Titre du document : Politique de signature des formulaires pour la gestion des certificats RGS et ETSI

Auteur : Emmanuel Montacutelli

Date : 02/09/2011

Réf : DBD_Cert ID_Formulaires_Politique de signature_v1.1.doc

POLITIQUE DE SIGNATURE : FORMULAIRES RGS

Version du document :	1.1	**Nombre total de pages :**	43
Statut du document :	☐ Projet	☒ Version finale	
Rédacteur du document :	Emmanuel Montacutelli		

Liste de diffusion :	☒ Externe	☒ Interne DocuSign France	
	Public		

Historique du document :				
Date	Version	Rédacteur	Commentaires	Vérifié par
02/09/2011	1.0	EM	Passage en v1.0	JYF
16/02/2016	1.1	EM	Modification suite au rachat de TDT par DocuSign	

SOMMAIRE

AVERTISSEMENT

La présente politique de signature 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 DOCUSIGN FRANCE.

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 DOCUSIGN FRANCE 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.

1 INTRODUCTION

1.1 Présentation générale

L'Autorité de Signature (ci-après dénommée « AS ») permet de signer électroniquement des Formulaires dans le cadre de la gestion du cycle de vie de certificat RGS émis par des AC qualifiée RGS de DOCUSIGN FRANCE.

L'AS met en œuvre les services suivants :

- La Signature électronique de documents métier par un Utilisateur ;
- L'horodatage et la validation OCSP des documents métiers signés.

Dans le cadre de la PS, DOCUSIGN FRANCE permet aux Utilisateurs de signer électroniquement des documents métiers, de les transmettre par Internet et de les conserver en leur conférant la même valeur légale qu'un écrit sur support papier, en conformité avec les dispositions des articles 1316-1 et de la première phrase du second alinéa de l'article 1316-4 du Code civil.

Le présent document constitue la Politique de Signature (ci-après dénommée « PS ») de l'AS pour le service de signature décrit ci-avant.

La présente Politique de Signature de l'AS, l'ensemble des politique de certification et la Pratique de signature forme l'ensemble des documents qui permettent de garantir la valeur probante des documents signés. Si une des parties de la communauté d'utilisateur, comme définit ci-après, ne respecte pas les règles qui lui incombent et définies par ces documents, alors le document signé pourra perdre sa valeur juridique.

Le présent document définit :

- Les règles applicables aux documents à faire signer ;
- Les règles applicables à la génération de signatures électroniques de documents au format électronique ;
- Les règles qu'il est nécessaire d'appliquer lors de la vérification des signatures apposées sur les documents signés ;
- Les règles applicables pour la mise à disposition des documents signés à l'Utilisateur et leur conservation ;
- Les engagements et les limites de responsabilité des acteurs dans le cadre de l'élaboration, signature et la validation de signature ;
- Les Autorités de certification et les types de certificats de signature autorisés pour la signature et la validation de signature de document.

Les pratiques de signature exposent les mécanismes mis en œuvre pour atteindre les règles de sécurité de la présente PS, en particulier les processus que la plate-forme de confiance de l'AS emploiera pour mettre en œuvre la cinématique signature des documents.

En raison de la confidentialité d'une partie de leur contenu, les pratiques sont des documents à diffusion restreinte, ils ne sont disponibles à la consultation qu'aux personnes habilitées à en prendre connaissance. Toute demande de consultation devra être adressée à l'AS.

1.2 Communauté d'utilisateur du service de signature

La communauté d'utilisateurs de la politique de signature est constituée des entités suivantes :

- L'AS ;
- L'AE KWA ;
- L'Utilisateur ;
- Le Vérificateur.

1.2.1 L'Autorité de Signature (AS)

Désigne l'entité qui a en charge l'application de la présente Politique de signature (PS). L'AS fait apposer les signatures électroniques par des Utilisateurs (Porteur et Mandataire de Certification et/ou Représentant habilité d'Entité Légale) sur des Formulaires via le Portail web de signature de DOCUSIGN FRANCE. DOCUSIGN FRANCE est AS.

L'AS définit un niveau de sécurité concernant les certificats KWA à utiliser pour signer et identifie et/ou autorise des AC qui délivrent et gèrent des certificats conformément au niveau de sécurité requis.

L'AS a également la charge de :

- La sécurité du processus de l'élaboration des documents métiers à signer ;
- La conservation des documents signés ;
- La mise en œuvre du portail de signature sur lequel s'authentifie l'Utilisateur ;
- Le suivi juridique avec l'AE KWA ;
- La définition des identités à utiliser dans les certificats KWA et les documents métiers signés ;
- Les types de documents métiers autorisés ;
- La définition des protocoles de consentements ;
- La définition, la validation et le contrôle de la politique de signature et des pratiques associées.

1.2.2 L'AE KWA

Désigne l'une des composantes de l'IGC (ou ICP), approuvée par l'AC KWA pour enregistrer les demandes d'émission de Certificats et de révocation de Certificats, les valider ou les rejeter et gérer l'identification et l'authentification de l'Utilisateur.

L'Autorité d'Enregistrement pour les Certificats KWA est soit l'AED ayant signée un contrat d'AED avec DOCUSIGN FRANCE dans le cadre des certificats RGS émis et gères par une AC de DOCUSIGN FRANCE soit DOCUSIGN FRANCE en tant qu'AE dans le cadre des certificats RGS émis et gérés par une AC de DOCUSIGN FRANCE.

1.2.3 Utilisateur

Désigne la personne physique, identifiée dans le Certificat KWA, ayant conclue une transaction électronique et auquel est associé un numéro unique de transaction (TransNUM) indiqué dans le Certificat KWA. L'identité KWA de l'Utilisateur est reconnue et validée par l'AE KWA.

Les Utilisateurs remplissent les documents métiers (Formulaires) et les signent sur le Portail de signature de l'AS.

1.2.4 Le vérificateur

Le vérificateur est une personne physique qui a la responsabilité du processus de vérification automatique ou manuelle. Processus dont le rôle est de valider, pour le compte d'une personne morale ou un particulier, la ou les signature(s) électronique(s) d'un Document métier signé conformément à la présente PS ou d'un Fichier de preuve. Selon le résultat de l'opération de validation, le processus de vérification automatique pourra décider de l'utilisation ou non du document.

Le processus de vérification automatique procède à la validation de la signature électronique selon l'ensemble des modalités de validations prévues dans la présente politique de signature.

1.3 Utilisation de la politique de signature

Ce service de signature permet de signer seulement les documents métiers de types Formulaires utilisés dans le cadre du cycle de vie des certificats émis par une AC RGS de DOCUSIGN FRANCE.

Ces signatures permettent de conférer une valeur probante aux Formulaires signés par l'Utilisateur. Il est rappelé que la valeur juridique de la signature dépend directement des procédures d'enregistrement (identification) et d'authentification de l'Utilisateur mises en œuvre par l'AE KWA.

De même, la politique de signature est complétée par les CGU figurant dans les Formulaires.

Suite à la signature d'un Formulaire par l'Utilisateur, DOCUSIGN FRANCE crée un fichier de preuve qui est stocké chez DOCUSIGN FRANCE. Le Formulaire signé est toujours remis à l'AE KWA et l'Utilisateur peut le télécharger sur le portail de signature une fois signé.

Les signatures de l'AS et de l'Utilisateur sont directement interprétables avec un logiciel de type « Adobe Reader » car les signatures sont directement embarquées avec le document.

1.4 Identification du document

La présente PS est dénommée : « Politique de Signature Formulaires RGS ».

1.5 Gestion de la PS et des pratiques associées

1.5.1 Elaboration de la PS et des pratiques associées

La politique de signature et les pratiques associées sont rédigées et/ou approuvées par l'AS.

Les pratiques qui supportent la présente PS sont approuvées par l'AS à laquelle toute demande de renseignements est à adresser. L'AS dispose d'un comité, qui a entre autres la responsabilité de veiller à la conformité des pratiques avec la présente politique de signature.

1.5.2 Délai de préavis

L'AS informera les AE KWA et les Utilisateurs qui utilisent le Service de signature en respectant un préavis de trente (30) jours calendaires avant de procéder à tout changement de la présente politique, susceptible de produire un effet majeur sur lesdits AE KWA et les Utilisateurs. Le délai de 30 jours pourra être plus court en cas de contraintes réglementaires de place, ou des autorités de tutelle.

L'AS informera les AE KWA et les Utilisateurs qui utilisent le Service de signature en respectant un préavis de quinze (15) jours calendaires avant de procéder à tout changement de la présente politique, susceptible de produire un effet mineur sur lesdits AE KWA et les Utilisateurs.

L'AS peut modifier la présente politique sans préavis lorsque, selon l'évaluation du responsable de la politique de signature, ces modifications n'ont aucun impact sur l'AE KWA et les Utilisateurs. Toutefois l'AS de signature informera les AE KWA de la nature de la modification.

1.5.3 Forme de diffusion des avis

Dans les cas de modification soumise à préavis, l'AS avise les AE KWA et les Utilisateurs qui utilisent le Service de signature des modifications apportées à la présente PS, par tous moyens à sa convenance dont notamment le site Internet de publication de la PS et la messagerie électronique, selon la portée des modifications.

1.5.4 Point de contact

Toute demande relative à la présente PS doit être adressée à :

- DocuSign France ;
- Mr. Thibault de Valroger ;
- Contact : Director, Business Development ;
- DocuSign France – 175, rue Jean-Jacques Rousseau - 92131 Issy-les-Moulineaux Cedex – France ;
- Email: PMA-DocuSignFrance@docusign.fr ;
- Phone: (+33) (0)1 53 94 22 00 ;
- Fax: (+33) (0)1 53 94 22 01.

Toute demande de consultation des pratiques associées à la présente politique de signature devra être motivée. Cette demande est instruite en tenant compte des éléments de motivation de la demande, la transmission éventuelle aura lieu conformément aux règles de protection de l'information appliquées par l'AS.

1.6 Définitions

Authentification : Conformément au document de l'ANSSI (Authentification, Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard ou renforcé, version 1.0 du 13 janvier 2010, l'authentification est définie de la manière suivante : « L'authentification a pour but de vérifier l'identité dont une entité (personne ou machine) se réclame. Généralement, l'authentification est précédée d'une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté. En résumé, s'identifier c'est communiquer une identité préalablement enregistrée, s'authentifier c'est apporter la preuve de cette identité ».

Authentification : pour l'émission de certificat KWA, c'est une opération organisationnelle réalisée par l'AE de l'AC KWA qui consiste à vérifier l'identité qui est portée le certificat KWA. Pour l'utilisation d'un certificat, c'est une opération technique qui consiste à valider un certificat. Pour la mise en œuvre du protocole de consentement c'est l'opération qui consiste à vérifier l'identité de l'Utilisateur et s'assurer qu'il est autorisé à signer un document grâce à l'authentification réalisée par l'application utilisatrice.

Autorité de Certification (AC) : Autorité de confiance qui émet et gère des certificats électroniques et des LCR. Il est à noter que dans le cadre de la politique de signature, plusieurs autorités de certification sont utilisées pour gérer les certificats de l'AH, de l'AS, des systèmes d'état de certificats (OCSP) et des signataires.

Autorité de Certification KWA (AC KWA) : Autorité de confiance qui émet et gère des certificats KWA. DOCUSIGN FRANCE est l'AC KWA.

Autorité d'Enregistrement KWA (ou AE KWA) : Cf. § 1.2.2.

Autorité d'Enregistrement Déléguée (AED) : désigne toute personne morale, concluant un Contrat avec DOCUSIGN FRANCE, aux termes duquel elle agit à l'égard des Utilisateurs pour le compte de l'Autorité d'Enregistrement de DOCUSIGN FRANCE d'une AC RGS de DOCUSIGN FRANCE. L'AED est l'intermédiaire entre l'AE et les Utilisateurs.

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 sources de temps choisies.

Autorité de Signature (AS) : Cf. § 1.2.1.

Bi-clé : 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. Plusieurs bi-clés interviennent dans l'IGC :

- La bi-clé de signature et/ou d'authentification dont la clé privée est utilisée à des fins de signature et/ou d'authentification et la clé publique à des fins de vérification ;
- La bi-clé 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.

Calcul d'empreinte numérique : désigne le processus algorithmique qui consiste à obtenir une empreinte numérique à partir d'une donnée électronique.

Centre de production : désigne l'environnement physique et informatique (logiciels et matériels) sécurisé de DOCUSIGN FRANCE pour la mise en œuvre du portail de signature. Le centre de production est en charge des opérations techniques, en particulier cryptographiques, nécessaires entre autre au processus de signature et de gestion des documents métiers, conformément à la présente politique de signature et aux pratiques de signature définies par l'AS.

Certificat : fichier contenant la clé publique d'une entité, ainsi que d'autres informations, rendu impossible à contrefaire grâce à la signature par la clé privée de l'autorité de certification qui l'a émis [ISO/IEC 9594-8; ITU-T X.509].

Certificat d'AC : certificat pour une AC fille émis par une AC racine.

Certificat d'AC auto signé : certificat d'AC signé par la clé privée de cette même AC (certificat d'une ACR).

Certificat(s) KWA: désigne(nt) les Certificats générés à la volée par l'AC de DOCUSIGN FRANCE pour le compte d'Utilisateurs (Porteur et Mandataire de Certification et/ou Représentant habilité d'Entité Légale) qui s'authentifient suivant un login/mot de passe fourni par l'AE KWA et un Protocole de consentement, et dont la clé privée associée est utilisée pour la signature électronique de Formulaires via le Portail web de signature. Chaque Certificat KWA contient des informations telles que le nom et prénom de l'Utilisateur, ainsi que le nom de l'Entité Légale à laquelle l'Utilisateur est rattaché.

Champ de signature : désigne une zone particulière dans un document (e.g au format PDF) dans laquelle pourront être positionnés les éléments visuels constituant la représentation de la signature électronique dans le document.

Chemin de certification (ou chaîne de confiance, ou chaîne de certification)**:** chaîne constituée de multiples certificats nécessaires pour valider un certificat. Il est à noter que dans le cadre de la

politique de signature il y a plusieurs chemins de confiance à prendre en compte qui sont les chemins de certification qui servent pour la validation des signatures, des contremarques de temps et des systèmes d'état de certificats (OCSP) apposés sur les Formualires.

Clé privée : clé de la bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

Clé publique : clé de la bi-clé asymétrique d'une entité qui peut être rendue publique. [ISO/IEC 9798-1].

Conditions Générales d'Utilisation (ou **CGU**) : désignent les conditions juridiques édictées par DOCUSIGN FRANCE, relatives à l'utilisation des Certificats RGS par les Utilisateurs, et les obligations et responsabilités des Utilisateurs. Ces CGU sont intégrées aux Formulaires. La signature desdits Formulaires vaut acceptation sans réserve par les Utilisateurs des CGU et de la Politique de Signature.

Contremarque de temps : désigne la donnée qui lie une empreinte numérique, par exemple l'empreinte numérique d'un document, 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.

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

Demande de Certificats : désigne toute demande d'émission ou de renouvellement de Certificats effectuée et signée par le Porteur, signée par le Représentant Habilité de l'Entité légale du Porteur ou le cas échéant son Mandataire de certification, puis vérifiée et contresignée par l'AE KWA, avant d'être transmise auprès de l'AE de DOCUSIGN FRANCE pour validation ou rejet.

Document électronique : désigne un ensemble de données structurées (contenu du document plus les méta-données associées) pouvant faire l'objet de traitement informatique par les applications informatiques.

Document électronique métier : désigne un document électronique sous un format PDF crée par DOCUSIGN FRANCE, complété par l'Utilisateur et qui sera signé par l'Utilisateur. Dans le cadre de la présente PS, les Documents métiers sont des Formulaires.

Document électronique métier signé : document signé électroniquement à l'aide des logiciels du portail de signature de DOCUSIGN FRANCE.

Données d'authentification : désigne des données secrètes qui permettent à l'Utilisateur de s'authentifier auprès du Portail de Signature et d'être lié à l'identité KWA qui lui est propre. Ces données associées à un Utilisateur lui permette de mettre en œuvre sa clé privée KWA. Dans le cadre de la présente Politique de Signature la donnée d'authentification KWA est un mot de passe temporaire lié à un seul et unique Utilisateur.

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

Empreinte numérique (ou Hash, condensa ou empreinte électronique) : désigne le résultat, d'une fonction de hachage à sens unique, c'est-à-dire d'une fonction calculant la réduction d'un message de telle sorte qu'une modification même infime du message entraîne la modification du résultat obtenu et permet donc de détecter que le message a été modifié.

Entité Légale : désigne la personne morale indiquée dans la Demande de Certificat, dont l'Utilisateur est salarié, et au nom de laquelle l'Utilisateur utilise les Certificats électronique RGS au moyen de son Identité professionnelle K.Sign. Le Représentant Habilité de l'Entité légale devra signer le Formulaire de demande de Certificats. Il peut néanmoins recourir à un Mandataire de certification tant pour la phase de demande de Certificat que pour la phase de remise des Supports.

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 crées lors de la signature d'un Formulaire par un Utilisateur permettant d'assurer la validité de l'acte signé. Le Fichier de preuve est signé électroniquement par DOCUSIGN FRANCE et non modifiable permettant ainsi d'assurer la traçabilité et la preuve de la réalisation de la signature conclue en ligne et ce conformément aux procédures décrites dans la présente PS. L'Utilisateur n'accèdera pas directement aux Fichiers de preuve stockés par DOCUSIGN FRANCE. L'accès au fichier de preuve est néanmoins possible en cas de litige.

Format de document : désigne le type de codage algorithmique utilisé pour créer, modifier et visualiser un document électronique. Les documents métiers signés sont au format PDF.

Format de document signé : désigne le type de codage algorithmique utilisé pour créer, modifier et visualiser un document électronique signé et le type de signature (PDF). Un document électronique signé est constitué par :

- Les métas-données ;
- Le document électronique ;
- L'identité électronique du signataire et/ou l'identité de la personne morale du Client (en fonction de l'application utilisatrice) ;
- La (ou les) valeur(s) de (ou des) signature(s) électronique(s) apposé(es) du document (incluant les métas-données) ;
- Une contremarque de temps ;
- Une validation OCSP pour chaque signature électronique apposée.

Formulaire(s) : désigne(nt) le ou l'ensemble des formulaires (demande de certificat RGS sans MC, demande de certificat RGS avec un MC, demande de création d'un MC, demande de révocation, fabrication de support suite à la perte du Support et fabrication du support suite à la perte du code PIN) signé(s) électroniquement par l'AC de DOCUSIGN FRANCE.

Identification : processus qui consiste à récupérer un ensemble d'informations (adresse IP, non et prénom, pseudonyme, donnée biométrique, courrier électronique, …), aussi appelés données d'identification, à partir de l'identité avérée et vérifiable de l'Utilisateur afin de pouvoir définir une identité qui sera attribuée à l'Utilisateur de manière non ambiguë et univoque et qui sera portée dans le document signé.

Identité-KWA Utilisateur : ensemble d'information (nom(s) et prénom(s)) qui caractérise l'Utilisateur en tant qu'individu de tel sorte qu'il puisse être reconnu comme tel et qu'il puisse le prouver sans nulle confusion à l'aide d'une pièce d'identité officielle (passeport ou carte nationale d'identité).

IGC (Infrastructure de Gestion de Clés) : Une infrastructure de gestion de clés est l'ensemble des ressources mises en œuvre pour sécuriser les couples de clés par la génération et la gestion complète de certificats de clés publiques.

Liste de certificats révoqués (LCR) : liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides et non expirés. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués.

Mandataire de Certification (MC) : Un Mandataire de Certification est une personne physique mandatée par le Représentant Habilité de l'Entité légale du Porteur, pour agir au nom et pour le compte de cette dernière lors des demandes de certificats auprès de l'AE KWA, et de la remise des Supports de bi-clés aux Porteurs.

Métadonnée : ensemble d'informations qui caractérise le document au regard du format de document utilisé.

PDF (*Portable Document Format)* : désigne un format de fichier informatique crée 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.

Politique de Certification (PC) : désigne l'ensemble des règles, des engagements énoncés et publiés par l'AC décrivant les caractéristiques générales des services de certification et des certificats qu'elle délivre.

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 le cas échéant, identifier les obligations et exigences portant sur les autres intervenants, notamment les clients et les utilisateurs de contremarques de temps.

Politique de Signature (PS) : désigne un ensemble de règles établies par DocuSign France pour la création ou la validation d'une signature électronique via le Portail web de signature (http://www.opentrustdtm.com/PC) sous lesquelles une signature électronique peut être déterminée comme valide. Une politique de signature comprend notamment les éléments suivants : (i) l'identification d'un ou plusieurs points de confiance et des règles permettant de construire un chemin de certification entre le certificat du signataire et l'un de ces points de confiance ; (ii) les moyens à mettre en œuvre pour obtenir une référence de temps destinée à positionner dans le temps la signature numérique du signataire et les données de validation; (iii) les moyens à utiliser pour vérifier le statut de révocation de chaque certificat du chemin de certification par rapport à cette référence de temps ; (iv) les caractéristiques que doit comporter le Certificat du signataire ; (v) l'ensemble des données de validation que le signataire doit fournir ; (vi) les algorithmes cryptographiques (signature et hachage) à utiliser dans le cadre de la vérification de la signature numérique du document et des données de validation.

Politique de validation de signature : sous-ensemble de la politique de signature qui fixe les exigences techniques applicables au signataire et au vérificateur de la signature afin de pouvoir procéder à la validation de cette signature.

Portail web de signature : Portail web de signature : désigne l'interface web par laquelle le Porteur, le MC et/ou le Représentant Habilité de l'Entité Légale du Porteur accèdent, en s'authentifiant à l'aide d'un login et d'un mot de passe, pour signer électroniquement des Formulaires nécessaires à l'obtention de certificat K.Sign RGS, au moyen d'une clé privée associée à un Certificat KWA dédié et délivré suite à la saisie par l'Utilisateur d'un mot de passe qu'il a préalablement reçu par sms ou courrier électronique. Le Portail de signature envoie, par courrier électronique, le Formulaire signé à l'AE KWA pour vérification.

Le Portail web de signature permet de signer électroniquement des Formulaires et de les conserver en leur conférant la même valeur légale qu'un écrit sur support papier, en conformité avec les dispositions des articles 1316-1 et de la première phrase du second alinéa de l'article 1316-4 du Code civil.

Il est précisé que le Portail web de signature ne permet de signer électroniquement que des Formulaires signés par DocuSign France. Tout autre document sera rejeté et ne sera pas signé.

Porteur : désigne la personne physique titulaire d'un Certificat RGS délivré par une AC RGS de DOCUSIGN FRANCE agissant, soit pour le compte d'entreprises ou d'administrations avec une identité professionnelle K.Sign, soit à titre personnel avec une identité personnelle K.Sign.

L'identification et l'authentification d'un Porteur au moment de l'émission de la demande et de la remise en face-à-face relèvent de la responsabilité de l'AE KWA. Le Porteur s'engage à respecter les Conditions Générales d'Utilisation (CGU) et ses obligations vis-à-vis de l'AE KWA telles que définies dans les Politiques de Certification de l'AC RGS de DOCUSIGN FRANCE.

Pratiques de signature : dans la suite de ce document, le terme « pratiques » désigne les procédures (organisation, procédures opérationnelles, moyens techniques et humains) que l'AS et ses composantes appliquent dans le cadre de la fourniture des services de signature et en conformité avec la ou les politiques de signature qu'elle s'est engagée à respecter.

Protocole de consentement : désigne une rubrique du Formulaire de demande de certificat par laquelle le Porteur atteste sur l'honneur de l'exactitude et la véracité des informations qu'il a fournies, de son engagement de signature, et de l'acceptation sans réserve des CGU de DocuSign France. Un protocole de consentement précise en outre l'ensemble des règles à savoir (i) la définition des actions à réaliser par le Porteur pour signer le document qu'il dépose lui-même sur le Portail web de signature (saisie d'un mot de passe reçu par SMS ou par courrier électronique), (ii) les modalités de création de l'identité (Nom, Prénom et nom de l'Entité Légale d'appartenance) de la personne.

Représentant Habilité : désigne toute personne physique disposant des pouvoirs de représenter une société de par la loi. Dans le cadre du présent contrat, une telle personne aura la faculté de procéder à des demandes d'émission, de renouvellement et de révocation de Certificat auprès de l'AE KWA au bénéfice des Porteurs qu'elle aura expressément et personnellement, ou via un MC, désignés.

Ressource cryptographique matérielle : désigne le module de sécurité matériel qui est dédié à la mise en œuvre des fonctions de signature de la plate-forme de confiance, notamment la génération, la conservation et la mise en œuvre des bi-clés KWA de signature ainsi que la génération des signatures des Documents métiers.

Signataire : désigne celui qui détient et met en œuvre le moyen de création de signature électronique et la clé privée de signature associée au certificat nécessaire à la validation de la signature.

La société DOCUSIGN FRANCE est signataire :

- Au nom de l'Utilisateur : pour la signature des Formulaires avec la clé privée du certificat KWA et suivant le protocole de consentement définit par l'AS ;

- Au nom de DOCUSIGN FRANCE : pour la signature du fichier de preuve élaboré par DOCUSIGN FRANCE.

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 physique ou morale qui l'appose et de manifester le consentement de la personne morale aux obligations qui découlent du document signé. Techniquement, le terme signature électronique représente la valeur de l'opération de mathématique effectuée sur l'empreinte d'un document (incluant les métas-données) à l'aide d'une clé privée.

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 (voir définition ci-après).

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 électronique embarquée : désigne un service ayant pour objet d'intégrer dans un document sous format PDF, la signature électronique de l'Utilisateur, et le cas échéant du Client. Ce service de signature embarquée utilise le logiciel Adobe LiveCycle Digital Signature ou le logiciel Certify.Center® hébergé chez DOCUSIGN FRANCE et s'appuie sur un certificat CDS et les services OCSP et horodatage pour signer les documents de format PDF. Cette fonctionnalité additionnelle confère ainsi au document PDF le rôle d'un original électronique (signé par les parties à l'acte) contenant l'ensemble des informations de signature (horodatage, identité du signataire et information de contrôle de validité des certificats mis en œuvre). Le document PDF devient alors autoportant, de sorte qu'il peut être conservé indépendamment par chaque partie à l'acte, et qu'il peut être visualisé et vérifié instantanément par toutes les parties au moyen du logiciel Adobe Reader (à partir de sa version 7) sur toutes les plateformes supportant ce logiciel (Mac, Linux, Windows). Dans ce cas, les Certificats de signature utilisés sont émis par l'Autorité de certification de DOCUSIGN FRANCE ayant été référencée par ADOBE dans le cadre du programme « CDS ».

Signature électronique valide : une signature électronique qui satisfait aux opérations de vérification définies dans une Politique de Signature.

Système d'état de certificats (OCSP) : Cette fonction fournit des informations signées sur l'état d'un certificat (révoqués ou valide).

Transaction électronique : désigne l'opération de signature d'un Formulaire réalisée par un Utilisateur au cours duquel un document métier est signé.

TransNUM : désigne un numéro de référence unique, composé de 64 caractères, généré par le Portail de signature permettant d'identifier une transaction électronique liée à un Formulaire sur lequel est apposée une Signature électronique par l'Utilisateur préalablement authentifié par le portail de signature.

Utilisateur : CF. § 1.2.3.

Validation de certificat : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de confiance et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC de la chaine de certification, ainsi que la vérification complète de la signature électronique de l'ensemble des AC du chemin de certification.

Validation de contremarque de temps : désigne l'action de l'utilisateur de contremarque de temps qui consiste à vérifier que la contremarque est valide. La vérification d'une signature électronique de contremarque de temps consiste en les opérations suivantes :

- Vérification de la signature de la contremarque de temps ;
- Vérification et extraction de la date et de l'heure contenues dans la contremarque de temps ;
- Identification et extraction du certificat de l'Unité d'Horodatage ayant émis la contremarque de temps ;
- Vérification que la date à laquelle la contremarque de temps a été émise est comprise dans la période de validité du certificat de l'Unité d'Horodatage ayant émis la contremarque de temps ;
- Vérification de l'état de validité du certificat de l'Unité d'Horodatage ayant émis la contremarque de temps au moment de la génération de la contremarque de temps ;
- Vérification que la date indiquée par l'AH dans la contremarque de temps est antérieure à la révocation éventuelle du certificat d'Unité d'Horodatage ayant émis la contremarque de temps.

Si l'ensemble de ces opérations est positif, alors la contremarque de temps est considérée comme valide.

Validation d'identité : consiste à vérifier que :

- L'identité portée dans le document électronique signé correspond à l'identité portée dans le certificat électronique utilisé pour la vérification de signature du document ;
- Que le certificat est signé par une AC reconnue et identifiée par l'AS dans la politique de signature pour le type de document électronique sur lequel portent la signature et la vérification.

Validation de signature d'un document signé : désigne l'ensemble des opérations de vérification suivantes effectuées par le vérificateur de la signature :

- Validation d'identité ;
- Validation de certificat ;
- Validation de contremarques de temps ;
- Vérification de signature électronique du document.

Ces opérations, si elles sont toutes valides, permettent au vérificateur d'attester que le document électronique a été signé par le signataire et/ou l'entité morale du Client souhaité.

Vérificateur : Se reporter au § 1.2.4.

Vérification de signature électronique d'un document signé : opération qui consiste à vérifier que le calcul d'empreinte effectué par le processus de vérification automatique (sous la responsabilité du vérificateur) sur le document (incluant les métas-données) correspond bien à l'empreinte obtenue à

l'aide de la clé publique contenue dans un certificat électronique et de la valeur de la signature électronique du document.

1.7 Acronymes

Pour le présent document, les acronymes suivants s'appliquent :

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
AGP	Autorité de Gestion de Preuves
AH	Autorité d'horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AS	Autorité de signature
ETSI	European Telecommunications Standards Institute
LCR	Liste des Certificats Révoqués
OCSP	Online Certificate Service Protocol
OID	Object Identifier
PC	Politique de Certification
PH	Politique d'Horodatage
PS	Politique de signature

2 DISPOSITIONS REGLEMENTAIRES ET LEGALES

2.1 Obligations

2.1.1 Obligations de l'Autorité de Signature

Dans le cadre de la présente Politique de signature, l'AS :

- Doit mettre à jour et publier la présente Politique de signature et les Pratiques de signature ;
- Publie l'ensemble des chemins de certification de références à utiliser pour valider les différentes signatures d'un Document métier ;
- Définit le contenu attendu des certificats pour l'ensemble des identités utilisées dans les Documents métiers signés ;
- Archive les versions successives de la Politique de signature et des Pratiques de signature ;
- Respecte et se conforme aux règles définies dans la présente Politique de signature et les Pratiques de signature ;
- Garantit la conformité des règles et des procédures décrites dans la Pratique de signature avec la présente Politique de signature ;
- Respecte la politique d'horodatage de l'AH ;

- Respecte l'ensemble des Politiques de certification des AC, en tant que Vérificateur de certificat et/ou Porteur, qui a délivré le certificat utilisé pour les Documents métiers signés et les Fichiers de preuves ;
- Met en œuvre le Portail de signature et fait signer le Document métier fourni par l'Utilisateur suivant le protocole de consentement choisit par l'AS ;
- Crée le Fichier de preuve associé à la transaction réussie ;
- Archive le fichier de preuve durant toute la période prévue ;
- Maintient le logiciel de lecture et de vérification des Fichiers de preuves pendant 5 ans ;
- Restitue le Fichier de preuve sur demande.
- Identifie et autorise les types de Documents métiers qu'il est possible de faire signer par l'Utilisateur ;
- Authentifie et autorise les personnes et machines qui vont créer des documents à faire signer ;
- Permet à l'Utilisateur de visualiser sur le Portail de signature le document qu'il lui propose de signer ;
- Rend disponible auprès de l'Utilisateur et du Vérificateur de manière explicite les différentes étapes à suivre pour signer et valider un Document métier ;
- Met à disposition de l'Utilisateur et du Vérificateur l'ensemble des références des logiciels à utiliser pour visualiser les documents, vérifier les signatures des documents ainsi que les conditions de conservation des documents mis en œuvre ;
- Met à disposition de l'Utilisateur et de l'AE KWA le document signé ;
- Protège les données personnelles des Utilisateurs.

2.1.2 Obligation de l'AE KWA

Dans le cadre de la présente Politique de signature, les obligations décrites ci-après s'appliquent à l'AED seulement quand une AED est utilisée par l'AE d'une AC RGS et à l'AE d'une AC RGS seulement quand cette AE n'utilise pas d'AED pour gérer des certificats au profit d'Utilisateur.

Dans le cadre de la présente Politique de signature, les obligations sont les suivantes :

- Authentifie et identifie les Utilisateurs selon les procédures définies par l'AC RGS de DOCUSIGN FRANCE ;
- Rend disponible les types de Documents métiers qu'il est possible de faire signer par un Utilisateurs ;
- Protège en confidentialité et en intégrité les informations d'authentification KWA qu'elle détient, et qu'elle fournit aux Utilisateurs, et qui servent pour l'authentification auprès du Portail de signature ;
- Informe sans délai l'AS en cas de compromission de ses données d'authentification utilisées pour l'authentification auprès du Portail de signature ;
- Respecte et se conforme aux règles définies dans la présente PS et le cas échéant quand l'AE KWA est une AED aux obligations du contrat AED ;
- Peut mettre à disposition de l'Utilisateur le Document métier signé ;
- Protège les données personnelles des Utilisateurs.

2.1.3 Obligation de l'Utilisateur

Dans le cadre de la présente Politique de signature, l'Utilisateur :

- Respecte et se conforme aux règles définies dans la présente PS qui la supporte et aux CGU émises par l'AC RGS de DOCUSIGN FRANCE qui lui incombent ;
- Protège en confidentialité les données d'authentification KWA qui lui permettent de mettre en œuvre le protocole de consentement et l'identifiant et mot de passe d'accès au Portail de signature (fournis par l'AE KWA) ;
- Alerte l'entité l'AE KWA en cas de problème lors de la mise en œuvre du protocole de consentement ;

- Alerte l'AE KWA en cas d'erreur constatée dans le document signé (mauvaise identité, contenu non conforme, …) ;
- S'assure de la sécurité du poste informatique dont il se sert pour interagir avec le Portail de signature.

2.1.4 Obligations du Vérificateur

Dans le cadre de la présente Politique de signature, le Vérificateur :

- Valide les Documents métiers signés conformément aux règles définies dans la présente Politique de Signature ;
- Respecte et se conforme aux règles définies dans la présente Politique de signature ;
- Respecte les différentes Politiques de certification en tant qu'utilisateur de Certificat ;
- Respecte la politique d'horodatage de l'AH en tant que Vérificateur de contremarques de temps.

2.2 Conformité avec les exigences légales

L'inapplicabilité d'une stipulation de la présente Politique de signature n'affecte en rien la validité des autres stipulations. En conséquence, l'ensemble des stipulations de la présente Politique de signature continueront à s'appliquer à la seule exception de la stipulation déclarée inapplicable.

Les intitulés de chaque Article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

En cas de conflit d'interprétation entre les intitulés et leur contenu, le contenu des clauses prévaudra.

2.2.1 Exonération des droits

Les exigences définies dans la présente politique de signature et ses pratiques doivent être appliquées par la Communauté d'utilisateurs telle que définie à l'article 2.2.1 dans le respect des stipulations de la présente politique de signature et des pratiques associées sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, ne soit possible.

2.2.2 Loi applicable

Les dispositions de la présente politique de signature sont régies par le droit français.

Plus particulière dans le cadre de la signature électronique et des obligations souscrites en lignes, les lois suivantes sont applicables :

- LOI n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, NOR: ECOX0200175L : notamment l'article 25 « Les obligations souscrites sous forme électronique » ;

- Loi portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique et ses articles « Art. 1316-1. - L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité » et 1316-4 « Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. » ;

- Article 1325 alinéa 5 du code civil « qu'il y ait autant d'originaux que de parties ayant un intérêt distinct (qui s'obligent) ».

2.2.3 Règlement des litiges

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.

2.2.4 Droits de propriété intellectuelle

Tous les droits de propriété intellectuelle relatifs au service de signature détenus par l'AS 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 distinctifs, 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.

2.2.5 Protection des données à caractère personnel

L'AS a mis en place et respecte des procédures de protection des données personnelles pour garantir la sécurité des informations caractérisées comme personnelles dans le cadre de signature de document.

Les Utilisateurs acceptent que les données personnelles les concernant recueillies lors de la demande de certificats fassent l'objet d'un traitement informatique aux seules fins (i) de pouvoir être authentifié et identifié par l'AE KWA et/ou le MC, (ii) de pouvoir permettre les vérifications nécessaires à la délivrance du certificat et le cas échéant à sa révocation, (iii) de pouvoir permettre la construction de l'identité K.Sign portée dans le certificat et (iv)d'apporter les preuves nécessaires à la gestion du certificat du porteur.

Les Utilisateurs sont informés que l'ensemble des informations qui sont conservées par l'AE KWA les concernant et portées dans les documents « demande de certificat », les « CGU » et la « pièce d'identité » sont transmis à l'Autorité d'Enregistrement (AE) DocuSign France dans leur intégralité. Le droit de rectification ne porte que sur ces informations et documents (hors pièces d'identité) et le certificat généré par l'AC DocuSign France.

Les Utilisateurs sont informés de leurs droits de faire rectifier les informations nous concernant dans la seule période de rétraction possible et prévu à cet effet, soit 15 jours après la réception du certificat par le Porteur. Toute modification est à adresser au information de contact fournies dans le formulaire.

Les utilisateurs sont informés que le fait de s'opposer à leur conservation empêche de fait d'obtenir un certificat et rend ainsi caduque la demande de certificat. Les Utilisateurs sont informés qu'en procédant à une demande de certificat via le Portail de signature, ils acceptent de fait que les données soient conservées aux seuls fin de traitement prévues à cet effet et ce pendant une période de 5 ans.

Pour toute autre information, les Utilisateurs peuvent s'adresser au Correspondant Informatique et Libertés de DocuSign France dont les informations de contact sont données dans le formulaire.

Les infractions aux dispositions de la loi Informatique et Libertés du 6 janvier 1978 sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

2.2.6 Effets de la résiliation et survie

La fin de validité de la présente Politique de signature, en cas de cessation du service de signature de l'AS, entraîne la cessation de toutes les obligations de l'AS au titre de la politique en question. Toutefois, les obligations de l'AE KWA ne sont pas impactées par la fin de validité de la présente Politique de signature.

2.3 Garantie et limite de responsabilité

La présente Politique de signature ne traite que le cas de la signature de Documents métiers signés et gérés par l'AE KWA et DOCUSIGN FRANCE conformément à la présente Politique de signature.

L'AS ne saurait être tenue responsable en cas de validation de signature électronique d'un Document métiers signés avec un certificat qui est déclaré révoqué à l'AC mais non encore pris en compte au niveau de la CRL émise par l'AC. Le Vérificateur doit appliquer une période de précaution et procéder à des vérifications auprès des AC impliquées et de l'AS afin de valider un Document métier signé.

Seules les entités de la communauté d'utilisateurs (Cf. § 1.2) impliquées dans le service de signature peuvent rechercher la responsabilité de l'AS au titre du service de signature.

En aucun cas, l'AS ne sera responsable des dommages indirects ou consécutifs subis par la personne physique ou morale qui serait victime, tel que notamment perte de clientèle, perte de chance, perte d'exploitation, manque à gagner, perte de bénéfices, etc ...

La responsabilité de l'AS ne saurait être engagée en cas de force majeure, ou de cas fortuit qui échappent raisonnablement à son contrôle.

Dans le cas où la responsabilité de l'AS serait retenue, il est expressément convenu que l'AS ne serait tenue à réparation que des dommages directs certains et immédiats, dans la limite d'un montant qui ne saurait excéder le montant annuel des prestations précisé dans la ou les convention(s) et/ou les contrats conclu entre avec chacune des entités de la communauté d'utilisateur.

Ces garanties sont exclusives de toute autre garantie de l'AS dans le cadre du service de signature.

Chaque partie impliquée dans le service de signature s'interdit de prendre un engagement au nom et pour le compte de l'autre partie à laquelle elle ne saurait en aucun cas se substituer.

A ce titre, DOCUSIGN FRANCE n'est aucunement responsable de :

- La signature électronique du Formulaire par un tiers non autorisé, résultant de la divulgation, directe ou indirecte, volontaire ou involontaire, par l'Utilisateur de ses données d'authentification KWA ;

- La perte ou vol du téléphone sur lequel l'Utilisateur a reçu le SMS, ou la destruction par l'Utilisateur du SMS contenant la donnée d'authentification KWA ;

- L'Utilisation par un tiers autre que l'Utilisateur de l'adresse de courrier électronique à laquelle l'Utilisateur a reçu la donnée d'authentification KWA, le vol, ou la destruction du courrier électronique contenant la donnée d'authentification KWA.

Il est en outre précisé que la Signature électronique des Formulaires par les Utilisateurs, n'acquiert de valeur juridique, eu égard au RGS, que par les vérifications qui sont effectuées par l'AE KWA.

2.4 Publication d'information

Les informations suivantes sont publiées :

- Politique de signature : https://www.opentrustdtm.com ;
- Informations pour les certificats utilisés par les applications utilisatrices (KWA) :
    - Certificats du chemin de confiance : https://www.opentrustdtm.com ;
    - Politique de certification de l'AC : https://www.opentrustdtm.com ;

- Informations pour les certificats utilisés par l'AH :
    - Certificats du chemin de confiance : https://www.opentrustdtm.com ;
    - Politique de certification de l'AC : https://www.opentrustdtm.com ;

- Information sur l'horodatage :
    - Politique d'horodatage de l'AH : https://www.opentrustdtm.com.

3 ELABORATION DU DOCUMENT METIER (FORMULAIRES)

3.1 Type de document métier éligible à la signature

C'est DOCUSIGN FRANCE qui détermine les types de document métiers (Formulaires) qui peuvent être signé par les Utilisateur en fonction de l'AE de l'AC KWA dont ils dépendent.

DOCUSIGN FRANCE tient à jour une liste des types de documents métiers qui peuvent être signés en utilisant les services de l'AS pour les besoins des AC RGS.

Ce service de signature permet de signer seulement les documents métiers de type :

- Formulaire de demande de certificat ;
- Formulaire de création de mandat de MC.

3.2 Logiciel pour l'élaboration et l'interprétation du document métier

Le responsable d'application identifie et définit pour l'application utilisatrice le logiciel d'élaboration de document et de document signé.

Le logiciel utilisé pour l'élaboration du document métier est le logiciel Adobe PDF creator.

3.3 Format du document métier

Le responsable d'application identifie et définit pour chacune des applications utilisatrice le format de document et le format de document signé.

Les formats de document autorisés sont :

- PDF pour le document métier.

Les formats de document signés autorisés sont :

- PDF signé qui se lit et se vérifie avec le logiciel Adobe Reader version 9 au minimum.

3.4 Politique de sécurité pour l'élaboration du document métier

Les Formulaires sont élaborés par DOCUSIGN FRANCE dans des conditions qui permettent de garantir les points suivants :

- Que ce qui est vu à l'écran est bien ce qui est élaboré et produit comme document ;
- Que le document ainsi élaboré est bien celui qui est transmis et utilisable sur le portail de signature de l'AS pour signature. Les documents sont signés par DOCUSIGN FRANCE et le Portail de signature valide cette signature ;
- Que les documents sont personnalisés en fonction de l'AE de l'AC KWA afin d'identifier clairement et distinctement les différentes AE de l'AC KWA ;
- Les documents ne peuvent pas embarquer du code exécutable ;

- Que la transmission de ce document métier élaboré pour visualisation par l'Utilisateur n'altère pas son contenu et garantisse que le document élaboré et bien celui vu par l'Utilisateur et signé par l'AS (« WYSWYS » : What You See is What You Sign).

Seules les personnes autorisées peuvent élaborer les types de document métiers, et personnaliser au profit d'une AE de l'AC KWA, à utiliser dans le portail de signature. Seules des personnes autorisées de DOCUSIGN FRANCE peuvent signer les documents métiers au nom de DOCUSIGN FRANCE. Tous les documents métiers qui peuvent être utilisé dans le portail de signature sont signés par DOCUSIGN FRANCE.

Ces Documents métiers servent de trame de fond pour élaborer ensuite les documents métiers à signer (Cf. § 4.5.2).

Les Documents métiers sont transmis par DOCUSIGN FRANCE à l'AE de l'AC KWA. L'AE de l'AC KWA est responsable de la diffusion des Documents métiers (Formulaires) aux Utilisateurs.

Ces documents métiers sont ensuite remplis par les Utilisateurs afin de créer les documents métiers à signer.

4 SIGNATURE DU DOCUMENT METIER PAR L'UTILISATEUR

4.1 Remplissage des documents métiers

4.1.1 Remplissage des documents métiers : Utilisateurs

Les seules personnes qui sont amenées à remplir des documents métiers et à les faire à signer sont des Utilisateurs préalablement identifiés par l'AE de l'AC KWA.

L'Utilisateur remplit le Document métier fournit par l'AE de l'AC KWA à l'aide d'un logiciel de type Adobe Reader. L'Utilisateur remplit les documents métier sur un poste informatique de son choix. Il n'utilise pas la plate-forme du portail de signature.

Les Documents métiers remplis constituent les documents métiers à faire signer par le portail web de signature.

4.1.2 Visualisation du document métier

La première visualisation est effectuée par l'Utilisateur sur le poste informatique qu'il utilise pour remplir le Formulaire. Cette visualisation est effectuée avec le logiciel Adobe Reader.

Le portail de signature est accessible via une session protégée en SSL.

La sécurité du portail de signature permet à l'Utilisateur d'être assuré que le document visualisé (« WYSWYS » : What You See is What You Sign) est bien celui qu'il a transmis pour signature et celui qu'il pourra signer conformément aux étapes décrites dans le § 5.2. Cette visualisation est effectuée à l'aide du logiciel Adobe Reader.

4.2 Signature du document métier par l'Utilisateur

Dès que l'Utilisateur à remplit le Document métier, alors elle utilise le portail de signature de DOCUSIGN FRANCE. Pour ce faire :

- Il utilise d'abord l'identifiant et le mot de passe que lui a fournit l'AE KWA afin de se connecter sur le portail de signature de DOCUSIGN FRANCE ;

- Il saisit sur l'interface du portail de signature, son « nom » et « Prénom » tel que porté sur la pièce d'identité contenue dans le formulaire ;

- Il saisit sur l'interface du portail de signature le nom de l'Entité légale telle que portée dans le formulaire et la pièce justificative de l'existence légale de l'Entité légale ;

- Il saisit un numéro de téléphone ou une adresse de courrier électronique afin de recevoir un SMS ou un courrier électronique contenant un mot de passe temporaire ;

- Ensuite, il transmet au portail de signature le document métier à signer. Le portail de signature vérifie l'ensemble des signatures électroniques apposées sur le document signé qui lui est soumis. Si le document n'est pas signé par DOCUSIGN FRANCE, alors il ne sera pas possible d'utiliser les services du portail de signature ;

- Il reçoit par SMS ou par courrier électronique un mot de passe temporaire transmis par le portail de signature électronique ;

- L'Utilisateur visualise le document afin de s'assurer que l'ensemble des informations sont correctes. S'il s'aperçoit qu'il y a des erreurs, alors l'Utilisateur a la possibilité d'annuler l'opération de signature et donc de ne pas signer le document ;

- Si l'Utilisateur souhaite singer signer le document métier qu'il visualise sur le portail de signature, alors il indique, conformément au Protocole de consentement de l'AS, son souhait de signer le document métier proposé qu'il vient de créer (Cf. § 5.4 et § 5.5) en cliquant sur une case à cocher. L'Utilisateur est avertit par la phrase : « J'atteste sur l'honneur de l'exactitude et de la véracité de l'ensemble des éléments d'informations que j'ai fournis dans le cadre du présent formulaire ainsi que des pièces justificatives qui l'accompagnent. Je déclare avoir pris connaissance des CGU ci-dessous et les accepte sans réserve. J'accepte en outre d'utiliser la Signature Electronique à l'aide du portail web de signature mis à ma disposition par la société DocuSign France pour valider mon engagement contractuel dans le respect des modalités et conditions définies dans les CGU ».

- Il saisit le mot de passe et déclenche ainsi la signature électronique du formulaire à faire signer. Le formulaire est signé avec une clé privée associé à un certificat KWA (Cf. PC AC KWA) dont la durée de vie est de 5 minutes et qui contient les informations d'identification du porteur suivantes : Nom, Prénom et nom de l'Entité légal de la personne qui ont été saisies par la personne sur le portail de signature. Le formulaire est horodaté et possède un jeton OCSP pour le certificat KWA. L'ensemble des champs saisit par la personne sont figé et ne peuvent être modifié dans le formulaire signé ;

- Il récupère le formulaire ainsi signé en le sauvegardant sur son poste informatique.

- Le portail de signature transmet par courrier électronique le formulaire signé électroniquement à l'AE KWA.

Sur l'interface de ce portail, l'Utilisateur visualise une feuille de style qui sert à mettre en œuvre le protocole de consentement.

Suite au succès de la mise en œuvre du protocole de consentement par l'Utilisateur, le portail de signature génère une bi-clé et un certificat KWA temporaire, à partir de l'identité KWA saisie par l'Utilisateur, et signe le document pour le compte de l'Utilisateur.

L'utilisation de l'algorithme RSA 2048 avec la fonction de hachage SHA-1 est utilisée par l'AS pour signer le document métier au nom de l'Utilisateur.

4.3 Horodatage

Dans le cadre de la présente PS, le format d'un document signé requiert une contremarque de temps, qui est apposée par la plate-forme de l'AS au moment de chacune des signatures réalisées au nom de l'Utilisateur. Il y a donc une contremarque de temps apposée suite à la signature de l'Utilisateur.

La contremarque de temps est contenue dans le document métier signé.

Les dispositions relatives à la génération des contremarques de temps sont décrites dans la politique d'horodatage de l'AH DOCUSIGN FRANCE à laquelle il est fait appel.

L'utilisation de l'algorithme RSA 2048 avec la fonction de hachage SHA-1 est utilisée par l'AS pour signer les contremarques de temps apposées sur le document métier.

4.4 Etat de validité des certificats

Dans le cadre de la présente PS, le format d'un document signé requiert une validation OCSP de l'état de validité pour les certificats de l'Utilisateur. La plate-forme de l'AS procède à l'apposition des jetons OCSP auprès du service de validité des certificats de DOCUSIGN FRANCE.

Le jeton OCSP est contenu dans le document métier électronique signé.

Le jeton de validation OCSP apposé est basé sur les LCR fournies, ou informations équivalentes, par les AC de DOCUSIGN FRANCE.

L'utilisation de l'algorithme RSA 2048 avec la fonction de hachage SHA-1 est utilisée par l'AS pour signer les réponses OCSP apposées pour les certificats KWA et KWS-S de l'AS sur le document métier.

5 IDENTIFICATION ET AUTHENTIFICATION

5.1 Identités utilisées pour les documents métiers et fichiers de preuves signés

Les identités qui sont utilisées dans le cadre de la signature de document métier sont les suivantes :

- Identité KWA de l'Utilisateur : correspond au nom(s) et prénoms(s) de l'Utilisateur tels que portés sur sa carte nationale d'identité ou son passeport. Cette identité est portée dans le certificat KWA (Cf. PC KWA), dans le champ « CN » du certificat (Cf. § 10), généré au profit de l'Utilisateur au moment de la signature du document métier par l'Utilisateur ;

- Identité de l'AS : nom de la personne morale telle que portée sur un extrait de K.BIS. Cette identité est portée dans le certificat (Cf. § 10) de l'entité légale qui sert à signer le document métier.

5.2 Authentification et identification de l'Utilisateur

5.2.1 Identité KWA portée dans le certificat KWA

L'identité portée dans le certificat KWA est définit par le portail de signature, de DOCUSIGN FRANCE, à partir des données transmises par l'Utilisateur.

Cette identité KWA permet donc d'authentifier l'Utilisateur avec son identité telle que portée sur sa pièce d'identité officielle (Porteur, MC et Représentant habilité) et sur l'extrait de KBIS de la société à laquelle il appartient (Représentant habilité).

De même, l'identité KWA permet d'authentifier l'Utilisateur comme appartenant à une entité légale.

Par conséquent, l'identité KWA de l'Utilisateur portée dans le certificat KWA et dans le document métier n'a de sens, en premier lieu, que suite aux vérifications effectuées par l'AE de l'AC KWA. De même, la validité de cette identité KWA ne vaut qu'au regard des vérifications et validations effectuées par l'AE de l'AC KWA et décrites ci-après (Cf. § 6.2.2).

Ces procédures permettent toutefois de garantir l'identité de l'Utilisateur vis-à-vis, entre autres, des Utilisateurs eux même et des vérificateurs et devant les tribunaux en cas de différends qui impliqueraient d'utiliser comme preuve les documents métiers signés.

5.2.2 Vérification et validation de l'identité KWA de l'Utilisateur

L'enregistrement des identités est effectué par l'AE KWA qui collecte les formulaires. Ces formulaires contiennent la copie des pièces d'identité (passeport ou CNI ou carte de séjour seulement) des Utilisateurs de types Porteur et Mandataire de Certification. De même ces Formulaires sont accompagnés des pièces justificatives suivantes :

- Structure Administrative : Un extrait de la pièce, valide au moment de la demande, portant délégation ou subdélégation de l'autorité responsable de l'Entité Légale administrative ;

- Entreprise : Un extrait de K.BIS valide de moins de 3 mois.

L'AE KWA établit et vérifie le lien entre l'identité des Utilisateur déclarée dans les Formulaires et les Utilisateurs de la manière suivante :

- Porteur : L'AE KWA établit et vérifie le lien entre l'identité de l'Utilisateur portée dans la demande de certificat et la pièce d'identité qui lui est présentée par l'Utilisateur lors du face-à-face pour la remise du support. Cette pièce d'identité doit comporter le même numéro de série que celle contenue dans la Demande de Certificat ;

- Mandataire de certification : L'AE KWA établit et vérifie le lien entre l'identité du MC déclaré dans la Demande de Certificat et dans le Mandat et la pièce d'identité que le MC lui fournit lors de la remise en face-à-face du Support. Cette pièce d'identité doit comporter le même numéro de série que celle contenue dans la Demande de Certificat et la demande de création de Mandataire de Certification ;

- Représentant Légale : L'AE KWA vérifie (i) la cohérence entre le nom et prénom du Représentant Habilité de l'Entité Légale et la pièce justificative de l'existence légale de l'entité mentionnée dans la demande de Certificat ou le mandat du MC, (ii) la cohérence entre la dénomination sociale de l'Entité légale et la pièce justificative de l'existence légale de l'entité mentionnée dans la demande de Certificat et le mandat du MC, (iii) la cohérence entre

l'adresse physique de l'Entité Légale et la pièce justificative de l'existence légale de l'entité mentionnée dans la demande de Certificat et le mandat du MC, (iv) vérifie l'ensemble de ces informations en consultant des bases de données officielles de référence et (iv) prend contact auprès du Représentant Habilité de l'Entité Légale suivant les procédures fournies par DOCUSIGN FRANCE.

6 STOCKAGE ET MISE A DISPOSITION DU DOCUMENT SIGNE

Suite à la signature du document métier par l'Utilisateur suivant le protocole de consentement, l'AS transmet le document signé à l'AE de l'AC KWA. L'Utilisateur a la possibilité de télécharger le Document métier signé sur le portail de signature juste après l'Opération de signature. Cette récupération ne peut se faire qu'une fois et seulement en fin de signature. Le fait de quitter l'application utilisatrice empêche tout téléchargement ultérieur du document.

6.1 Conservation et archivage du document métier signé

Dans le cadre de la cinématique de signature mise en œuvre par l'AS, le document signé est conservé et utilisé par l'AE KWA et l'AE DOCUSIGN FRANCE. Le document signé est protégé en intégrité par les signatures qui sont apposées et embarquées.

Le document est conservé suivant deux périodes qui son déterminées comme suit :

- Archive vivante et intermédiaire : période qui débute de la création du certificat jusqu'à 5 ans après. Pendant cette période, le document signé est toujours disponible auprès de l'AE KWA et de l'AE DOCUSIGN FRANCE (Service Clients). L'AE DOCUSIGN FRANCE ne communique ce document qu'à l'AE KWA en cas de besoin. Le document est aussi dans les logs techniques de l'AS ;

- Archive définitive : période qui commence après la période vivante et intermédiaire. Le certificat n'est plus valide depuis 2 ans et le document signé n'existe plus que dans les logs techniques de la plate-forme. Ces logs techniques de l'AS sont conservés 5 ans de plus. Pendant cette période, le document n'est plus accessible sauf cas exceptionnel et sur demande auprès du DS de DOCUSIGN FRANCE.

6.2 Mise à disposition du document signé par l'AS

Le document métier signé est disponible sur demande auprès de l'AS dans son intégralité au seul profit de l'AE de l'AC KWA. Pour le récupérer, l'AE de l'AC KWA s'authentifie auprès de l'AS.

Cette mise à disposition du document n'est possible que pendant toute la période ou le document est classé comme archive vivante et intermédiaire. Pendant la période d'archive définitive, alors le document métier correspondant n'est plus rendu disponible par l'application utilisatrice au profit de l'Utilisateur. Il est toutefois toujours conservé dans la plate-forme de l'application.

Il est à noter que si l'Utilisateur imprime le document métier signé électroniquement, alors le document ainsi imprimé n'a aucune valeur juridique. Seul le document métier signé électroniquement a une valeur légale.

7 VALIDATION ET UTILISATION DE DOCUMENT SIGNÉ

La validation d'un document consiste à valider techniquement les signatures de l'AS, de l'Utilisateur, de l'AH et de l'OCSP, les identités et les vérifications propres au contenu du document métier.

Les conditions pour le vérificateur afin qu'il vérifie les documents signés sont les suivantes :

- Utilisation du logiciel Adobe Reader PDF version 9 minimum ;
- Utilisation du service de validation de contenu de document (Cf. § 7.3) disponible auprès de l'application utilisatrice ;
- Utilisation des règles de validation à mettre en œuvre et décrites dans le chapitre 8 ;
- Utilisation des certificats d'AC disponibles publiés et référencés dans la présente PS (Cf. § 3.6) afin de pouvoir valider les signatures électroniques.

7.1 Validation des signatures AS et Utilisateur

La vérification de signature nécessite le respect des étapes suivantes par le vérificateur :

- Obtenir la politique de signature appliquée pour la génération des signatures à vérifier ;
- Vérifier que la politique de signature appliquée est la politique de signature de l'AS ;
- Vérifier que le contexte de vérification des signatures (y compris AH et OCSP) est conforme à la politique de signature de l'AS ;
- Consulter auprès de l'AS les certificats racines reconnus pour valider les signatures des documents ;
- Vérifier la validité de l'ensemble des certificats utilisés pour la signature du document :
    - Valider les certificats des chemins de certification auxquels ils appartiennent ;
    - Vérifier que la politique de certification selon laquelle le certificat a été émis s'applique au contexte de la vérification ;
    - Consulter auprès de l'AS et de l'AGP les certificats racines reconnus pour valider la signature ;
- Vérifier la contremarque de temps :
    - Vérifier que la politique d'horodatage selon laquelle a été émise la contremarque de temps qui accompagne la signature s'applique au contexte de la vérification ;
    - Consulter auprès de l'AS les certificats racines reconnus pour valider la contremarque de temps ;
- Vérifier la réponse OCSP :
    - Vérifier que la politique de validation de certificat selon laquelle a été émise la réponse OCSP qui accompagne la signature s'applique au contexte de la vérification ;
    - Consulter auprès de l'AS les certificats auto-signés reconnus pour valider la réponse OCSP.

Les documents métiers signés sont émis par l'AS avec un statut « valide » d'un point de vue vérification de signature complet (AS, Utilisateur, AH et OCSP). C'est-à-dire que les certificats utilisés sont tous valides au moment de leur utilisation.

Les certificats de l'AS et de l'Utilisateur sont confirmés par un jeton OCSP. Par conséquent, la validation d'un document avec le logiciel Adobe Reader version 9 donnera toujours une vérification des signatures de l'AS et de l'Utilisateur valide.

Lorsque c'est Adobe Reader version 9 qui est utilisé pour valider un document métier signé alors il faut qu'il soit mise à jour pour la banque de confiance d'AC autorisées (celles utilisées par DOCUSIGN FRANCE pour signer les certificats, les contremarques de temps et les jetons OCSP). Cette mise à jour s'effectue en utilisant le menu d'Adobe Reader. Pour ce faire, dans la barre de menu d'Adobe Reader, il faut allez dans le menu « Edition\Préférences\Gestionnaire des approbations\ » et cliquer sur « Chargés les certificats racine approuvés à partir d'un serveur Adobe (pas d'envoi d'informations personnelles) puis cliquer sur « Mettre à jour ».

Il incombe donc au Vérificateur, en cas de doute, de s'assurer qu'il n'y a pas de changement dans le statut des certificats utilisés auprès de l'AS comme expliqué ci-dessus.

7.2 Utilisation d'un document signé

Le document signé au format PDF est autoportant et vérifiable avec un logiciel de type Adobe Reader, version 9 minimum. Pour la vérification il est nécessaire d'utiliser un logiciel Adobe Reader version 9 minimum.

Un document contient des engagements dont la réalisation, et la contestation possible, ont une durée. Cette durée peut être soit :

- Inférieure à la durée de validité des certificats utilisés ;
- Supérieure à la durée de validité des certificats utilisés.

Il donc important de distinguer ces deux périodes pour la validation d'un document signé. Les mesures à prendre par le responsable d'application pour permettre la validation d'un document sont dépendantes de ces 2 périodes.

Les documents signés sont conservés par l'AS. Par conséquent, les données de validation (certificats, signatures, …) sont aussi archivées et conservées.

7.2.1 Pendant la période de validité des certificats

Les documents signés sont vérifiables pendant la période de validité des certificats utilisés à l'aide des informations fournies par l'AS et utilisées et du logiciel Adobe Reader version 9 minimum.

L'AS tient à jour les informations qui permettent de valider les différentes signatures, contremarques de temps et jetons OCSP.

L'AS ne tient à jour que les informations pour des certificats en cours de validité mais pas pour des certificats expirés.

L'AS ne tient à jour que des informations portant sur le contenu du document et les identités portées dans les certificats.

Le document signé peut donc être utilisé comme tel sans autre forme de traitement par un Vérificateur. Il est en général en état d'archive courante ou intermédiaire.

7.2.2 Après la période de validité d'un ou des certificats

Suite à la fin de la validité de tous les certificats utilisés pour un document signé, l'AS ne s'engage plus sur les informations nécessaires à la validation de la signature de ce même document signé.

L'AS s'engage toutefois sur l'intégrité du document signé et des données de validation associées tant qu'ils sont conservés par elle. L'intégrité du document signé et des données de validation associées est assurée par les mécanismes mis en œuvre par l'AS.

Normalement, pendant cette période le document métier est dans un état « archive définitive ».

Il est à noter que les documents signés sont tout de même techniquement vérifiables après la période de validité des certificats utilisés à l'aide des informations fournies par l'AS et des informations fournies par les AC utilisées et du logiciel Adobe Reader version 9 minimum.

Si à cause des évolutions technologiques, le logiciel Adobe Reader ne permettait pas de vérifier les signatures, alors le Vérificateur pourra demander une vérification des signatures d'un document à l'AS.

7.3 Vérification des identités

L'authentification au sens de la présente PS consiste à décrire les moyens qui permettent de vérifier l'ensemble des identités portées dans le document signé. Ces identités sont vérifiables à l'aide de certificats électroniques délivrés par les AC référencées dans la présente PS.

La vérification des identités est effectuée à partir des seuls certificats KWA. Il est rappelé que l'identité de l'Utilisateur est crée et vérifiée suivant des procédures qui sont définies par l'AE KWA (Cf. § 5). Les règles décrites au § 5 permettent de s'assurer du niveau de sécurité, et donc du niveau d'acceptation, de l'identité portée dans le certificat KWA pour l'Utilisateur.

7.3.1 Document métier signé

7.3.1.1 AH

Les certificats de l'AH de l'Utilisateur portent des identités définies comme suit :

Champ de base	Valeur
Issuer (identifie l'AC émettrice)	cn=KEYNECTIS CDS CA ou=KEYNECTIS for Adobe o=KEYNECTIS c=FR
Subject (identifie l'AH)	cn=KEYNECTIS TSA for CDS ou=KStamp for Adobe CDS o=KEYNECTIS c=FR

La durée de vie du certificat est d'au moins 5 ans.

L'utilisation de l'algorithme RSA 2048 avec la fonction de hachage SHA-1 est utilisée pour l'AC.

L'utilisation de l'algorithme RSA 2048 avec la fonction de hachage SHA-1 est utilisée pour l'AH pour les contremarques de temps.

7.3.1.2 Certificat de l'Utilisateur (KWA) : identité KWA

Les certificats KWA de l'Utilisateur portent des identités définies comme suit :

Champ de base	Valeur
Issuer (identifie l'AC émettrice)	cn=KEYNECTIS K.Websign CDS ou=KEYNECTIS for Adobe o=KEYNECTIS

	c=FR
Subject (identifie l'Utilisateur)	email=<adresse de courrier électronique de l'Utilisateur> cn=<nom et prénom de l'Utilisateur> ou=<nom et prénom de l'entité légale de l'Utilisateur> ou=<nom de l'AE KWA> ou=<TransNum> ou=<nom de l'AE KWA> o=KWEBSIGN c=FR

La durée de vie du certificat est de 5 minutes.

L'utilisation de l'algorithme RSA 2048 avec la fonction de hachage SHA-1 est utilisée pour l'AC.

7.3.1.3 Certificats d'AH : date et heure de signature de l'Utilisateur

Les certificats de l'AH de l'Utilisateur portent des identités définies comme suit :

Champ de base	**Valeur**
Issuer (identifie l'AC émettrice)	cn=KEYNECTIS CDS CA ou=KEYNECTIS for Adobe o=KEYNECTIS c=FR
Subject (identifie l'AH)	cn=KEYNECTIS TSA for CDS ou=KStamp for Adobe CDS o=KEYNECTIS c=FR

La durée de vie du certificat est d'au moins 5 ans.

L'utilisation de l'algorithme RSA 2048 avec la fonction de hachage SHA-1 est utilisée pour l'AC.

L'utilisation de l'algorithme RSA 2048 avec la fonction de hachage SHA-1 est utilisée pour l'AH pour les contremarques de temps.

8 EXIGENCES PHYSIQUES ET ENVIRONNEMENTALES, PROCÉDURALES ET ORGANISATIONNELLES

8.1 Exigences physiques et environnementales

L'ensemble des opérations de génération et de délivrance des signatures par les plates-formes au titre de la présente PS sont réalisées au sein des locaux sécurisés du centre de production, par des personnels habilités.

En particulier :

- L'accès physique aux équipements concernés par la plate-forme est limité aux personnels autorisés ;
- Des moyens de prévention et des contrôles sont mis en œuvre pour éviter la perte, des dégâts ou la compromission de bien sensibles et l'interruption des activités ;
- Des moyens de préventions et des contrôles sont mis en œuvre pour éviter la compromission ou le vol d'informations ou d'équipements informatiques ;
- Les installations d'infrastructures sont bâties, installées et mise en œuvre de telle manière que les systèmes se voient fournir les informations et éléments nécessaires à leur bon fonctionnement dans le respect les conditions d'engagement de service de signature.

La politique de sécurité physique et environnementale du centre de production pour les systèmes concernés par la gestion de la plate-forme concerne au minimum le contrôle d'accès physique, la protection vis à vis des catastrophes naturelles, les facteurs de sécurité liés au feu, la défaillance des services de base (par exemple le secteur, les télécommunications), l'écroulement de la structure, des inondations ou suintement, la protection contre le vol, la casse et l'intrusion. En outre le maintien et le rétablissement de la sécurité après un désastre fait l'objet d'une attention particulière.

8.2 Exigences procédurales

L'ensemble des opérations menées par la plate-forme sont soumises au respect de la politique de sécurité du centre de production, ainsi que de l'ensemble des politiques et procédures qui s'y rattachent.

En particulier, font l'objet d'une attention toute particulière pendant toute la durée de vie des documents :

- Les informations et supports d'informations nécessaires à la bonne conduite des opérations des plates-formes ;
- Les informations confiées au centre de production à des fins de délivrance de ses services de signature, notamment les informations à caractère personnel ;
- La mise en œuvre des matériels nécessaires à la conduite des opérations de mise à la clé des plates-formes de signature ;
- Les personnels en charge de la conduite des opérations de gestion de clés ;
- Le centre de production a dans cette optique adopté une organisation avec séparation des rôles.

Le comité des politiques de sécurité du centre de production est supporté par une entité interne d'audit afin de vérifier la bonne application de la PS et des pratiques supportant la présente politique. Cette entité d'audit a notamment pour rôle d'identifier toute information de nature à mettre en évidence les non-conformités éventuelles et les évènements de sécurité, ainsi que de faire procéder aux vérifications nécessaires et corrections éventuelles.

En complément de ces mesures et afin d'assurer un fonctionnement cohérent, sûr et auditable de la plate-forme de confiance, celle-ci s'engage à ce que soient formalisées et respectées les règles internes relatives à :

- La mise en place, le fonctionnement et la maintenance des systèmes ;
- La protection et le service des systèmes ;
- La prise en compte des incidents et la mise en œuvre des mesures nécessaires à en limiter les impacts sur le service de signature ;
- La traçabilité des évènements ;
- Les rôles et responsabilités des personnes en charge des opérations ;
- La mise en œuvre et le contrôle d'accès aux systèmes et installations.

8.2.1 Manipulation et sécurité des supports

Les supports d'information utilisés dans le cadre de la délivrance du service de signature font l'objet d'un suivi qui tient notamment compte du niveau de sensibilité des informations qu'ils renferment.

Le cycle de vie des supports contenant des informations sensibles est soumis au respect des procédures qui sont précisés dans les pratiques. Seuls les personnels habilités du centre de production et dûment affectés aux rôles de confiance ont accès à ces supports.

8.2.2 Planification de Système

Les charges de la plate-forme sont contrôlées et des projections de charge dans le futur sont effectuées pour garantir que des puissances de traitement nécessaires, les stockages adéquats et les engagements de services sont disponibles et atteints.

8.2.3 Rapport d'incident et réponse

Le traitement des incidents est assuré au sein du centre de production afin de centraliser la prise en compte, le suivi des incidents et la communication auprès des entités concernées.

Chaque incident est clairement identifié, est affecté à une entité du centre de production et fait l'objet d'une fiche de suivi. En fin de traitement, l'incident est clos si la vérification est faite que les systèmes de la plate-forme sont revenus dans une configuration normale de fonctionnement.

Les interventions correctives sur les systèmes des plates-formes font également l'objet de fiches de traitement. Les détails du processus de traitement des incidents sont précisés dans les pratiques de signatures.

8.2.4 Procédures de fonctionnement et responsabilités

Les opérations de sécurité sont séparées des autres opérations.

Les opérations de sécurité incluent :

- Les procédures opérationnelles et les responsabilités ;
- La gestion des clés ;
- La protection vis-à-vis des codes logiciels malveillants ;
- La maintenance ;
- La gestion du réseau ;
- Le contrôle actif des journaux d'audit, l'analyse des événements et les suites à donner ;
- Le traitement et la sécurité des médias.

Ces opérations sont gérées par du personnel habilité et dûment désigné du centre de production, selon les règles relatives au partage des rôles et des responsabilités au sein du centre de production.

8.2.5 Gestion d'Accès au Système

Seuls les personnels habilités et dûment désigné de centre de production ont accès aux plates-formes. Les accès sont donnés au regard des rôles qui leurs sont confiés.

L'accès aux fonctions du système, à l'information et aux applications est limité conformément à la politique de contrôle d'accès. Les plates-formes possèdent des contrôles informatiques de sécurité qui permettent la mise en œuvre de la séparation des rôles de confiance identifiés. En particulier, l'utilisation de programmes systèmes utilitaires est limitée et très contrôlée.

Le personnel du centre de production est identifié et authentifié avant de pouvoir utiliser des applications critiques liées au service de signature. Le personnel du centre de production est tenu responsable de ses activités et est soumis au règlement du centre de production.

Une surveillance des équipements de sécurité est maintenue pour permettre au centre de production de détecter, d'enregistrer et de réagir rapidement à n'importe quelle tentative non autorisée et/ou irrégulière d'accès à ses ressources.

8.2.6 Déploiement et Maintenance

Le déploiement des plates-formes est contrôlé et fait l'objet d'enregistrement et fiches. Une politique de gestion de la configuration et des changements s'applique aux plates-formes de confiance.

Les détails des principes et procédures appliqués sont donnés dans les pratiques.

8.3 Exigences organisationnelles

Afin de garantir le bon fonctionnement et la sécurité de ses opérations pour le service de signature, le centre de production met en œuvre une politique d'habilitation des personnels impliqués dans la réalisation des tâches de définition, création, installation, administration, support et maintenance, audit, application et gestion de la sécurité, liées au fonctionnement des plateformes de confiance. Cette politique se traduit notamment par le respect d'une politique d'habilitation des personnels du centre de production aux rôles de confiance.

La mise en place de profils de personnels pour les rôles de confiance, de principes de répartition des rôles et responsabilités, ainsi que du double contrôle complète ce dispositif. Les politiques et procédures opérationnelles permettent non seulement de définir les principes applicables, mais aussi de détailler les rôles et opérations de chacun dans la délivrance des services de signature.

Le centre de production emploie un personnel qui possède l'expertise, l'expérience et les qualifications nécessaires pour les services offerts. Le personnel applique la PS et les pratiques, pour les parties qui le concernent, conformément à la politique de sécurité du centre de production.

Les rôles de confiance et les responsabilités, comme spécifié dans la politique de sécurité du centre de production, sont documentés dans des descriptions de poste. Les rôles de confiance, sur lesquels la sécurité du fonctionnement de la plate-forme repose, sont clairement identifiés. Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes :

- Les responsables de la sécurité : responsabilité complète d'administrer la mise en œuvre des pratiques de sécurité ;
- Les personnels d'administration : autorisés à installer, configurer et maintenir les services de signature ;
- Les personnels d'exploitation : responsables pour faire fonctionner la plate-forme de signature de manière quotidienne. Autorisés pour effectuer les opérations de sauvegarde et de secours ;

- Les personnels contrôleurs : autorisés à consulter les archives et les fichiers d'audit et journaux liés au fonctionnement du service de signature.

Le personnel lié aux services de la plate-forme est formellement nommé aux rôles de confiance par le centre de production.

Le centre de production ne nomme pas aux rôles de confiance ou de gestion une personne connue pour avoir eu une condamnation pour un crime sérieux ou une autre infraction qui affecte son adéquation avec la position. Le personnel n'a pas accès aux fonctions de confiance avant que les contrôles nécessaires ne soient achevés par le centre de production.

8.4 Journalisation et archivage

Les journaux d'évènements relatifs aux services sont régulièrement enregistrés puis archivés par le centre de production et conservés pendant une période de temps précisée dans les pratiques, notamment dans le but de fournir des éléments de preuve en cas de litige ou en cas d'enquête judiciaire. Toute demande en ce sens est à adresser à l'AS.

Une datation est fournie pour chacun de ces évènements ainsi que l'identification de l'entité ayant déclenché ou réalisé l'évènement, ainsi que le résultat obtenu.

Les informations enregistrées et archivées sont conservées dans des conditions de nature à en assurer la confidentialité et l'intégrité.

La liste détaillée des évènements est précisée dans les pratiques.

Les événements sont enregistrés de telle façon qu'ils ne puissent pas être facilement supprimés ou détruits (sauf s'ils sont transférés sur un support de sauvegarde) durant la période de temps où l'on exige qu'ils soient conservés.

8.4.1 Evènements liés à la mise en œuvre d'une plate-forme

Font l'objet de cette collecte d'information les informations suivantes :

- Tous les événements liés à la mise en œuvre des moyens sur lesquels l'AS s'appuie pour générer et délivrer des signatures électroniques, depuis leur mise en marche jusqu'à leur arrêt définitif ;
- Tous les évènements liés à la mise en œuvre des services de la plate-forme ;
- L'ensemble des dossiers élaborés pour identifier les Utilisateurs (Cf. § 4.2.1 et 4.2.2).

8.4.2 Evènements liés à la gestion des clés de la plate-forme de signature de l'AS

Les enregistrements concernant tous les événements touchant au cycle de vie des clés de signature (personne morale) sont effectués.

Les enregistrements concernant tous les événements touchant au cycle de vie des certificats des plates-formes de confiance sont effectués.

8.4.3 Durée de conservation

La durée de conservation des journaux est de 5 ans en droit commercial (archive vivante et intermédiaire).

Les archives sont protégées en confidentialité et en intégrité.

8.4.4 Archivage

Les journaux sont archivés pendant une période de 5 ans (archive définitive).

Les archives sont protégées en confidentialité et en intégrité.

8.5 Compromission et plan de continuité

Le centre de production informe les entités impliquées dans le service de signature des d'événements qui affectent la sécurité des services de la plate-forme.

Le plan de secours développé par l'AS traite le cas de la compromission réelle ou suspectée de la clé privée de signature de la plate-forme qui héberge le module TransID® et de compromission de la plate-forme.

Dans le cas d'une compromission, réelle ou suspectée, la génération de signature à l'aide de la plate-forme de confiance en question est arrêtée. La reprise de la génération de signature ne sera autorisée que lorsque l'ensemble des conditions normales d'exploitation sera restauré.

En cas d'un évènement majeur dans le fonctionnement de la plate-forme qui affecte des documents signés, l'AS met à la disposition des vérificateurs et de chacune des entités de la communauté d'utilisateurs les informations permettant d'identifier les documents signés qui pourraient avoir été affectées, à moins que cela ne contrevienne au respect des règles de protection de la vie privée des personnes physiques associée aux données électroniques ou à la sécurité des services de signature. Des détails sur les moyens prévus par l'AS sont donnés dans les pratiques de signatures.

8.6 Fin d'activité

L'AS s'engage à informer les entités impliquées dans le service de signature, avec un préavis d'au moins 6 mois, de sa décision d'arrêter ses activités de délivrance de signature.

Avant que l'AS ne mette fin au service de signature, elle ;

- Met fin aux éventuelles autorisations données à des sous-traitants dans l'exécution d'une des fonctions relatives au processus de génération de signature ;
- Transfère à une entité que l'AS désigne ses obligations de maintien des fichiers d'audit et des archives nécessaires à démontrer son fonctionnement correct pour assurer le respect des modalités prévue, si elle ne les maintient pas elle-même ;
- Demande à l'AC la révocation de ses certificats délivrés (de personnes morale pour les applications) dans le cadre du service de signature ;
- Détruit les clés privées de telle façon que ces clés ne puissent pas être recouvrées.

L'AS indique dans les pratiques de signature les dispositions précises prises pour assurer la fin du service de signature.

8.6.1 Transfert d'activité

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AS :

- Met en place des procédures dont l'objectif est d'assurer un service constant en respectant des clauses de continuité de service.

9 EXIGENCES DE SECURITE SUR LES CLES DE SIGNATURE DES UTILISATEURS

9.1 Génération des bis-clés de signature de l'Utilisateur

La génération des clés d'un porteur KWA est effectuée par l'AS dans un module cryptographique matériel (HSM) suite à la saisie d'informations et d'actions définies dans le protocole de

consentement de l'AS. La génération de la bi-clé est effectuée suite à l'accord de l'Utilisateur de vouloir signer électroniquement le document (Cf. § 4.2).

9.2 Certification des bi-clés de l'Utilisateur

L'Utilisateur est à l'origine de la demande de certificat. Cette demande se déclenche lors de la mise en œuvre du Protocole de consentement par l'Utilisateur. La mise en œuvre du Protocole de consentement déclenche la génération de la bi-clé et sa certification par l'AC. Ensuite, le processus de signature par l'AS au nom de l'Utilisateur est déclenché.

9.3 Gestion de la durée de vie des clés privées et du certificat de l'Utilisateur

Le certificat KWA de l'Utilisateur a une durée de vie de 5 minutes. Il n'existe donc pas de mécanisme de révocation pour un certificat KWA.

9.4 Protection des clés privées de l'Utilisateur

La clé privée de l'Utilisateur est générée, utilisée et détruite dans le HSM de l'AS.

9.5 Exigences de sauvegarde des clés de l'Utilisateur

Aucune copie de clé privée ne peut être réalisée.

9.6 Destruction de clés de l'Utilisateur

Dès que la signature est apposée sur le document, suite à mise en œuvre du Protocole de consentement par l'Utilisateur, l'AS détruit la clé privée. Il n'existe plus aucunes informations permettant de retrouver la clé privée de l'Utilisateur.

9.7 Algorithmes utilisés

Dans le cadre de la présente politique de signature, les algorithmes autorisés pour la plateforme de confiance sont :

- Algorithme d'empreinte : les algorithmes et la taille des valeurs d'empreinte générées et signées sont conformes aux exigences des autorités compétentes en la matière comme par exemple [ANSSI_ALGO] :
    - L'algorithme de calcul d'empreinte numérique accepté est SHA-1 et SHA 2 ;

- Bi-clé : les algorithmes et les longueurs de clés sont conformes aux exigences des autorités compétentes en la matière comme par exemple [ANSSI_ALGO] :
    - Une bi-clé acceptée est donc au minimum une bi-clé RSA de 2048 bits.

Le choix des algorithmes doit être cohérent. Par conséquent, une contremarque de temps apposée sur un document doit utiliser un mécanisme cryptographique de même robustesse.

10 MÉCANISMES DE SÉCURITÉ DES SYSTÈMES INFORMATIQUES

10.1 Exigences techniques de sécurité des ressources informatiques

Les fonctions suivantes sont fournies par le système d'exploitation, ou par une combinaison du système d'exploitation, de logiciels et de protection physiques. La plate-forme comprend les fonctions suivantes :

- Authentification des rôles de confiance ;
- Contrôle d'accès discrétionnaire ;

- Interdiction de la réutilisation d'objets ;
- Possède des logiciels de protection contre les codes malicieux ;
- Requiert l'identification des utilisateurs ;
- Assure la séparation rigoureuse des tâches.

Ces règles sont applicables sur les machines des signataires, des applications utilisatrices et de la plate-forme de confiance.

10.2 Mécanismes de sécurité du réseau

Les composantes accessibles des plates-formes sont connectées à d'autres réseaux dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu (sauf lors des interventions de maintenance ou de sauvegarde).

Les machines utilisent des mesures de sécurité appropriées pour s'assurer qu'elle est protégée contre des attaques d'intrusion. Ces mesures comprennent l'utilisation de pare-feu. Les ports et services réseau non utilisés sont coupés.

11 CONTROLES DE CONFORMITE ET AUTRES ÉVALUATIONS

11.1 Fréquence et motifs des audits

L'AS a la responsabilité du bon fonctionnement global des services de l'application utilisatrice et de l'AS.

L'AS a la responsabilité du bon fonctionnement des composantes de la plate-forme, conformément aux dispositions énoncées dans le présent document. Elle effectuera des contrôles réguliers de conformité et de bon fonctionnement des composantes de la plate-forme.

L'AS peut déléguer au Responsable d'Application Utilisatrice le contrôle des services mis en œuvre par les applications utilisatrices dont les documents métier font l'objet de signature.

11.2 Identité / Qualification des auditeurs

Le contrôleur est désigné par l'AS.

Les auditeurs doivent démontrer leurs compétences dans le domaine des audits de conformité, ainsi qu'être familiers avec les exigences de la PS. Les auditeurs en charge de l'audit de conformité doivent effectuer l'audit de conformité comme tâche principale.

11.3 Lien entre l'auditeur et l'entité contrôlée

Dans le cas où le contrôle est effectué à la demande d'un tiers, le contrôleur est choisi selon des critères d'indépendance et d'expertise dans le domaine de la sécurité informatique.

Dans les autres cas, le contrôleur désigné pourra éventuellement être une entité d'audit experte dans le domaine de la sécurité informatique et appartenir à l'AS.

11.4 Points couverts par l'évaluation

L'objectif de l'audit de conformité est de vérifier que le centre de production opère le service de signature en conformité avec la présente PS, les pratiques et ses procédures.

11.5 Mesures prises en cas de non-conformité

En cas de non-conformité, l'AS décide de toute action correctrice nécessaire.

Selon le type de non-conformité mise en évidence, l'AS peut :

- Demander la mise en place d'actions correctives dont la réalisation sera vérifiée lors du prochain audit ;
- Demander la correction des non-conformités selon un calendrier spécifique au titre duquel un contrôle de mise en conformité sera effectué ;
- Révoquer un ou des certificats d'application utilisatrice ;
- Détruire les bi-clés de signature de l'AS.

11.6 Communication des résultats

Un rapport de contrôle de conformité, incluant la mention des mesures correctives déjà prises ou en cours par la composante, est remis à l'AS. Les non-conformités révélées durant les audits seront publiées aux responsables des entités impliquées dans le service de signature, pour lesquelles l'AS s'y oblige contractuellement.

Eu égard au caractère confidentiel de ces informations, la publication des résultats est limitée et strictement contrôlée.

12 ANNEXE 1 : DOCUMENTS CITÉS EN RÉFÉRENCE

12.1 Réglementation

Renvoi	Document
[DirSig]	DIRECTIVE 1999/93/CE DU PARLEMENT EUROPÉEN ET DU CONSEIL du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
[LCEN]	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
[LCEN]	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 25 concernant la souscription d'obligations en ligne.
[LSIGN]	Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.
[SIG]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

12.2 Documents techniques

Renvoi	Document
[ANSSI_ALGO]	Mécanismes cryptographiques, Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version du 1.2 26 janvier 2010
[ETSI_101733]	Politique de signature TS 101733