suivants :

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

- Mesures de sécurité vis-à-vis du personnel
- Procédures de vérification des antécédents judiciaires disponibles
- Exigences en matière de formation initiale
- Exigences et fréquence en matière de formation continue
- Gestion des métiers
- Sanctions en cas d'actions non autorisées
- Exigences vis-à-vis du personnel des prestataires externes
- Documentation fournie au personnel
- Séparation des rôles et des pouvoirs

Des précisions sont fournies dans le référentiel documentaire sécurité & qualité de KEYNECTIS.

### 5.2.3 **Procédures de constitution des données d'audit**

La journalisation d'événements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.

KEYNECTIS procède à l'analyse régulière de ces journaux afin de prévenir chaque Organisme client des incidents constatés dans le fonctionnement du service. Cette information est réalisée par le Service Clients de KEYNECTIS (Email vers un administrateur désigné représentant de l'Organisme client).

#### 5.2.3.1 **Type d'événements enregistrés**

KEYNECTIS journalise les événements concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'Application K.Websign® :

- création / modification / suppression de comptes utilisateur et administrateur des machines (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et tentatives non réussies correspondantes.

D'autres événements sont également recueillis. Il s'agit des événements concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques aux zones sensibles ;
- les actions de maintenance et de changements de la configuration des systèmes ;
- les changements apportés au personnel ayant des rôles de confiance ;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation...).

Chaque enregistrement d'un événement dans un journal contient les champs suivants :

- type de l'évènement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement ;
- résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement contient les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'évènement ;

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

- toute information caractérisant l'évènement.

### 5.2.3.2 Processus de journalisation

Les opérations de journalisation sont effectuées au cours du processus considéré.  
En cas de saisie manuelle, l'écriture se fera, sauf exception, le même jour ouvré que l'évènement.

### 5.2.3.3 Procédures de sauvegardes des journaux d'événements

KEYNECTIS met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'événements pour les composantes de l'Application K.Websign, conformément aux exigences de la présente PGP.

### 5.2.3.4 Evaluation des vulnérabilités

Les journaux d'événements, hors ceux de l'application, sont contrôlés régulièrement afin d'identifier des anomalies.

### 5.2.4 Archivage des données d'exploitation

L'archivage des données permet d'assurer la pérennité des journaux et fichiers constitués par les différentes composantes de l'Application K.Websign®.

## 5.3 Pour l'Organisme client

L'ensemble des mesures applicables à l'Organisme client en matière de sécurité des données d'identité des Utilisateurs et de protection des différents Certificats utilisés dans le cadre du Service K.Websign® est décrit dans un document qui lui est propre.

## 5.4 Pour le tiers archiveur

L'ensemble des mesures applicables au tiers archiveur en charge de la fourniture des fonctions d'archivage est décrit dans le référentiel documentaire (ou le cas échéant la politique d'archivage) de la société concernée.

## 5.5 Pour le tiers horodateur

L'ensemble des mesures applicables au tiers horodateur en charge de la fourniture des Contremarques de temps est décrit dans la politique d'horodatage applicable de la société concernée.

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

## 6 MESURES DE SECURITE TECHNIQUES ET LOGIQUES

### 6.1 Pour le Service de certification électronique

L'ensemble des mesures techniques et logiques relatives au Service de certification électronique est décrit dans les politiques de certification des l'Autorité de certification concernée.

### 6.2 Pour l'Utilisateur

L'utilisation du Service K.Websign® par l'Utilisateur à savoir l'utilisation d'un formulaire HTML standard pour le déroulement du Protocole de consentement n'impose pas de mesure particulière à appliquer sur le poste de l'Utilisateur. Il n'y a de ce fait pas d'installation de logiciel ou de scanning de son poste.

Pour les besoins de l'utilisation du Service K.Websign®, On suppose que le système de l'utilisateur pour la présentation des données fournies possède une ou plusieurs applications de présentation qui :

- soit retranscrivent fidèlement le type du document à signer ;
- soit préviennent le signataire des éventuels problèmes d'incompatibilités dispositif de présentation avec les caractéristiques du document.

### 6.3 Pour l'Organisme client

Les mesures de sécurité techniques et logiques à la charge de l'Organisme concerne la partie de l'Application K.Websign® (à savoir le module TransID) qui est hébergée sur le site informatique de l'Organisme client.

Pour les besoins de l'utilisation du Service K.Websign®, l'Organisme client doit sécuriser ses mécanismes techniques qui mettent en œuvre cette application selon les règles de l'état de l'art et de la technique applicable à la sécurisation d'un serveur.

La machine hôte sur laquelle l'applicatif s'exécute peut être soit directement sous la responsabilité de l'Organisme client, soit sous la responsabilité d'une personne morale ou physique qui lui garantit que les mesures ci-après sont bien appliquées :

- le système d'exploitation de la machine hôte doit offrir des contextes d'exécution séparés pour les différentes tâches qu'il exécute.
- l'Organisme client respecte l'état de l'art et de la technique, en particulier les mesures suivantes :
  - o la machine hôte est protégée contre les virus
  - o les échanges entre la machine hôte et d'autres machines via un réseau ouvert sont contrôlés par au moins un pare feu contrôlant et limitant les échanges
  - o l'accès aux fonctions d'administration de la machine hôte est restreint aux seuls administrateurs de celle-ci (différenciation compte utilisateur/administrateur)
  - o l'installation et la mise à jour de logiciels sur la machine hôte est sous le contrôle de l'administrateur
  - o le système d'exploitation de la machine hôte refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres

L'Organisme client doit se prémunir des menaces où des processus informatiques viendraient perturber l'exécution des services de l'applicatif TransID et par exemple modifier les données (TransNUM, BLOB, ...) lorsqu'elles sont sous son contrôle.

L'Organisme client doit prendre les mesures nécessaires pour que l'Utilisateur puisse authentifier le serveur applicatif à l'aide d'un certificat permettant l'établissement d'une session SSL.

### 6.4 Pour le fournisseur de l'Application K.Websign

Ce chapitre traite de la partie de l'Application K.Websign®, qui est hébergée sur un système d'informations dédié au sein de KEYNECTIS et auquel accède l'Organisme client pour les besoins de ses Applications web.

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

#### **6.4.1 Mesures de sécurité de l'outil de signature mis à disposition de l'Organisme client**

Lorsque l'Organisme client choisit de mettre en œuvre la Signature électronique embarquée dans le document PDF par l'utilisation de la Plateforme K.Websign (Cf 2a), il transmet à KEYNECTIS une demande d'apposition de sa Signature de certification dans un champ de signature qu'il a créé au sein du document, s'il souhaite que sa signature soit intégrée dans le document. Cette signature est réalisée au moyen d'un élément de sécurité hardware appelé HSM localisé dans le Centre de production de KEYNECTIS et accessible dans les mêmes conditions de sécurité que les HSM des Autorités de certification. Le choix et l'utilisation du bclé de signature et du certificat associé au sein du HSM sont régis par le contrôle du certificat de signature KWS enveloppant les données métiers et contenu dans le Fichier de preuve.

#### **6.4.2 Mesures de sécurité de l'outil de signature mis à disposition de l'Utilisateur**

Lorsque l'Utilisateur consent au document proposé par l'Organisme client conformément au Protocole mis en œuvre par l'Application web, l'Utilisateur active sous son contrôle, un outil de signature qui utilise un bclé généré automatiquement par la plateforme K.Websign®. Ce bclé sera affecté, par le biais de la création d'un Certificat KWA, d'une part à la transaction (TransNUM) et à l'identité de l'Utilisateur (transférée par l'Organisme client). Ce bclé sera ensuite utilisé pour signer le Hash des Données métiers signées, puis détruit immédiatement après utilisation.

#### **6.4.3 Mesures de sécurité des systèmes informatiques**

Le niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de la plateforme K.Websign® répond aux objectifs de sécurité suivants :

- identification et authentification des Utilisateurs pour l'accès au système ;
- gestion de sessions d'utilisation ;
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- gestion des comptes des Utilisateurs, notamment modification et suppression rapide des droits d'accès;
- protection du réseau contre toute intrusion d'une personne non autorisée ;
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- fonctions d'audits (non-répudiation et nature des actions effectuées) ;

Le serveur applicatif de KEYNECTIS dédié à la gestion et à la mise en œuvre de l'Application K.Websign® est authentifié par l'Utilisateur à l'aide d'un certificat permettant l'établissement d'une session SSL.

#### **6.4.4 Mesures de sécurité du système durant son cycle de vie**

##### **6.4.4.1 Mesures de sécurité liées au développement des systèmes**

L'implémentation du système permettant de mettre en œuvre les composantes de l'Application K.Websign® est documentée. La configuration du système des composantes de l'Application K.Websign® ainsi que toute modification et mise à niveau sont documentées et contrôlées.

##### **6.4.4.2 Gestion de la sécurité**

Toute évolution significative d'un système ou d'une composante de l'Application K.Websign® est documentée et est conforme au schéma de maintenance de l'Application K.Websign®.

##### **6.4.5 Mesures de sécurité réseau**

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'Application K.Websign®.

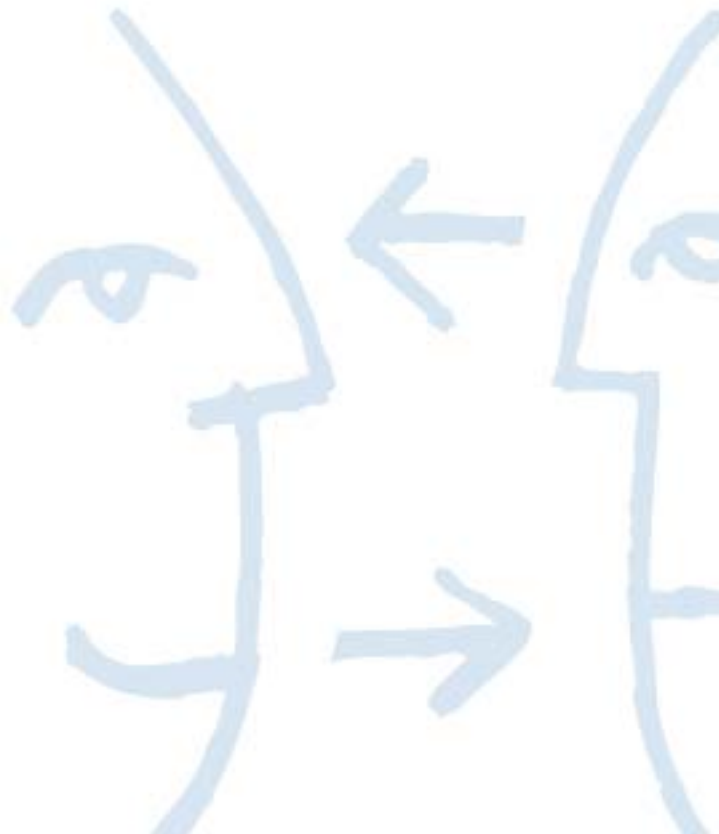
 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

## 6.5 Pour le tiers archiveur

L'ensemble des mesures applicables au tiers archiveur en charge de la fourniture des fonctions d'archivage est décrit dans le référentiel documentaire (ou la politique d'archivage le cas échéant) de la société concernée.

## 6.6 Pour le tiers horodateur

L'ensemble des mesures applicables au tiers horodateur en charge de la fourniture des Contremarques de temps est décrit dans la politique d'horodatage applicable de la société concernée.



 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
	<b>Service K.Websign®</b>	<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
		<b>Version :</b>	34

## 7 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et les évaluations concernent ceux que KEYNECTIS doit réaliser, ou faire réaliser, afin de s'assurer que l'ensemble de son service est bien conforme à ses engagements affichés dans sa politique de gestion de preuve.

### 7.1 Fréquences et / ou circonstances des évaluations

Les évaluations seront réalisées à la demande de l'Organisme client ou à l'initiative de KEYNECTIS.

### 7.2 Identités / qualifications des évaluateurs

Le contrôle d'une composante doit être assigné par KEYNECTIS ou par l'Organisme client à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

### 7.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne doit pas appartenir à l'entité opérant la composante de l'application contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

### 7.4 Sujets couverts par les évaluations

Les contrôles de conformité peuvent porter sur une composante ou l'ensemble de l'Application et vise à vérifier le respect des engagements et pratiques définies dans la politique de gestion des preuves ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

### 7.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à KEYNECTIS, un avis parmi les suivants : "réussite", "échec", "à confirmer".

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas de résultat « Echec » ou « A confirmer », et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations. Le choix de la mesure à appliquer est effectué par KEYNECTIS et doit respecter ses politiques de sécurité internes. KEYNECTIS détermine un délai à l'issue duquel les non-conformités doivent être résolues. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, KEYNECTIS acte de la conformité de l'Application ou de la composante de l'Application contrôlée aux exigences de la PGP.

### 7.6 Communication des résultats

Les résultats des audits sont tenus à la disposition des Organismes clients sur demande expresse de ces derniers.

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

## 8 DISPOSITIONS DE PORTEE GENERALE

### 8.1 Barèmes des prix

Les dispositions relatives aux conditions financières du Service K.Websign® sont prévues dans les documents contractuels conclus entre KEYNECTIS et l'Organisme client d'une part, et le cas échéant entre l'Organisme client et l'Utilisateur d'autre part.

### 8.2 Responsabilité financière

Les dispositions relatives à la responsabilité financière concernant le Service K.Websign® sont prévues dans les documents contractuels conclus entre KEYNECTIS et l'Organisme client d'une part, et le cas échéant entre l'Organisme client et l'Utilisateur d'autre part.

Seul l'Organisme client peut engager la responsabilité financière de KEYNECTIS.

### 8.3 Loi applicable et juridictions compétentes

Les dispositions de la Politique de gestion de preuve sont régies par le droit français.

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente Politique, et faute de parvenir à un accord amiable, tout différend sera porté devant les tribunaux compétents de Paris.

### 8.4 Droits de propriété intellectuelle

Tous les droits de propriété intellectuelle relatifs au Service K.Websign® détenus par KEYNECTIS et ses fournisseurs sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, ...etc.) est sanctionnée par les articles L 716-1 et suivants du Code de la propriété intellectuelle.

### 8.5 Protection des données à caractère personnel

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique au contenu de toutes les données collectés, détenues ou transmises par l'Organisme client et l'Utilisateur dans le cadre du Service K.Websign®.

En vertu des articles 323-1 à 323-7 du Code pénal applicable lorsqu'une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc. Les peines encourues varient de 1 à 3 ans d'emprisonnement assorties d'une amende allant de 15.000 à 225.000 euros pour les personnes morales.

### 8.6 Durée et fin anticipée de validité de la politique de gestion des preuves

#### 8.6.1 Durée de validité

La politique de gestion des preuves doit rester en application au moins jusqu'à la fin de l'archivage du dernier Fichier de preuve créé par K.Websign® au titre de cette politique de gestion des preuves.

#### 8.6.2 Effets de la fin de validité et clauses restant applicables

Certaines fonctions du Service K.Websign®, notamment d'archivage, de protection des données confidentielles seront maintenues jusqu'à leur terme contractuel.

### 8.7 Administration de la politique de gestion des preuves

Le présent article indique les dispositions prises par KEYNECTIS en matière d'administration et de gestion de la présente politique de gestion des preuves.

 <b>KEYNECTIS</b>	<b>POLITIQUE DE GESTION DE PREUVES</b>	<b>Date :</b>	30 Octobre 2009
		<b>OID :</b>	1.3.6.1.4.1.22234.2.4.6.1.4
	<b>Service K.Websign®</b>	<b>Version :</b>	34

### 8.7.1 Délai de préavis

KEYNECTIS informera les Organismes clients et leurs Utilisateurs du Service K.Websign® en respectant un préavis de trente (60) jours calendaires avant de procéder à tout changement de la présente politique de gestion de preuves susceptible de produire un effet majeur sur lesdits clients.

KEYNECTIS informera les Organismes clients et leurs Utilisateurs du Service K.Websign® en respectant un préavis de quinze (30) jours calendaires avant de procéder à tout changement de la présente politique de gestion de preuves susceptible de produire un effet mineur sur lesdits clients.

KEYNECTIS peut modifier la présente politique sans préavis lorsque, selon l'évaluation du responsable de la Politique de Gestion des Preuves, ces modifications n'ont aucun impact sur eux. Toutefois il informera le client de la nature de la modification.

### 8.7.2 Forme de diffusion des avis

Dans les cas de modification soumise à préavis, KEYNECTIS avise les clients des modifications apportées à la présente politique de gestion de preuves, par tous moyens à sa convenance dont notamment le site web de KEYNECTIS et la messagerie électronique, en fonction de la portée des modifications.

### 8.7.3 Modifications nécessitant l'adoption d'une nouvelle politique

Si un changement apporté à la présente politique de gestion des preuves a, selon l'évaluation du responsable de la politique, un impact majeur sur un nombre important de clients, le responsable de la politique peut, à sa discrétion, instituer une nouvelle politique avec un nouvel identificateur d'objet (OID).

## 8.8 Limite de responsabilité

La responsabilité de KEYNECTIS ne peut être mise en cause que par les Organismes clients conformément aux dispositions prévues par le contrat conclu avec ces derniers pour l'utilisation du Service K-Websign®.

KEYNECTIS décline toute responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, et quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication.

KEYNECTIS ne saurait être tenue responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1148 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des cours et tribunaux français, les conflits sociaux, la défaillance du réseau ou des installations ou réseaux de télécommunications externes.

KEYNECTIS décline toute responsabilité à l'égard de l'usage qui est fait du Service K.Websign® dans des conditions et à des fins autres que celles prévues dans la présente politique de gestion de preuve et dans tout autre document contractuel applicable associé.

KEYNECTIS décline également toute responsabilité à l'égard du choix de l'acte ou du type du contrat proposé par l'Organisme client pour signature dans le cadre du Service K.Websign®.

KEYNECTIS ne pourra en aucun cas être tenue pour responsable des préjudices indirects, ceux-ci n'étant en aucun cas préqualifiés par avance par les présentes.

La responsabilité de KEYNECTIS retenue en cas de préjudice subi par l'Organisme client, l'Utilisateur ou toute autre personne dans le cadre des présentes est limitée pour chaque période annuelle pour l'ensemble des préjudices subis pour chaque Organisme client et ses Applications y afférentes, au montant précisé dans le contrat conclu avec l'Organisme client concerné.