

ONESYS

**Politique de Signature
de la plateforme PIOTT**

Pour la signature des contrats par les EU et les ETT

Date : 24 Octobre 2007

Version : 1.0

Nombre de pages : 13

TABLE DES MATIERES

1. OBJET DU DOCUMENT	3
2. POLITIQUE DE SIGNATURE ELECTRONIQUE	4
2.1 Champ d'application	4
2.2 Identification	4
2.3 Publication de documents	4
2.4 Processus de mise à jour	4
2.4.1 Circonstances rendant une mise à jour nécessaire	4
2.4.2 Prise en compte des remarques	4
2.4.3 Information des acteurs	5
2.5 Entrée en vigueur d'une nouvelle version et période de validité	5
3. ACTEURS	6
3.1 Les représentants des ETT et des EU	6
3.2 La plateforme PilOTT	6
3.3 Obligations des ETT et des EU	6
3.3.1 Environnement du poste de travail	6
3.3.2 Choix des représentants de l'entreprise.....	6
3.4 Obligations du représentant d'une ETT ou d'une EU	7
3.4.1 Outil de signature utilisé.....	7
3.4.2 Type de certificat utilisé.....	7
3.4.3 Protection du support du certificat.....	7
3.4.4 Révocation du certificat	7
3.5 Obligations de OneSYS	7
3.5.1 Données de vérification	7
3.5.2 Protection des moyens	7
3.5.3 Journalisation	8
3.5.4 Reprise en cas d'interruption de service	8
3.5.5 Assistance aux établissements	8
4. SIGNATURE ELECTRONIQUES ET VALIDATION.....	- 9 -
4.1 Données signées	- 9 -
4.2 Caractéristiques de la signature.....	- 9 -
4.2.1 Type de signature.....	- 9 -
4.2.2 Norme de signature	- 9 -
4.3 Algorithmes utilisables pour la signature.....	- 10 -
4.3.1 Algorithme de condensation.....	- 10 -
4.3.2 Algorithme de chiffrement	- 10 -
4.3.3 Canonicalisation.....	- 10 -
4.4 Conditions pour déclarer valide le fichier signé	- 10 -
4.4.1 Vérification de la signature	- 10 -
4.4.2 Vérification des droits du signataire en fonction de données transmises.....	- 11 -
5. POLITIQUE DE CONFIDENTIALITE	- 11 -
5.1 Classification des informations.....	- 11 -
5.2 Communications des informations à des tiers	- 11 -
6. DISPOSITIONS JURIDIQUES	- 11 -
6.1 Données nominatives	- 11 -
7. CERTIFICAT AYANT SIGNE LE PRESENT DOCUMENT	13

1. OBJET DU DOCUMENT

La signature électronique apposée sur un ensemble de données permet de garantir l'intégrité des données transmises et l'authenticité de leur émetteur.

Une politique de signature est un document décrivant les conditions de recevabilité d'un fichier sur lequel est apposé une ou plusieurs signatures électroniques dans le cadre d'échanges électroniques prédéfinis.

Le présent document, « Politique de Signature de la plateforme PiLOTT », décrit ces conditions dans le cadre des échanges électronique entre les entreprises de travail temporaire et les entreprises utilisatrices.

Ce document est destiné :

- aux entreprises utilisatrices;
- aux entreprises de travail temporaire ;
- à OneSYS.

Dans la suite de ce document, les entreprises de travail temporaire sont désignées par le terme « ETT » et les entreprises utilisatrices par le terme « EU ».

2. POLITIQUE DE SIGNATURE ELECTRONIQUE

Champ d'application

La présente politique de signature, s'applique aux contrats de mise à disposition d'intérimaire échangés entre les ETT et les EU via la plateforme PIOTT.

Afin que ces contrats est une valeur juridique ils doivent faire l'objet d'une signature électronique des deux parties.

Ces contrats font l'objet d'une signature apposée sur l'intégralité des données d'un contrat classique de mise à disposition d'intérimaire.

Cette signature doit être apposée par une personne habilitée à engager son établissement auprès de la plateforme PiOTT pour l'ensemble de données transmises.

Identification

La présente politique de signature est identifiée par l'OID (Object IDentifier) : 1.2.205.182.1.1.2
Cette référence doit figurer dans les données signées conformément au paragraphe 4.2.2 de ce document afin d'attester du régime sous lequel le signataire adresse sa remise.

Publication de documents

La présente politique est publiée après approbation formelle de ONESYS et apposition d'une signature électronique.

La présente politique est consultable à l'adresse suivante:

http://www.onesys.fr/ps_1_1_1_2.pdf

Processus de mise à jour

Circonstances rendant une mise à jour nécessaire

La mise à jour de la présente politique de signature peut avoir pour origines, l'évolution du droit, l'apparition de nouvelles menaces et de nouvelles mesures de sécurité, les observations des différents acteurs, etc.

La présente politique est réexaminée a minima tous les 2 ans.

Prise en compte des remarques

Toutes les remarques, ou souhaits d'évolution, sur la présente politique sont à adresser par courriel à l'adresse suivante:

support@pilott.fr

Ces remarques et souhaits d'évolution sont examinés par OneSYS qui engage si nécessaire le processus de mise à jour de la présente politique de signature.

Information des acteurs

Les informations relatives à la version courante de cette politique et aux versions antérieures sont disponibles sur le site de OneSYS où une rubrique documentaire référence toutes les versions précédentes de ce document.

La publication d'une nouvelle version de la politique de signature consiste à

1) mettre en ligne les éléments suivants :

- la politique de signature au format PDF,
- l'identifiant de la politique de signature (OID),
- l'empreinte de la politique de signature,
- l'algorithme de hachage utilisé pour réaliser l'empreinte de la politique de signature,
- la valeur de la signature apposée sur la politique de signature,
- l'algorithme de hachage et de chiffrement utilisé pour réaliser la signature de la politique de signature,
- la date et l'heure d'entrée en vigueur de la politique de signature.

2) archiver la version précédente après apposition de la mention « obsolète » sur chaque page.

Entrée en vigueur d'une nouvelle version et période de validité

Une nouvelle version de la politique de signature n'entre en vigueur que 15 jours ouvrés après sa mise en ligne sur le site Internet de OneSYS, et reste valide jusqu'à l'entrée en vigueur d'une nouvelle version.

Le délai de 15 jours est mis à profit par OneSYS pour prendre en compte les changements et mettre à jour, dans l'application de signature de la plateforme PilOTT, la référence à la politique courante.

3. ACTEURS

Les représentants des ETT et des EU

Le rôle des représentant des établissements assujettis est de :

- apposer leur signature électronique sur un contrat;
- s'assurer que le contrat signé est transmis à la plateforme PilOTT.

Pour apposer une signature électronique sur un contrat, les représentants des entreprises doivent disposer d'un certificat de signature et de la plateforme PilOTT.

La qualité d'un signataire ne figurant pas dans son certificat, seuls les représentants préalablement enregistrés auprès de la plateforme PilOTT peuvent engager leur entreprise pour un contrat donné en y apposant leur signature.

La plateforme PilOTT

Le rôle de la plateforme PilOTT est de :

- vérifier la validité de la signature et du certificat ayant servi à sa création ;
- vérifier l'habilitation du signataire à engager son entreprise pour un contrat donné ;
- vérifier la cohérence des données transmises ;
- traiter les données figurant dans les contrats.

La plateforme PilOTT peut déléguer tout ou partie de ces tâches à des prestataires de service en s'assurant de la conformité des services rendus par ces prestataires avec la présente politique de signature.

Obligations des ETT et des EU

Environnement du poste de travail

L'opération de création de la signature doit être réalisée sur le poste de travail du signataire.

L'établissement assujetti doit s'assurer que les postes de travail de ses représentants sont protégés notamment contre l'utilisation frauduleuse de leur identité et de leur outil de signature dans le cadre des applications dont la présente politique de signature fait objet.

Choix des représentants de l'entreprise

Dans chaque entreprise, un responsable établit et transmet à OneSys, la liste des personnes habilitées à signer les contrats sous PilOTT.

Obligations du représentant d'une ETT ou d'une EU

Outil de signature utilisé

Le représentant d'une entreprise utilisatrice doit contrôler les données qu'il va signer avant d'y apposer sa signature.

Type de certificat utilisé

Le représentant d'une entreprise utilisatrice doit utiliser un certificat de signature reconnu par la politique de signature OneSys.

Protection du support du certificat

Le représentant doit prendre toutes les mesures nécessaires pour protéger l'accès à son certificat et aux données secrètes associées, notamment le support qui lui a été remis (carte à puce, dongle, token, ...) et le code PIN associé.

Révocation du certificat

Le représentant d'une entreprise utilisatrice doit demander dans les plus brefs délais à l'organisme émetteur de son certificat la révocation de celui-ci en cas de perte, de vol, de compromission ou de simple suspicion de compromission de sa clé privée.

Obligations de OneSYS

Données de vérification

Pour effectuer les vérifications, le service de validation utilisé par la plateforme PiOTT utilise les données transmises par les entreprises utilisatrices concernant les habilitations de leurs représentants, ainsi que des données publiques relatives aux certificats des signataires, telles que les listes de révocations ou les certificats des prestataires de services de certification électronique émetteurs.

Selon les familles de certificat, un délai variable s'applique entre le moment où est demandée la révocation d'un certificat et le moment où la liste des certificats révoqués est mise à disposition du public. OneSYS ne saurait être tenu responsable des conséquences d'une validation de signature effectuée pendant ce délai de latence.

Protection des moyens

OneSYS s'assure de la mise en œuvre des moyens nécessaires à la protection des équipements fournissant les services de validation.

Les mesures prises concernent à la fois :

- la protection des accès physiques et logiques aux équipements aux seules personnes habilitées;
- la disponibilité du service ;

- la surveillance et le suivi du service.

Journalisation

OneSYS s'assure de la conservation des traces relatives :

- à la circulation des échanges au sein des réseaux et des équipements informatiques ;
- au traitement des données échangées.

OneSYS s'assure que les preuves de traitement relatives à la vérification des signatures électroniques sont conservées pendant 10 ans.

Reprise en cas d'interruption de service

OneSYS s'assure de la mise en œuvre des moyens nécessaires à la reprise d'activité en cas d'interruption de service d'un des composants nécessaire aux tâches dont il a la responsabilité.

Il s'assure en particulier que ces moyens font l'objet de tests à intervalles réguliers.

Assistance aux établissements

Les établissements assujettis peuvent s'adresser par courriel aux correspondants OneSYS pour toute information complémentaire ou pour signaler tout dysfonctionnement à l'adresse suivante :

support@pilott.fr

4. SIGNATURE ELECTRONIQUES ET VALIDATION

Données signées

Au sein d'un fichier signé, les données signées sont composées des éléments suivants :

- l'intégralité des données constituant le contrat ;
- les propriétés de signature telles que définies aux paragraphes 0 du présent document.

Ces deux éléments doivent figurer dans des balises « Object » distinctes, la première balise « Object » contenant les données relatives aux contrats.

Chaque fichier ne devant signé que par un seul et unique représentant, les fichiers ne doivent contenir que les données pour lesquelles le représentant est habilité à engager son établissement.

Les données devant être signées par des personnes distinctes, les données doivent donc figurer dans des fichiers distincts.

Caractéristiques de la signature

Type de signature

Les signatures électroniques apposées par les représentants des ETT et des EU doivent être de types enveloppants.

Norme de signature

Les signatures doivent respecter la norme XAdES (ETSI TS 101 903) en version v1.3.2. Le format XAdES étant un format XML, le jeu de caractères imposé est UTF-8.

Conformément à la norme XAdES, les propriétés signées (SignedProperties / SignedSignatureProperties) doivent contenir les éléments suivants :

- le certificat du signataire (SigningCertificate)
- la date et l'heure de signature (SigningTime)
- la référence au présent document (SigningPolicyIdentifier / SigPolicyIdType)
 - OID de la présente politique de signature (SigPolicyId)
 - Valeur de condensé de la politique de signature calculé et algorithme de condensation utilisé (SigPolicyHash)

Une fois signé, le fichier ne doit plus faire l'objet d'aucun transcodage, et doit transiter dans le système d'information de l'établissement sous la forme d'un flux binaire, avant d'emprunter les canaux habituels de transmission entre les ETT/EU et la plateforme PiOTT.

Algorithmes utilisables pour la signature

Algorithme de condensation

Les algorithmes de condensation à utiliser sont SHA-1 ou SHA-256

Algorithme de chiffrement

L'algorithme de chiffrement à utiliser est RSA.

Canonicalisation

L'algorithme de forme canonique exclusive xml-exc-c14n identifié par l'URI <http://www.w3.org/2001/10/xml-exc-c14n#> est préconisé comme algorithme de canonicalisation.

Conditions pour déclarer valide le fichier signé

Un fichier signé est considéré comme valide par la plateforme PiLOTT lorsque les conditions suivantes sont remplies :

- vérification positive de la signature électronique du signataire ;
- vérification positive des droits du signataire en fonction des données transmises.

Vérification de la signature

La vérification de la signature porte sur :

- la vérification du respect de la norme de signature ;
- la vérification de l'appartenance du certificat du signataire à une famille de certificat reconnue par la plateforme PiLOTT;
- la vérification du certificat du signataire et de tous les certificats de la chaîne de certification:
 - validité temporelle,
 - statut,
 - signature cryptographique ;
- la vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue ;
- la vérification de la signature électronique apposée sur le fichier en utilisant la clé publique du signataire contenue dans le certificat transmis ;
- la vérification de l'identifiant de la politique de signature référencée.

Vérification des droits du signataire en fonction de données transmises

La vérification porte sur:

- l'identification du signataire à l'aide de son certificat ;
- la vérification des droits associés à ce certificat en fonction du type de données signées.

La collecte des droits relatifs aux représentants est gérée au fil de l'eau par les administrateurs de la plateforme PiLOTT en fonction des informations fournies par les ETT et les EU.

5. POLITIQUE DE CONFIDENTIALITE

Classification des informations

Les informations suivantes sont considérées comme confidentielles :

- les journaux du service de validation,
- les procédures internes du service de validation,
- les rapports de contrôle de conformité et les plans d'action référents.

Communications des informations à des tiers

On entend par tiers, tout organisme n'étant pas dans la chaîne de traitement des informations de la plateforme PiLOTT.

La diffusion des informations à un tiers ne peut intervenir qu'après acceptation de OneSYS.

6. DISPOSITIONS JURIDIQUES

Droit applicable

Le présent document est régi par la loi Française.

Données nominatives

En conformité avec les dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le traitement automatisé des données nominatives réalisé à partir de la plateforme de vérification de signature de OneSYS a fait l'objet d'une déclaration auprès de la Commission Nationale de l'informatique et des Libertés (CNIL).

Conformément à l'article 32 de la loi n° 78-17 du 6 janvier 1978, le signataire d'un contrat sur la plateforme OneSYS est informé que les données à caractère personnel qu'il communique sont utilisées par la plateforme de vérification de signature pour la gestion et le suivi des habilitations dans l'application ainsi que pour la constitution de la Preuve.

Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978, l'utilisateur est informé qu'il dispose d'un droit d'accès, de rectification et d'opposition, pour des motifs légitimes, portant sur les données le concernant. A ces fins, il peut adresser une demande écrite signée et accompagnée de

la photocopie d'un document officiel d'identité portant la signature du titulaire (Carte Nationale d'Identité ou passeport) à l'adresse suivante :

OneSYS
6-8 rue George Maranne
69200 Vénissieux

7. CERTIFICAT AYANT SIGNE LE PRESENT DOCUMENT