Protect and Sign: Personal Signature

Politique de Signature et de Gestion de Preuve

Emmanuel Montacutelli

15/10/2014

POLITIQUE DE SIGNATURE ET DE GESTION DE PREUVE

Version du document :	V1.4	**Nombre total de pages :**	56
Statut du document :	☐ Projet	☒ Version finale	
Rédacteur du document :	Emmanuel Montacutelli	DocuSign France	

Liste de diffusion :	☒ Externe	☒ Interne DocuSign France
	Public	

Historique du document :				
Date	Version	Rédacteur	Commentaires	Vérifié par
22/11/2013	V1.0	EM	Passage en v 1.0	
09/12/2013	V1.1	EM	Intégration plan de continuité, compromission et fin de vie de l'AGP	JYF
14/03/2014	V1.2	EM	Précision sur l'archivage temporaire et de la purge des fichiers de preuves et la sur-signature.	EM
15/10/2014	V1.3	EM	Intégration commentaires et relecture cabinet avocat.	TdV
23/01/2016	V 1.4	EM	Modification suite au rachat de TDT par DocuSign	

SOMMAIRE

AVERTISSEMENT

Le présent document est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle, 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-droits, sont strictement interdites.

En outre, l'article L.122-5 du Code de la Propriété Intellectuelle n'autorise 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.

Par ailleurs, « Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants-droits ou ayants-cause est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque. » (Article L.122-4 du Code de la Propriété Intellectuelle). Ainsi, toute représentation, modification, ou reproduction de la présente Politique de Signature et de Gestion de Preuve par quelque moyen que ce soit constituerait une contrefaçon, sanctionnée notamment par les Articles L. 335-3 et suivants du Code de la Propriété Intellectuelle.

1 INTRODUCTION

1.1 Présentation générale de la Politique de Signature et de Gestion de Preuves

Ce document constitue la Politique de Signature et de Gestion de Preuve (PSGP) associée au Service « Protect and Sign (Personal Sign) » (ci-après appelé le Service) que la société DOCUSIGN FRANCE fournit à ses Clients.

Le service Protect and Sign (Personal Sign) est couvert par la présente PSGP. La présente PSGP s'applique aux services de signature dont les descriptions et OID sont précisés au paragraphe 1.2 ci-dessous. Deux niveaux de services Protect and Sign (Personal Sign) existent, les spécificités du niveau présentant le plus de fonctionnalités sont identifiées par l'indication (V4) dans la suite de la présente PSGP.

Les services de signature du service K-Websign, dont « Protect and Sign (Personal Sign) » est une évolution, sont couverts par les Politiques de Gestion de Preuve (PGP) publiées par DocuSign France sur son site internet dans la rubrique « Politiques de certification \ Protect and Sign (anciennement K-Websign®) PGP.

La présente PSGP décrit les règles que DocuSign France, ses Clients et les Utilisateurs doivent respecter pour signer électroniquement des Documents métier et constituer et conserver des Fichiers de preuves relatifs aux Transactions électroniques réalisées entre eux, afin d'être en mesure de démontrer ultérieurement l'existence et l'intégrité de la (ou des) signature(s) des Documents métier. L'objet de la présente PSGP est aussi de décrire en synthèse les règles pour utiliser un service certifié ETSI 101 456 QCP (face à face) et 102 042 LCP (à distance) afin qu'un Client puisse bénéficier d'un service de signature d'un niveau avancé au sens de la directive européenne EC/93 de 1999 définissant un cadre communautaire pour les signatures électroniques.

Les personnes signataires sont :

- D'une part, l'entité légale cliente de DocuSign France (ci-après désigné « Client ») et/ou la ou les entités légales expressément désignées par le Client aux termes du contrat de services conclu entre le Client et DOCUSIGN FRANCE ;
- D'autre part, le(s) Utilisateur(s) » qui signe(nt) un Document métier à distance ou en face à face via l'Application Client.

A ce titre, DOCUSIGN FRANCE, en sa qualité de Prestataire de Services de Confiance et d'Autorité de Gestion de Preuve (AGP), propose en mode « *SaaS* » (Software As A Service) un service de signature de Document métier par voie électronique avec gestion de Fichier de preuve associée (ci-après désigné « le Service »), qui a pour objet :

- La signature électronique au nom du Client ou d'une entité légale désignée par lui, si le Client a fait ce choix, d'un ou de plusieurs (V4) document(s) métier(s)
- La Signature électronique d'un document métier par l'Utilisateur avec le principe du « WYSIWYS » (« What You See Is What You Sign ») et suivant un Protocole de consentement mis en œuvre par DOCUSIGN FRANCE ;
- Le recueil du consentement de l'Utilisateur par DOCUSIGN FRANCE en fonction du choix du Client. Il est précisé que le présent document exclut la délégation totale à une entité tierce du recueil de consentement et que le Client ne peut gérer seul le Protocole de consentement d'un point de vue technique. Dans le cadre du présent document DOCUSIGN FRANCE met en œuvre soit le protocole de consentement complet soit une partie technique du protocole de consentement et en ce cas le Client met en œuvre la partie complémentaire du Protocole de consentement (dans ce dernier cas DOCUSIGN FRANCE doit approuver les moyens qui sont mis en œuvre par le Client pour la partie du Protocole de consentement qui lui incombe afin d'en vérifier l'adéquation avec les exigences de DocuSign France sur le « WYSIWYS »)

- La signature électronique de plusieurs Documents métiers par l'Utilisateur avec le principe du « WYSIWYS » et suivant un Protocole de consentement mis en œuvre par DOCUSIGN FRANCE (V4).
- L'horodatage (apposition d'une Contremarque de temps) des Documents métiers ;
- La mise à disposition, par téléchargement (en V4 seulement) par le Client ou par envoi par DOCUSIGN FRANCE, au Client d'une Enveloppe sécurisée contenant un Accusé Réception signé par DOCUSIGN FRANCE et l'Original signé et horodaté ;
- La création de Fichiers de preuve signés et horodatés par DOCUSIGN FRANCE ;
- La mise à disposition du Client d'un accès au Coffre-fort électronique d'archivage des Fichiers de preuves du Prestataire d'Archivage Electronique (PSAE) si le Client a fait le choix d'utiliser le PSAE de DocuSign France ;
- L'archivage des Fichiers de preuve pendant une durée fixée par Contrat avec le Client si le Client a fait le choix d'utiliser le PSAE de DocuSign France ;
- La matérialisation des Fichiers de preuve archivés en cas de litige sur demande écrite auprès de DocuSign France.

A cet égard, le Service « Protect and Sign (Personal Sign) » permet aux Clients de DocuSign France et aux Utilisateurs de signer électroniquement des Documents métiers et de les conserver en leur conférant la même valeur légale qu'un écrit sur support papier, en conformité avec les dispositions de l'article 1316-1 et de la première phrase du second alinéa de l'article 1316-4 du Code civil.

Si le Client remplit les conditions définies dans la Politique de Certification ETSI, alors le niveau des signatures électroniques des Utilisateurs seulement sont du niveau avancé au sens de la directive européenne de 1999 définissant un cadre communautaire pour les signatures électroniques.

Il est à noter que la signature du Client revêt deux types de besoins différents, étant précisé que dans les deux cas, cette signature garantit l'intégrité du Document métier :

- Authentification du Client : permet d'authentifier l'origine du Document métier, soumis à signature par l'Utilisateur. En ce cas le Document métier est signé électroniquement à des fins seulement d'authentification ;
- Signature au nom du Client : qui engage l'entité légale dans le cadre de l'Application Client.

Il est à cet égard précisé que DocuSign France dans le cadre de la réalisation de ses prestations de Service « Protect and Sign (Personal Sign) » n'intervient pas sur le contenu des données, leur format et/ou sur le choix du type de document sous forme électronique signé entre le Client et les Utilisateurs.

En fonction de l'Application Client, du type de document sous forme électronique devant être signé et de ses besoins de preuve, d'identification et d'authentification spécifiques, le client devra compléter cette présente Politique de Signature et de Gestion de Preuve par un document propre (appelé Politique de Signature) à son application Client utilisant le Service « Protect and Sign (Personal Sign) ».

1.2 Identification de la Politique de Signature et de Gestion de Preuve

La présente Politique de Signature et de Gestion de Preuve (PSGP), dite « de niveau Avancé » décrit les conditions selon lesquelles DOCUSIGN FRANCE, en tant qu'Autorité de Certification, Autorité et opérateur de Signature et de Gestion de Preuve, recueille la signature d'un Utilisateur, et constitue la preuve de son consentement, en connexion directe avec lui, par un processus de type « What You See Is What You Sign ». La présente PSGP couvre également le cas d'un Client DE DOCUSIGN FRANCE qui agirait lui-même en tant qu'Autorité de Certification, cette AC étant positionnée dans la hiérarchie de confiance de DocuSign France, opérée par DOCUSIGN FRANCE et dont la politique de certification est validée expressément par DOCUSIGN FRANCE comme étant conforme à la présente PSGP.

Elle distingue 4 catégories de cas d'utilisation :

- Remote : La signature à distance, avec authentification de l'Utilisateur par un moyen informatique automatisé ;
- Face to face : La signature en présence physique d'un Opérateur d'Autorité d'Enregistrement (dénommé « Opérateur d'AE ») qui vérifie l'identité de l'Utilisateur en face à face au moyen d'un justificatif d'identité ;
- Qualified certificate without SSCD (ETSI 101 456 QCP): La signature en présence physique d'un Opérateur d'Autorité d'Enregistrement (dénommé « Opérateur d'AE ») qui vérifie l'identité de l'Utilisateur en face à face au moyen d'un justificatif d'identité et l'utilisation par l'Utilisateur d'une donnée d'authentification Utilisateur technique (OTP ou certificat reconnu par exemple) obligatoire pour le Protocole de Consentement conformément au Politique de Certification ETSI ;
- Remote (ETSI 102 042 LCP) : La signature à distance, avec authentification de l'Utilisateur suivant des procédures approuvées par l'AGP et l'utilisation par l'Utilisateur d'une donnée d'authentification Utilisateur technique (OTP ou certificat reconnu par exemple) obligatoire pour le Protocole de Consentement conformément au Politique de Certification ETSI.

Chaque catégorie est identifiée par les OID suivants :

- Remote (signature à distance) : 1.3.6.1.4.1.22234.2.4.6.1.5 : associé à la PSGP niveau Avancé pour la signature à distance avec utilisation d'une donnée d'Authentification Utilisateur et avec le principe de WYSIWYS. Cette PSGP est associé à l'OID de Politique de Certification (PC) : 1.3.6.1.4.1.22234.2.8.3.10 ;
- Face to face (signature en face à face) : 1.3.6.1.4.1.22234.2.4.6.1.6 : associé à la PSGP niveau Avancé pour la signature en présence physique d'un Opérateur délégué de l'Autorité d'Enregistrement et avec le principe de WYSIWYS. Cette PSGP est associé à l'OID de PC : 1.3.6.1.4.1.22234.2.8.3.8 ;
- Remote (ETSI 102 042 LCP) : 1.3.6.1.4.1.22234.2.4.6.1.7 : associé à la PSGP niveau ETSI 102 042 LCP certifié pour la signature à distance avec utilisation d'une donnée d'Authentification Utilisateur et avec le principe de WYSIWYS et en conformité avec la Politique de certification ETSI. Cette PSGP est associé à l'OID de PC (Politique de Certification ETSI) : 1.3.6.1.4.1.22234.2.8.3.9.
- Qualified certificate without SSCD (ETSI 101 456 QCP): 1.3.6.1.4.1.22234.2.4.6.1.8 : associé à la PSGP niveau ETSI 101 456 QCP certifié pour la signature en présence physique d'un Opérateur délégué de l'Autorité d'Enregistrement, avec le principe de WYSIWYS et l'utilisation d'une donnée d'Authentification Utilisateur et avec le principe de WYSIWYS et en conformité avec la Politique de certification ETSI. Cette PSGP est associé à l'OID de Politique de Certification ETSI : 1.3.6.1.4.1.22234.2.8.3.7 ;

Les numéros d'OID de la présente PSGP sont indiqués à titre de gestion documentaire pour la société DOCUSIGN FRANCE et pour décrire les niveaux de sécurité à un instant. Les OID sont aussi contenus dans les Fichiers de preuve (et aussi dans le document de mise en production du Client) afin de référencer un niveau de sécurité unique par Client en fonction du niveau de sécurité qu'il a choisi.

La Politique de Signature et de Gestion de Preuve correspondant aux OID ci-dessus indiqués est ci-après désignée sous le nom de « PSGP « Protect and Sign (Personal Sign) » de niveau Avancé».

1.3 Entités impliquées

1.3.1 Client

Le Client désigne l'entité légale, cocontractante de DocuSign France et responsable de :

- L'application Client qui génère le Document métier à signer et qui appelle l'Application « Protect and Sign (Personal Sign) » pour mettre en œuvre une Cinématique de signature ;
- L'identification et de l'authentification des Utilisateurs conformément à sa politique d'enregistrement établie et mise en œuvre en sa qualité d'Autorité d'Enregistrement ;
- Choisir parmi les OID de la PSGP pour sélectionner un niveau de sécurité.

Il génère, notamment à partir des informations transmises par l'Utilisateur, le Document métier qui sera présenté à l'Utilisateur pour signature suivant un Protocole de consentement défini par le Client.

Si le Document métier est au format PDF et que le Client souhaite mettre en œuvre les mécanismes de signature embarquée au sein du document PDF, le document devra inclure des champs de signatures prédéfinis par le Client (avant la V4 uniquement) qui seront utilisés par le Service « Protect and Sign (Personal Sign) ». En V4 la création des champs de signature sur « Protect and Sign (Personal Sign) » pour la signature du Document métier.

En sa qualité d'Autorité d'Enregistrement, le Client doit définir :

- Un Protocole de consentement. Dans le cas des niveaux ETSI 101 456 QCP et ETSI 102 042 LCP, le Protocole de consentement doit être approuvé par l'AGP. Dans tous les cas, le Protocol de consentement requiert au minimum les éléments suivants :
    - Avancé à distance : requiert l'authentification de l'Utilisateur (mot de passe, OTP, SMS, certificat…) lors de la mise en œuvre du Protocole de consentement ;
    - Avancé en face à face : requière l'identification et l'authentification des Utilisateurs lors du face-à-face avec l'Opérateur d'AE en demandant à chaque Utilisateur de présenter une pièce d'identité officielle et en conserver une copie (qui soit valide et constituant un original) ;
- Une politique d'enregistrement et la gestion de l'AE et des AED (Autorité d'Enregistrement Déléguée) des Utilisateurs en fonction du niveau de sécurité :
    - Quel que soit le niveau de sécurité, l'enregistrement de l'Utilisateur par le Client requiert que le Client s'assure de l'identité de L'Utilisateur (transmission d'une pièce d'identité, utilisation d'un processus automatisé qui permette d'authentifier l'Utilisateur, ...) ;
    - ETSI 101 456 QCP : la politique d'enregistrement doit être approuvé par l'AGP et être conforme aux exigences de la Politique de Certification ETSI ;
    - ETSI 102 042 LCP : la politique d'enregistrement doit être approuvée par l'AGP et être conforme aux exigences de la Politique de Certification ETSI ;
- Une Cinématique de signature et la Politique de signature afférente aux modalités de réalisation d'une Transaction électronique dans le respect des conditions de la présente PSGP ;
- Une Politique d'archivage électronique liée à l'archivage des Fichiers de preuve dans le cadre de la présente PSGP ;
- L'élaboration de Conditions Générales d'Utilisation (ou de vente ou de service) à destination des Utilisateurs et qui doivent être référencées dans le document métier signé et/ou le Protocole de consentement. Dans le cas des niveaux ETSI 101 456 QCP et ETSI 102 042 LCP, les CGU doivent être signé par l'Utilisateur et être approuvé par l'AGP.

1.3.2 Utilisateur

L'Utilisateur est une personne physique qui réalise une Transaction portant sur un (ou plusieurs) Document(s) métier(s) qui lui est(sont) présenté(s) par le Client sur un Terminal d'affichage.

L'identité de l'Utilisateur est reconnue et validée préalablement par le Client en sa qualité d'Autorité d'Enregistrement.

Au cours de cette Transaction, l'Utilisateur manifeste son consentement pour le Document métier ou les Documents métiers (en V4) en signant le ou les Document(s) métier(s) au moyen du Service « Protect and Sign (Personal Sign) » suivant le Protocole de consentement choisi par le Client et en utilisant un Terminal d'affichage. Dans le cas des niveaux ETSI 101 456 QCP et ETSI 102 042 LCP, le protocole de consentement doit être approuvé par l'AGP.

1.3.3 AE

L'AE désigne le Client, ou le cas échéant, toute entité légale désignée par le Client et placée sous sa responsabilité, en charge d'authentifier et d'identifier les Utilisateurs.

L'AE est désignée et habilitée par l'AC dans le cadre d'un contrat de service « Protect and Sign (Personal Sign) » signé par le représentant habilité respectif du Client et de DocuSign France. Le rôle de l'AE est d'établir que le futur Utilisateur du Service justifie de l'identité qui sera indiquée dans le Certificat Utilisateur. Ces procédures d'identification sont variables selon le niveau de confiance que le Client, ou l'entité légale désignée par le Client, entend apporter à cette vérification.

L'AE devra en tout état de cause respecter les procédures d'enregistrement qu'elle aura préalablement définies et mises en œuvre dans le cadre de ses pratiques commerciales ainsi que la PC de DocuSign France.

Dans le cadre de la présente PSGP, pour le niveau « Avancé en face à face », l'AE peut déléguer l'authentification et l'identification des Utilisateurs à une AED (Autorité d'Enregistrement Déléguée). Une AE ou une AED utilise des Opérateurs d'AE qui authentifient, identifient les Utilisateurs et gère la signature électronique par l'Utilisateur à l'aide d'un Terminal d'affichage. Dans la suite du document le terme « Opérateur d'AE » est utilisé pour un opérateur qui réalise des fonctions d'enregistrement des utilisateurs, indépendamment qu'il dépende d'une AE et l'AED, afin de facilité la lisibilité des exigences. De même, les exigences sont seulement rédigées pour l'AE ou un Opérateur d'AE. L'AED agît conformément à la présente PSGP et aux politique d'enregistrement, de certification et de signature du Client. Dans le cadre des niveaux ETSI 101 456 QCP et ETSI 102 042 LCP, l'AE doit :

- Garantir que les opérateurs d'AE sont connus de l'AE ;
- Etre auditée annuellement par l'AGP et tous les 3 ans par un auditeur externes.

1.3.4 AGP

L'AGP désigne l'entité qui a en charge la création d'un Fichier de preuve permettant d'attester de la Signature électronique d'un Document métier lors d'une Transaction en ligne conclue entre le Client et un Utilisateur, afin d'être en mesure de démontrer ultérieurement l'existence, à partir d'une date et d'une heure certaines (contremarque de temps), l'intégrité et la validation du Document métier signé (conservation de l'Original dans un fichier de preuve). Les engagements de l'AGP sont formalisés au travers de la présente Politique de Signature et de Gestion de Preuve.

Le rôle d'AGP est pris en charge par DOCUSIGN FRANCE.

En outre, DOCUSIGN FRANCE met en œuvre les applications logicielles nécessaires à la génération du Fichier de preuve et est en charge de l'hébergement de l'applicatif de signature utilisé par l'Utilisateur pour signer les Documents métiers conformément au Protocole de consentement établi par le Client.

1.3.5 Prestataire de Service d'Archivage Electronique (PSAE)

Le PSAE désigne l'entité en charge de la conservation des Fichiers de preuve et mettant à la disposition du Client un Coffre-fort électronique pour l'archivage des Fichier de preuve, garantissant ainsi, en conformité avec les dispositions des articles 1316-1 et 1316-4 du Code Civil, leur pérennité et leur intégrité pendant la

durée d'archivage définie aux termes du contrat de service « Protect and Sign (Personal Sign) » conclus entre le Client et DOCUSIGN FRANCE.

Il conserve les Fichiers de preuve créés et transmis par DOCUSIGN FRANCE conformément à la politique d'archivage établie et communiquée par le Client et ses pratiques d'archivage.

Dans le cadre des présentes, le rôle de PSAE est placé sous la responsabilité de DocuSign France ou sous la responsabilité d'une entité désignée par le Client.

1.3.6 Vérificateur

Le vérificateur est une personne physique (par exemple ; un juge et un expert lors d'un procès, une personne désignée par le Client dans le cadre d'une application, une personne désirant vérifier le Document métier dans le cadre d'une application qui utilise les Documents métiers signés, …) qui réalise la Validation, automatique ou manuelle pour le compte d'une personne morale ou un utilisateur, de la ou les signature(s) électronique(s) d'un Original ou d'un Fichier de preuve conformément à la PSGP. Selon le résultat de l'opération de Validation, le vérificateur pourra décider de l'utilisation ou non de l'Original ou de Fichier de preuve.

Le Vérificateur procède à la Validation de la signature électronique selon l'ensemble des modalités prévues dans la politique de signature du Client, la PSGP de l'AGP, la politique d'archivage du Client et les pratiques du PSAE.

1.4 Usages et applications concernés par la Politique de Signature et de Gestion de Preuve

La présente Politique de Signature et de Gestion de Preuve s'applique aux Transactions réalisées au moyen d'un Terminal d'affichage entre le Client et ses Utilisateurs dans le cadre de l'utilisation du Service « Protect and Sign (Personal Sign) ».

Le Client peut utiliser le Service « Protect and Sign (Personal Sign) » pour toutes Transactions métiers de son choix, étant précisé qu'il est le seul à apprécier l'adéquation du Service « Protect and Sign (Personal Sign) » à ses besoins et qu'il est seul chargé de définir le Protocole de consentement (incluant les procédures d'identification et d'authentification des Utilisateurs lors de la génération du Certificat Utilisateur) applicable à ses Transactions métiers utilisant le Service « Protect and Sign (Personal Sign) ».

Les Signatures électroniques créées dans le cadre du Service « Protect and Sign (Personal Sign) » sont admises à titre de preuve au même titre qu'un écrit sur support papier, conformément à l'article 1316-1 du Code Civil, dans la mesure où :

- Le signataire est clairement identifié ;
- L'acte est établi et conservé dans des conditions de nature à en garantir l'intégrité ;
- L'écrit est lié de façon indissociable à la Signature.

Il est également précisé que le Certificat électronique associé à la Signature électronique apposée sur l'acte validé et accepté par le Client et l'Utilisateur est conforme au RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and Certificate, Revocation List (CRL) Profile, Cooper et. al., May 2008, http://www.ietf.org/rfc/rfc5280.txt).

Il est toutefois précisé que :

- Les signatures électroniques générées dans le cadre de l'utilisation du Service ne sont pas « *présumées fiables* » au sens du décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code civil et relatif à la signature électronique, de sorte qu'en cas de contestation, c'est à celui qui veut se prévaloir des effets juridiques de la signature d'apporter la preuve de la fiabilité du système mis en œuvre ;

- L'identification du signataire demeure à la charge du Client en sa qualité d'Autorité d'Enregistrement ;
- Dans le cadre des niveaux ETSI 101 456 QCP et ETSI 102 042 LCP, la signature est de niveau avancée au sens de la directive européenne de 1999 définissant un cadre communautaire pour les signatures électroniques.

Par ailleurs, il est rappelé qu'en vertu des dispositions de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), et notamment son article 25 modifiant les dispositions des articles 1369-1 et 1369-2 du Code Civil, le Client est tenu d'établir sa propre politique de signature, destinée à informer les Utilisateurs des modalités d'élaboration, de signature, d'utilisation et de Validation des Documents métiers présentés à leur signature.

Le Client définit sa propre Politique de signature électronique afin de décrire au minimum les aspects suivants :

- Le niveau de sécurité choisi entre « Avancé en face à face » et « Avancé à distance » ;
- La description des types de Transactions électroniques conclues via le service « Protect and Sign (Personal Sign) » ;
- La description des types d'Utilisateurs autorisés à utiliser le service « Protect and Sign (Personal Sign) » pour un ou plusieurs types de Transactions électroniques ;
- Le type de Documents métiers qui peut être utilisé et proposé aux Utilisateurs dans le cadre des Transactions électroniques autorisées ;
- La description des Cinématiques de signature ;
- La définition des Données d'authentification et du Protocole de consentement en fonction des types de Documents métiers, d'Utilisateurs et de Transactions électroniques ;
- Les règles (notamment de sécurité) applicables pour l'élaboration et l'utilisation des Documents métiers dans le service « Protect and Sign (Personal Sign) » (en amont de l'utilisation du Service ; par exemple : format et outil de composition de PDF, analyse anti-virus, gestion du contenu et des versions, …) ;
- La définition des règles d'identification et d'authentification des Utilisateurs en fonction de la politique d'enregistrement ;
- Les règles de mise à disposition des Documents métiers signés (Original) ;
- Le choix des modalités d'archivage parmi les possibilités offertes par le Service dans le cadre du service optionnel d'archivage (indexation, durée de conservation, désignation des Administrateurs ayant accès au(x) coffre-fort(s)) ;
- Les règles de sécurité du système d'informations qui (i) met en œuvre l'Application Client, (ii) gère l'identification et l'authentification des Utilisateurs, (iii) gère les documents métiers présentés aux Utilisateurs, (iv) s'interface avec l'Application « Protect and Sign (Personal Sign) » de DocuSign France et (v) met à disposition les Documents métiers signés (Originaux) ;
- La gestion des données à caractère personnel des Utilisateurs ;
- L'information des Utilisateurs.

S'il décide de ne pas utiliser le service d'archivage optionnel proposé par DOCUSIGN FRANCE dans le cadre de la présente PSGP alors il incombe au Client de rédiger sa propre Politique d'archivage afin de répondre à l'ensemble des exigences soulevées par l'article 25 chapitre VII de la loi LCEN concernant la conservation des Fichiers de preuve.

La Politique d'archivage électronique du Client a pour objet de définir au minimum les aspects suivants :

- La catégorisation des archives de Fichiers de preuve en archive courante, intermédiaire et définitive ;
- L'utilisation des archives en fonction de leurs catégories (archive courante, intermédiaire et définitive) ;
- La procédure et les modalités d'accès au Coffre-fort électronique et aux archives de Fichiers de preuves ;
- L'identification, l'attribution et le remplacement des Administrateurs pour l'accès au Coffre-fort électronique ;
- La durée d'archivage des Fichiers de preuve au regard des besoins juridiques de la Transaction ;
- Les modalités de restitution des Fichiers de preuve ;
- Les modalités de changement de format étant précisées que DocuSign France ne fournit pas de service de reversement des Fichiers de preuve dans le Coffre-fort électronique ;
- Les actions à mener en cas de compromission des archives de Fichiers de preuve ;
- La veille cryptographique portant sur les algorithmes de signature utilisés pour la signature des Documents métier et des Fichiers de preuve afin de déterminer les mesures à prendre pour la pérennisation dans le temps des archives de Fichiers de preuve ;
- Les obligations et limites de responsabilité des entités utilisatrices du service « Protect and Sign (Personal Sign) » ;
- La gestion des données à caractère personnel des Utilisateurs.

Le Client doit a minima informer par écrit les Utilisateurs en leur communiquant ou publiant sur son site internet une synthèse de ces modalités au travers notamment de Conditions Générales d'Utilisation (ou équivalent) émises par le Client et qui contiennent à minima les informations suivantes :

- L'application et les Documents métiers visés ainsi que le niveau de sécurité visé (Avancé en face à face ou Avancé à distance) ;
- Un rappel du contexte juridique ;
- Les références à la PSGP, aux PC applicables de DocuSign France applicables en fonction du choix de l'OID de PSGP, politique d'enregistrement, PS et PA du Client ;
- Les définitions relatives au service de signature électronique ;
- La description synthétique des entités impliquées ;
- Une synthèse de la Cinématique de signature électronique des Documents métiers ;
- Les obligations et limites de responsabilités des entités impliquées ;
- La gestion, la mise à disposition et l'archivage des Originaux et Fichiers de preuve ;
- La gestion des données à caractère personnel.

1.5 Gestion de la Politique de Signature et de Gestion de Preuve

1.5.1 Entité gérant la Politique de Signature et de Gestion de Preuve

L'entité en charge de l'administration et de la gestion de la Politique de Signature et de Gestion de Preuve est la Direction Business Development (DBD) au sein de la société DOCUSIGN FRANCE. La DBD est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente Politique de Signature et de Gestion de Preuve.

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

Toute évolution de la PSGP effectuée par la société DOCUSIGN FRANCE le sera dans le cas d'évolution de l'Application « Protect and Sign (Personal Sign) » et/ou dans le cas de changement de la législation et/ou réglementation en vigueur.

1.5.2 Délai de préavis

DOCUSIGN FRANCE informera les Clients du Service « Protect and Sign (Personal Sign) » en respectant un préavis de trente (30) jours calendaires avant de procéder à tout changement de la présente Politique de Signature et de Gestion de Preuves susceptible de produire un effet majeur sur lesdits Clients.

DOCUSIGN FRANCE informera les Clients du Service « Protect and Sign (Personal Sign) » en respectant un préavis de quinze (15) jours calendaires avant de procéder à tout changement de la présente Politique de Signature et de Gestion de Preuves susceptible de produire un effet mineur sur lesdits Clients.

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

1.5.3 Forme de diffusion des avis

Dans les cas de modification soumise à préavis, DOCUSIGN FRANCE avise les Clients des modifications apportées à la présente Politique de Signature et de Gestion de Preuve, par tous moyens à sa convenance dont notamment le site web de DocuSign France et la messagerie électronique, en fonction de la portée des modifications.

1.5.4 Modifications nécessitant l'adoption d'une nouvelle politique

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

1.5.5 Point de contact

La DMS est l'entité à contacter pour toutes questions concernant la présente Politique de Signature et de Gestion de Preuve « Protect and Sign (Personal Sign) ».

Le représentant habilité est :

- 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.

Les termes qui sont utilisés dans la présente Politique de Signature et de Gestion de Preuve avec une majuscule auront la signification décrite dans l'annexe 1 « Définitions ».

2 IDENTIFICATION ET AUTHENTIFICATION

2.1 Identité utilisées

Les identités qui sont utilisées dans le cadre de la signature de Documents métiers sont les suivantes :

- Identité Utilisateur : correspond au(x) nom(s) et prénoms(s) figurant sur la pièce d'identité officielle de l'Utilisateur tels qu'identifié par l'AE, ou l'AED, et certifié par l'AC. Cette identité est portée dans le dans le champ « CN » du certificat Utilisateur (selon la PC applicable) généré au moment de la signature du Document métier par l'Utilisateur ;
- Identité Client (du Client ou de de l'entité légale désignée par le Client) : nom de la personne morale figurant sur un document officiel d'immatriculation (un extrait K.BIS, …) telle qu'identifiée par l'AC. Cette identité est portée dans le certificat Client-S et le cas échéant Client-CDS de l'entité légale (« S » pour Signature) qui sert à signer le Document métier au nom de l'entité légale (selon PC Client applicable) ;
- Identité AGP : c'est le nom de l'entreprise « KEYNECTIS » en tant que personne morale. Cette identité est portée dans les certificats d'AH et d'OCSP (Cf. PC Client) de DocuSign France utilisés pour signer les Fichiers de preuves et les Enveloppes sécurisées ;
- Identité AC : c'est l'identité des AC utilisées pour gérer le cycle de vie des Certificats.

2.2 Authentification et création de l'Identité de l'Utilisateur

L'enregistrement des identités est effectué par l'AE qui définit les règles et procédures pour construire et vérifier l'identité des Utilisateurs. Ces règles sont définies dans un document propre à l'AE (politique d'enregistrement et/ou politique de signature). L'AE transmet l'ensemble des informations nécessaires au Service « Protect and Sign (Personal Sign) » afin de permettre à DOCUSIGN FRANCE de porter l'identité dans les certificats.

L'identification de l'Utilisateur est effectuée en premier lieu afin de répondre aux seuls besoins de la Transaction de l'entité légale désignée par le Client où une identification et une authentification de l'Utilisateur sont nécessaires pour les besoins de la Transaction.

Par conséquent l'identité Utilisateur de l'Utilisateur portée dans le certificat Utilisateur et dans le Document métier n'a de sens que dans le cadre de la transaction. De même, la validité de cette identité Utilisateur ne vaut qu'au regard des procédures appliquées par l'AE.

La certification des identités Utilisateur est réalisée suivant la PC Utilisateur.

Dans le cadre des niveaux ETSI 101 456 QCP et ETSI 102 042 LCP, l'authentification des Utilisateurs est réalisée suivant les exigences respectives des standards ETSI 101 456 QCP et ETSI 102 042 LCP et de la Politique de Certification ETSI de DocuSign France (se reporter au § 1.2).

2.2.1 Enregistrement « Avancé en face à face »

Dans le cadre du niveau « Avancé en face à face », le Client s'engage à informer chaque AE et AED des obligations prévues au présent article et de celles qui lui incombent.

A cet égard, le Client, pour le niveau « Avancé en face à face » devra s'assurer du respect par chaque AE et AED des obligations suivantes :

- Identifier et authentifier les Utilisateurs lors du face-à-face par l'Opérateur d'AE en demandant à chaque Utilisateur de présenter une pièce d'identité officielle (un original en cours de validité) ;
- Documenter ses règles de vérification de la ressemblance entre les informations de l'Utilisateur portées sur le Terminal d'affichage, les informations portées sur sa pièce d'identité officielle présentée à l'Opérateur d'AE et, pour les professionnels seulement, les informations portées dans

les justificatifs d'appartenance à une entité légale le cas échéant sa fonction au sein de l'entité légale ;

- Mettre en forme les informations d'Identité Utilisateur, notamment en reportant, dans le Document Métier, les nom et prénoms figurant sur les justificatifs d'identité ou obtenus le protocole utilisé pour vérifier l'identité de l'Utilisateur ;
- Assurer la sécurisation des « Terminaux d'Affichage » utilisés par les Opérateurs d'AE pour se connecter, transmettre les données à l'Application Client et à l'Application « Protect and Sign (Personal Sign) » et réaliser le Protocole de consentement ;
- Collecter et conserver une copie des pièces justificatives de l'identité de l'Utilisateur ainsi que les données d'identité et d'authentification ;
- Respecter la Politique de signature et la politique d'enregistrement de l'AE ainsi que la Politique de Certification Utilisateur applicable ;
- Informer l'Utilisateur de la gestion de ses données personnelles et des conditions générales d'utilisation de la signature électronique.

En outre, le Client veillera à ce que chaque AE et AED n'utilise le Service que pour des Transactions conclues avec un Utilisateur sur le lieu de vente, au moyen des seuls outils prévus à cette fin (Terminal d'affichage), et uniquement à des fins de signature de Documents métiers du Client en conformité avec la Politique de signature définie par le Client.

Enfin, il devra informer chaque AE et AED de leur obligation de l'alerter immédiatement pour tout incident de sécurité survenant sur son Terminal d'affichage et/ou sur le lieu de vente. Le Client s'engage par suite à en informer sans délai DOCUSIGN FRANCE.

En tout état de cause, le Client se porte-fort du respect par chaque AE et AED des obligations définies dans la présente PSGP.

2.2.2 Enregistrement « Avancé à distance »

Dans le cadre du niveau « Avancé à distance », le Client s'engage à informer chaque AE et AED des obligations prévues au présent article et celles qui leur incombent.

A cet égard, le Client, pour le niveau « Avancé à distance » devra s'assurer du respect par chaque AE des obligations suivantes :

- Identifier et authentifier les Utilisateurs
    - Si l'Utilisateur n'a pas fait l'objet d'une vérification d'identité préalable, l'AE doit s'assurer de l'identification et l'authentification des Utilisateurs par l'Opérateur d'AE ou le processus automatique équivalent en demandant à chaque Utilisateur de transmettre des justificatifs d'identité (par exemple une pièce d'identité officielle dans le cadre de l'ouverture d'un compte en ligne) ou d'utiliser un autre moyen équivalent (utilisation d'un processus automatisé qui permette d'authentifier l'Utilisateur à partir d'une base de connaissance ou qui s'appuie sur un tiers ayant déjà authentifié l'Utilisateur)
    - Si l'Utilisateur a déjà fait l'objet d'une vérification d'identité préalable par l'AE ou par un tiers reconnu par l'AE, l'AE doit utiliser un moyen d'authentification permettant de s'assurer que l'Utilisateur est bien la personne ayant fait l'objet de la vérification initiale (exemple : utilisation d'un compte protégé par un mot de passe, envoi d'un code unique aléatoire par SMS sur un numéro de téléphone mobile vérifié comme étant celui de l'Utilisateur, certificat, etc…)
- Documenter ses règles de vérification des pièces justificatives ;

- Mettre en forme les informations d'Identité Utilisateur, notamment en reportant, dans le Document Métier, les noms et prénoms figurant sur les justificatifs d'identité ou le protocole utilisé pour vérifier l'identité de l'Utilisateur ;
- Collecter et conserver une copie des pièces justificatives de l'identité de l'Utilisateur ainsi que les données d'identité et d'authentification collectées lors de la vérification d'identité initiale
- Respecter la Politique de signature et la politique d'enregistrement de l'AE ainsi que la Politique de Certification Utilisateur applicable ;
- Informer l'Utilisateur de la gestion de ses données personnelles et des conditions générales d'utilisation de la signature électronique.

En outre, le Client veillera à ce que chaque AE n'utilise le Service que pour des Transactions conclues avec un Utilisateur dans le cadre de l'Application Client et uniquement à des fins de signature de Documents métiers du Client en conformité avec la Politique de signature définie par le Client.

Enfin, il devra informer chaque AE de leur obligation de l'alerter immédiatement pour tout incident de sécurité survenant. Le Client s'engage par suite à en informer sans délai DOCUSIGN FRANCE.

En tout état de cause, le Client se porte-fort du respect par chaque AE des obligations définies dans la présente PSGP.

2.3 Authentification et création de l'identité Client de l'Entité légale

Les identités de personnes morales portées dans les certificats Client sont établies et vérifiées suivant les règles et procédures de DocuSign France (Cf. PC Client et PC Utilisateur) ou suivant les règles du Client lorsqu'il choisit ses propres Politiques de certification.

2.4 Identité DOCUSIGN FRANCE

Les identités DOCUSIGN FRANCE sont gérées par DOCUSIGN FRANCE suivant les Politiques de certification applicables et publiées par DOCUSIGN FRANCE.

3 DOCUMENT METIER

Il appartient au Client, ou à tout entité légale expressément désignée par le Client et placée sous la responsabilité de ce dernier, de :

- Déterminer les types de Documents métiers qui peuvent être signés, le type de Transactions et le type d'Utilisateurs suivant une Cinématique de signature définie par le Client ;
- Identifier et définir pour chacune des Transactions le format du Document métier et le format des Documents métiers signés ;
- Déterminer les mesures de sécurité applicables aux Documents métiers pour l'élaboration, le stockage, la présentation à l'Utilisateur et la transmission à DOCUSIGN FRANCE dans le cadre du service « Protect and Sign (Personal Sign) » ;
- Définir si le Document doit être signé par le Client (ou une entité légale désignée par le Client), ou uniquement par l'Utilisateur.

Les formats de Documents métiers et Documents signés autorisés sont :

- XML ;
- PDF.

4 PROTOCOLE DE CONSENTEMENT ET DONNEES D'AUTHENTIFICATION UTILISATEUR

Il appartient au Client, ou à toute entité légale désignée par le Client, de définir et choisir le Protocole de consentement en fonction des Utilisateurs, des types de Documents métiers et des types de Transaction.

Le Protocole de consentement est affiché par DOCUSIGN FRANCE en tant qu'Autorité de Gestion de Preuve, en connexion directe avec l'Utilisateur sur le Terminal d'affichage, mettant ainsi en œuvre un processus de signature de type « What You See Is What You Sign ».

4.1 Avancé en face à face

L'Opérateur d'AE doit authentifier et identifier l'Utilisateur sur la base d'une pièce d'identité officielle. L'Opérateur d'AE doit vérifier à minima l'identité Utilisateur et l'ensemble des informations qui sont portées dans le Document métier que l'Utilisateur souhaite signer.

Des informations permettant de préciser les conditions de la vérification d'identité de l'Utilisateur par l'Opérateur d'AE (identité et authentification de l'Opérateur d'AE, localisation et date précise, etc…) peuvent être transmises pour être ajoutées dans le Fichier de preuve.

4.2 Avancé à distance

Un Protocole de consentement doit nécessiter des Données d'authentification Utilisateur (un mot de passe, 2 mots de passe, un OTP, un certificat, des données transmises par l'Utilisateur, …) en fonction du choix fait par le Client dans le Protocole de consentement.

Les données d'authentification Utilisateur transmises lors de la mise en œuvre du Protocole de consentement sont contenues dans le Fichier de preuve. Les Données d'authentification Utilisateur transmises à DOCUSIGN FRANCE sont donc conservées ensuite par le PSAE en fonction du Protocole de consentement.

La Donnée d'authentification Utilisateur est définie soit par le Client, soit par l'Application « Protect and Sign (Personal Sign) ».

La gestion des données d'activation est sous la responsabilité du Client ou de DocuSign France qui doit décrire les mesures de sécurité applicables aux données d'activation utilisées par l'Utilisateur dans la Politique de signature.

DOCUSIGN FRANCE implémente les Protocoles de consentement choisis par le Client.

Lors de la mise en œuvre du Protocole de consentement, l'Utilisateur peut être amené à communiquer des Données d'authentification Utilisateur. La communication des Données d'authentification Utilisateur est toujours protégée en intégrité et en confidentialité entre l'Utilisateur et DOCUSIGN FRANCE et entre DOCUSIGN FRANCE et le l'Application Client (ou de l'entité légale désignée par le Client).

4.3 ETSI 101 456 QCP

Le Protocol de Consentement doit utiliser une donnée d'Authentification Utilisateur (certificat ou OTP) en conformité avec la Politique de certification ETSI.

4.4 ETSI 102 042 LCP

Le Protocol de Consentement doit utiliser une donnée d'Authentification Utilisateur (certificat ou OTP) en conformité avec la Politique de certification ETSI.

5 HORODATAGE

Dans le cadre de la présente PSGP, le format d'un Document signé peut contenir une Contremarque de temps si le Client choisit un service « Protect and Sign (Personal Sign) » avec le format PDF et une Signature embarquée.

Au moment de chacune des signatures réalisées au nom du Client et de l'Utilisateur par DOCUSIGN FRANCE une Contremarque de temps est apposée pour chaque signature.

Les Contremarques de temps sont contenues dans l'Original.

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 (avant la V4) et SHA-2 (V4) est utilisée par l'AGP pour signer les Contremarques de temps apposées sur le Document métier.

6 VALIDATION OCSP

Dans le cadre de la présente PSGP, le format d'un Document métier signé peut contenir un jeton OCSP si le Client choisit un service « Protect and Sign (Personal Sign) » avec le format PDF et une Signature embarquée.

Au moment de chacune des signatures réalisées au nom du Client et de l'Utilisateur par DOCUSIGN FRANCE un jeton OCSP est apposé pour chaque signature.

Les jetons OCSP sont contenus dans l'Original.

L'utilisation de l'algorithme RSA 2048 avec la fonction de hachage SHA-1 (avant la V4) et SHA-2 (V4) est utilisée par l'AGP pour signer les jetons OCSP apposées sur le Document métier.

7 CINEMATIQUE DE SIGNATURE « PROTECT AND SIGN (PERSONAL SIGN) »

Ce chapitre expose le processus de signature d'un Document métier et de constitution du Fichier de preuve de manière générique. L'objet de ce chapitre est de décrire la cinématique « Protect and Sign (Personal Sign) » de manière générale en donnant les principes et les règles pour certaines particularités types. La cinématique exacte pour chaque Client est précisée dans le Document de mise en production et dans le contrat établi entre le Client et DOCUSIGN FRANCE. Qui plus est, le Client décrit la Cinématique de signature complète dans sa Politique de signature. Le Client élabore le Document métier avec un système d'information choisi par lui.

Dans le cadre de la Cinématique de signature, le Client devra faire autant d'appels au service « Protect and Sign (Personal Sign) » qu'il y a de signataires pour signer le Document métier. Chaque appel fait l'objet d'une nouvelle Transaction « Protect and Sign (Personal Sign) ». En V4, toutes ces Transactions sont rattachées à un même Dossier. En pratique, le Client envoie le Document à signer autant de fois qu'il y a d'Utilisateurs devant signer selon le Protocole de consentement expliqué ci-après. Il est à noter que c'est le principe de sur-signature qui est utilisé, c'est-à-dire que le premier Utilisateur signe le Document, le deuxième Utilisateur signe le Document signé par le premier Utilisateur (qui est en plus horodaté) et ainsi de suite.

Dans le cadre d'une Transaction unitaire, le Client présente à l'Utilisateur le Document métier à signer sur le Terminal d'affichage en fonction du Protocole de consentement.

L'Application Client récupère ou dispose des informations d'identification de l'Utilisateur qui permettront de construite l'Identité Utilisateur.

Le Document métier est ensuite signé par le Connecteur Client afin de fabriquer automatiquement une Enveloppe sécurisée de Requête Client et l'ensemble des informations en accord avec le Protocole de consentement.

L'enveloppe sécurisée est transmise à l'Application « Protect and Sign (Personal Sign) » par l'Application Client soit directement via une session sécurisée (V4), soit en la faisant transiter via le poste de l'utilisateur au sein d'une enveloppe chiffrée (avant la V4). Seule l'Application « Protect and Sign (Personal Sign) » peut déchiffrer l'enveloppe et extraire les informations qui y sont contenues. L'Application « Protect and Sign (Personal Sign) » applique une ou plusieurs signatures de personnes morales sur le Document au nom du Client ou de son ou ses délégataires, si la Cinématique de signature le stipule.

L'utilisateur est alors dirigé vers le service « Protect and Sign (Personal Sign) » qui met en œuvre le Protocole de consentement (Cf. § 4) soit immédiatement (avant la V4) soit ultérieurement (V4) avec un délai maximum défini par le Client.

Le Protocole de consentement doit toujours laisser à l'Utilisateur la possibilité de refuser de signer le Document métier. Une fois que l'Utilisateur a accepté de signer le Document métier conformément aux conditions du Protocole de consentement, l'Application « Protect and Sign (Personal Sign) » :

- Génère la bi-clé (RSA 2048) Utilisateur, ou utilise une bi-clé pré-générée à l'avance et non utilisée (V4), pour l'Utilisateur dans un HSM (Module cryptographique) et certificat Utilisateur (SHA-1 (avant la V4) et SHA-2 (V4)) à durée de vie limitée (5 minutes) valables pour cette Transaction UNIQUEMENT (lié l'identifiant de Transaction) en s'adressant à une AC hébergée chez DOCUSIGN FRANCE ;
- Procède à la génération du hash (SHA-1 (avant la V4) et SHA-2 (V4)) du "Document métier signé" (Données et signature) ;
- Signe avec la clé Utilisateur le Document métier avec de créer l'Original ;
- Détruit la bi-clé Utilisateur générée précédemment ;
- Prépare les informations pour l'AR ;
- Signe l'AR avec un certificat Client-S propre à DOCUSIGN FRANCE ;
- Constitue, signe et horodate le Fichier de preuve constitué essentiellement de l'Original et de l'AR (cf. 9.1) (avant la V4) ;
- Crée une enveloppe Sécurisée Résultat DOCUSIGN FRANCE contenant l'AR et l'Original ;
- Envoie l'enveloppe sécurisée Résultat DOCUSIGN FRANCE à l'Application Client ;
- Constitue, signe et horodate le Fichier de preuve constitué essentiellement de l'Original et de l'AR (cf. 9.1) (V4).

Avant la V4, l'Application Client reçoit l'Enveloppe sécurisée, et grâce au Connecteur Client, procède à son déchiffrement et à l'extraction des informations qui l'intéressent (Code retour de l'Accusé réception, TAG, Original, …) pour conservation. En V4, l'Application Client, au travers du Connecteur Client, récupère auprès de l'application « Protect and Sign (Personal Sign) » via une session sécurisée l'Original et l'AR.

En V4, lors de l'appel pour la 1ère Transaction, l'Application « Protect and Sign (Personal Sign) » crée un nouveau Dossier et renvoie l'identifiant de dossier dans l'Enveloppe sécurisée de résultat DOCUSIGN FRANCE. Pour les Transactions suivantes, l'Application Client fournit cet identifiant dans la Requête Client, ce qui permet à l'Application « Protect and Sign (Personal Sign) » de lier ces Transactions au même Dossier. Pour le dernier signataire, l'Application Client indique dans la Requête Client que la Transaction est la dernière du Dossier. A l'issue de cette Transaction, l'Application « Protect and Sign (Personal Sign) » clôt le Dossier et génère le Fichier de preuve. Tant que le Ficher de preuve n'est pas généré, les Documents et les éléments permettant de constituer le Fichier de preuve sont conservés chiffrés par l'Application « Protect

and Sign (Personal Sign) ». Pendant cette période, qui s'arrête à la fermeture du Dossier sur instruction du Client, les Documents sont traités dans le cadre des Transactions initiées par le Client (signature par plusieurs Utilisateurs, ajout de Document à signer, …).

Suite à la clôture du Dossier, DOCUSIGN FRANCE gère l'archivage temporaire du Fichier de preuve (stocké chiffré par DOCUSIGN FRANCE en V4). L'archivage temporaire se termine à l'issue de l'un des événements suivants : expiration de la période d'archivage temporaire (défini par le Client), confirmation de prise en compte du Fichier de preuve par le PSAE ou rétractation autorisée par le Client sur la Transaction. A l'issue de l'un des évènements cités ci-dessus, les Fichiers de preuves sont détruits et DocuSign France n'en conserve aucune trace ni données permettant de les reconstruite. L'archivage temporaire est relayé par un archivage électronique de longue durée. Le fonctionnement de l'archivage temporaire est décrit dans une annexe technique à la présente PSGP qui ne peut être communiquée qu'aux Clients et aux auditeurs sur demande auprès de l'AGP. En fonction du choix du Client pour tous les Fichiers de preuves pour un type de transaction, cet archivage « longue durée » du Fichier de preuve est traité de la manière suivante :

- DOCUSIGN FRANCE gère l'archivage du Fichier de preuve : L'application « Protect and Sign (Personal Sign) » archive chez un Prestataire de Service d'Archivage Electronique, les Fichiers de preuve permettant ainsi à des Administrateurs habilités, en cas de litige, d'aller les rechercher sur le site d'archive via une interface WEB. La liaison DOCUSIGN FRANCE Prestataire de Service d'Archivage Electronique est sécurisée au moyen d'une liaison sécurisée. Des procédures de surveillance.de l'état des Fichiers de preuve au sein du référentiel permettent la gestion des reprises sur erreur d'archivage et la mise à jour du référentiel (effacement données métier en conservant le record de traçabilité) après l'opération d'archivage. Un accusé réception est retourné par le PSAE après réception du Fichier de preuve à archiver ;
- Le Client gère l'archivage du fichier de preuve : L'Application Client récupère le Fichier de preuve auprès de l'Application « Protect and Sign (Personal Sign) ». L'Application « Protect and Sign (Personal Sign) » conserve le Fichier de preuve pendant un délai défini pour l'expiration de la période d'archivage temporaire dans le contrat avec le Client pour mise à disposition pour l'Application Client. Le Service « Protect and Sign (Personal Sign) » tient à disposition du Client un fichier d'activité récapitulatif comprenant l'ensemble des enveloppes sécurisées de retour échangées pendant la journée. Ces données ne sont compréhensibles que par l'Application Client. Ce dernier procède à un téléchargement.

8 MISE A DISPOSITION DU DOCUMENT SIGNE (ORIGINAL)

Dans le cadre de la Cinématique de signature mise en œuvre par le Client et DocuSign France, l'Original ou la Capsule de Signature est remis seulement à l'AS (Application Client) par l'AGP (application « Protect and Sign (Personal Sign) »).

A cet égard, le Client est averti que DocuSign ne remet à l'Utilisateur :

- Ni le Fichier de preuve,
- Ni l'enveloppe sécurisée de Résultat.
- Ni l'Original, sauf demande explicite qui conduirait DocuSign France à l'envoyer par mail à l'Utilisateur

En conséquence il appartient au Client de mettre en œuvre les moyens et procédures nécessaires pour permettre à chaque personne la remise ou l'accès à l'Original conformément à l'article 1325 alinéa 5 du Code Civil.

9 FICHIER DE PREUVE

9.1 Eléments constituant le fichier de preuve

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

- L'OID de la PSGP choisi par le Client ;
- L'Enveloppe sécurisé Requête Client ;
- Le compte-rendu de la Validation de la signature de l'Enveloppe sécurisé Requête Client et de l'identité de l'Application Client appelant ;
- Le Document métier soumis ;
- L'Original ;
- Le Certificat CDS Client de signature utilisé par le Client pour signer le Document métier ;
- Le compte-rendu de la validation de la signature Client avec CDS Client du Document métier signé par l'Application « Protect and Sign (Personal Sign) » ;
- L'identifiant de Transaction ;
- Les éléments d'identité de l'Utilisateur ;
- Les éléments du Protocole de consentement (copie d'écran d'exemple de la page de consentement) ;
- Le compte-rendu de la validation par l'Application « Protect and Sign (Personal Sign) » de la signature du Document métier signé par l'Utilisateur.

Et en V4 le fichier de preuve contient en complément :

- Le Document métier préparé ;
- Le Document métier présenté ;
- L'identifiant de dossier ;
- Fiche introductive ;
- Fiche descriptive qui contient la traçabilité des opérations et la description des éléments constitutifs du Fichier de preuve ;
- Les éléments issus de la capture réalisée par le Terminal d'Affichage qui contiennent les pages que l'Utilisateur a obligatoirement dû voir et sur lesquelles il a dû cocher des « cases à cocher » avant de pouvoir visualiser le Protocole de consentement (optionnel et seulement si le Terminal d'Affichage peut techniquement transmettre ce type d'information à l'Application « Protect and Sign (Personal Sign) ») ;
- Indication du mode de transmission de l'Enveloppe sécurisée Requête Client ;
- Les fichiers qui permettent de rejouer le Protocole de consentement tel que transmit par DOCUSIGN FRANCE à l'Utilisateur (optionnel et laissé au choix du Client).

Le Fichier de preuve est signé et horodaté électroniquement par DOCUSIGN FRANCE et non modifiable.

9.2 Archivage du fichier de preuve par DOCUSIGN FRANCE

Le PSAE permet d'archiver le Fichier de preuve généré et transmis par DOCUSIGN FRANCE en qualité d'AGP. Le PSAE génère un Accusé Réception PSAE pour tous les Fichiers de preuve transmis par

DOCUSIGN FRANCE. DOCUSIGN FRANCE conserve pour chaque Fichier de preuve stocké par le PSAE les Accusé réception du PSAE.

Lorsque le PSAE est sous la responsabilité de DocuSign France :

- La durée de conservation est de 10 ou 20 ans au choix du Client ;
- La liste et le contenu des Fichiers de preuve seront accessibles par toute personne habilitée par le Client en qualité d'Administrateur à l'aide d'un identifiant et d'un mot de passe communiqués par DOCUSIGN FRANCE ;
- Un module technique sécurisé procède à l'envoi des Fichiers de preuve résultant d'un Dossier dont le résultat est « complet » vers le Coffre-fort électronique.

L'Utilisateur n'accèdera pas aux Fichiers de preuve stockés dans le Coffre-fort électronique. Seul le Client sera en mesure de lui fournir l'Original, dans le respect des dispositions de l'article 1325 alinéa 5 du Code Civil.

Au cas où le type de Transaction prévoit la faculté de rétractation, le Fichier de preuve est conservé pendant la durée de rétractation dans la base de données de l'Application « Protect and Sign (Personal Sign) ». Si pendant cette période, une Transaction de rétractation associée à cette Transaction initiale est effectuée, le Fichier de preuve est supprimé de la base de données de l'Application « Protect and Sign (Personal Sign) ». Si au contraire aucune rétractation n'a été effectuée à l'issue de la période de rétractation, l'archivage définitif du fichier de preuve est effectué.

Le Client peut le cas échéant demander au service-clients de DocuSign France, par écrit, les informations de supervision et de traçabilité de l'Application « Protect and Sign (Personal Sign) » de DocuSign France.

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

DOCUSIGN FRANCE permet au Client d'avoir un ou plusieurs compartiments de stockage dans le coffre DOCUSIGN FRANCE chez le PSAE. Chaque compartiment contient les fichiers de preuve du Client. L'accès à ce coffre est réservé aux seuls Administrateurs désignés par le Client au moyen de données d'activation (mot de passe, …). L'accès au compartiment ne permet que de lire et copier des fichiers de preuve.

DOCUSIGN FRANCE communique les données d'activation au Client qui lui permettront d'accéder au coffre d'archivage chez le PSAE. Le Client est responsable de désigner expressément des Administrateurs « coffre » au sein d'entité légales désignées par le Client.

9.3 Archivage du fichier de preuve par le Client

Le Client est seul responsable de l'archivage des fichiers de preuves. DOCUSIGN FRANCE n'archive pas les fichiers de preuves.

9.4 Proofviewer: utilisation du Fichier de preuve

Le Client peut accéder à tout moment au site du PSAE pour procéder au téléchargement sur un poste informatique d'un Fichier de preuve dont l'intégrité est garantie par l'apposition de la signature électronique de DocuSign France.

Au moyen d'un outil logiciel fourni par DOCUSIGN FRANCE, le Client peut visualiser le contenu d'un Fichier de preuve.

L'outil logiciel fourni par DOCUSIGN FRANCE permet la visualisation du Document métier signé qui a été présenté au consentement de l'Utilisateur sous réserve que le Client ait fourni la Feuille de style utilisée lors de la fabrication de l'enveloppe sécurisée.

Cette vérification peut être faite manuellement par le Client en utilisant l'outil logiciel fourni par DOCUSIGN FRANCE appelé Proofviewer à la date d'application des présentes en version 1.5.

En V4, l'utilisation du Proofviewer est optionnelle car les logiciels Microsoft Word, Reader PDF et P7Z suffisent pour extraire et visualiser les éléments de preuve.

9.5 Lisibilité et pérennité

DOCUSIGN FRANCE ne prend pas d'engagement dans la conservation des Fichiers de preuve au sein de la base de données de l'Application « Protect and Sign (Personal Sign) » mais assure la conservation technique des sauvegardes de cette base de données.

Les fichiers de preuves sont effacés de la plate-forme « Protect and Sign (Personal Sign) » une fois le délai d'archivage temporaire expiré après qu'une copie ait été préalablement transférer sur bandes magnétiques qui sont ensuite mises au coffre sous multiples contrôles pour une conservation de 10 ans maximum

La lisibilité et la pérennité du format utilisé pour le Fichier de preuve sont liées à la pérennité du format XML et PDF (avant la V4).

En V4, la lisibilité et la pérennité du format de Fichier de preuve sont liées en plus au format de document DOCX (OpenXML) et d'archive de compression 7z/LZMA. DocuSign France en assure la pérennité par la conservation de l'application Proofviewer associée.

10 VALIDATION ET UTILISATION DE DOCUMENT SIGNE

10.1 Validation de signature

La Validation de signature nécessite le respect des étapes suivantes par le Vérificateur :

- Obtenir la référence de la Politique de signature du Client ;
- Obtenir la Politique de signature appliquée pour la génération de la signature à vérifier ;
- Vérifier que la Politique de signature appliquée est la Politique de signature du Client ;
- Vérifier que la Politique de signature du Client s'applique au contexte de Validation de la signature ;
- Consulter auprès du Client et/ou de l'AGP les Certificats d'AC du chemin de confiance reconnus pour valider la signature des Originaux et/ou des Fichiers de preuve ;
- Vérifier la validité de l'ensemble des certificats utilisés pour la signature de l'Original et/ou du Fichier de preuve :
    - 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 du Client et de l'AGP les Certificats racines reconnus pour valider la signature ;
- Si présente, alors 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 du Client et/ou de l'AGP les Certificats racines reconnus pour valider la Contremarque de temps ;
- Si présente, alors vérifier les ARL des AC de la chaîne de confiance ;

- Si présente, alors 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 du Client et/ou de l'AGP les Certificats auto-signés reconnus pour valider la réponse OCSP.

Les conditions générales établies par le Client définissent les moyens disponibles pour le Vérificateur afin qu'il vérifie les documents signés. Par exemple, utilisation de :

- Reader PDF ; ou
- Service de validation du Client ; ou
- Les règles de validation à mettre en œuvre et décrites ci-dessous et complété par le Client.

10.2 Utilisation d'un Original

Ca paragraphe définit les règles pour la Validation de signature d'un Original par un Vérificateur qui n'utilise pas le Ficher de preuve pour Valider la signature d'un Original. En effet, l'Original est aussi contenu dans le Fichier de preuve et en cas de doute, en fonction des périodes définies dans ce paragraphe, le recours au Fichier de preuve sera utile afin d'apporter une preuve supplémentaire pour la Validation des signatures électroniques de l'Orignal et ainsi de son contenu.

Si le format est XML alors, la Validation de signature de l'Original et du Ficher de preuve n'est pas vérifiable en dehors de son enveloppe fournie par DOCUSIGN FRANCE.

Si le document est au format PDF avec signature embarquée, alors le document au format PDF est autoportant et vérifiable indépendamment par le Vérificateur. Le même document est aussi contenu dans le Fichier de preuve. Pour la vérification il est nécessaire d'utiliser un logiciel Adobe Reader.

Un Original 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 Original. Les mesures à prendre par le responsable d'application Client pour permettre la Validation d'un document sont dépendantes de ces 2 périodes.

10.2.1 Pendant la période de validité des Certificats utilisés

La validation des signatures (Utilisateur, Client si présente, AH et OCSP) de l'Orignal sont vérifiables pendant la période de validité des Certificats utilisés (Utilisateur, …) à l'aide des informations fournies par l'AGP et le Client et des informations fournies par les AC utilisées.

10.2.2 Après la période de validité des Certificats utilisés

Suite à la fin de la validité de tous les Certificats utilisés pour un Original, et si rien n'est convenu entre l'AGP et le Client pour prolonger leur capacité de vérification, l'AGP et les AC ne s'engagent plus sur la capacité de vérification de la signature de ce même Orignal. C'est-à-dire que l'AC ne diffuse plus d'information sur la validité des certificats utilisés pour la Validation des signatures de l'Original.

Toutefois l'AGP peut communiquer sur la robustesse des algorithmes utilisés, en fonction des communications officielles effectuées par l'ANSSI sur les recommandations algorithmiques, pour les signatures de l'Original afin de garantir que les signatures apposées sont toujours valides et permettent, malgré la fin de vie des certificats, la Validation de signature correctes sans attaques possibles.

Préalablement à la fin de validité de tous les Certificats, le Client et l'AGP pourront se réunir pour définir les modalités de prolongation de la capacité de vérification de la signature des Originaux au regard de l'état de l'art technique (robustesse des algorithmes de signatures, logiciel de lecture des documents, …).

Si aucune modalité de prolongation de la capacité de vérification, il est alors du ressort du Client de définir et de mettre en œuvre les mécanismes de protection permettant de répondre au besoin de Validation des signatures des Originaux. Le besoin de Validation des signatures d'

un Original, et la sécurité y afférant, est déterminé par la durée des engagements juridiques portés dans le document et les contraintes légales liées au métier même dans lequel s'inscrit l'application.

Les mécanismes définis par le Client seront fonction de la durée légale d'obligation de détenir l'Original et des besoins de sécurité pour sa Validation au regard des engagements portées dans l'Original.

10.3 Vérification des identités

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

La vérification des identités est effectuée à partir des seuls certificats Utilisateur et Client. Il est rappelé que l'identité de l'Utilisateur est créé et vérifiée suivant des procédures qui sont définies par le Client et mise en œuvre par l'AE Les règles décrites par le Client permettent de s'assurer du niveau de sécurité, et donc du niveau d'acceptation, de l'identité portée dans le certificat Utilisateur pour l'Utilisateur.

Il est donc possible que le Vérificateur soit amené, en fonction du niveau de sécurité qu'il doit appliquer pour authentifier un Utilisateur, à faire des compléments de vérification afin de valider l'identité de l'Utilisateur portée dans le certificat Utilisateur ou l'identité portée de l'entité légale portée dans le certificat Client.

Si le Document métier est au format PDF avec signature embarquée, alors il est possible que le document métier ne soit signé que par l'Utilisateur. Auquel cas, seul l'identité Utilisateur (Utilisateur) est vérifiable à partir d'un certificat. Si le document métier ne contient pas d'information désignant l'entité légale comme telle, alors le Vérificateur est averti que l'identité de l'entité légale n'est portée que dans un champs « OU » du seul certificat Utilisateur. Ce champs permet d'authentifier l'origine du document métier mais n'engage pas l'entité légale au sens contractuel du terme.

10.4 Utilisation du Fichier de preuve

Le Fichier de preuve n'est accessible que sur demande auprès du Client et de l'AGP. Il n'est lisible qu'en utilisant un logiciel spécifique de lecture disponible auprès de l'AS (Client). Seul l'AS peut extraire des Fichiers de preuve auprès du PSAE. Un Fichier de preuve sert pour les besoins de la Transaction du Client où en cas de litige sur un Original avec un Utilisateur (se reporter au § 10.2).

Les Certificats utilisés pour le Fichier de preuve sont donnés dans la PSGP. Le Fichier de preuve est horodaté par DOCUSIGN FRANCE et possède un jeton OCSP.

Le Fichier de preuve est aussi signé par le PSAE.

Le Fichier de preuve se valide suivant les mêmes règles définies (Cf. § 10.1 et § 10.2) pour un document signé car il est lui aussi signé.

Suite à la fin de la validité de tous les Certificats (principalement le Certificat de la Contremarque de temps) utilisés pour un Fichier de preuve, si rien n'est convenu entre l'AGP et le Client pour prolonger leur capacité de vérification l'AGP et les AC ne s'engagent plus sur la capacité de vérification de la signature de ce même Fichier de preuve. C'est-à-dire que l'AC ne diffuse plus d'information sur la validité des certificats utilisés pour la Validation des signatures du Fichier de preuve.

Toutefois l'AGP peut communiquer sur la robustesse des algorithmes utilisés, en fonction des communications officielles effectuées par l'ANSSI sur les recommandations algorithmiques, pour les

signatures du Fichier de preuve afin de garantir que les signatures apposées sont toujours valides et permettent, malgré la fin de vie des certificats, la Validation de signature correctes sans attaques possibles.

Préalablement à la fin de validité de tous les Certificats, le Client et l'AGP pourront se réunir pour définir les modalités de prolongation de la capacité de vérification de la signature des Fichier de preuve au regard de l'état de l'art technique (robustesse des algorithmes de signatures, logiciel de lecture des documents, …).

Si le Fichier de preuve est archivé par l'AGP alors l'AGP s'engage sur le contenu du Fichier de preuve, pendant sa durée de conservation.

11 STIPULATIONS JURIDIQUES

11.1 Obligations

11.1.1 Client

Les obligations sont :

- Choisir l'OID de PSGP qu'il souhaite utiliser ;
- Définir le Protocol de Consentement en fonction du choix de l'OID ;
- Définir des CGU (ou équivalent) conforme aux exigences de la Politique de Certification ETSI et aux exigences de l'ETSI ;
- D'établir, publier, mettre en œuvre et mettre à jour sa propre Politique de signature en sa qualité d'Autorité de Signature ;
- D'établir, publier, mettre en œuvre et mettre à jour sa Propre politique d'archivage en sa qualité d'Autorité d'Archivage ;
- Identifier et habiliter les personnes et machines qui procèdent aux requêtes de consultation auprès du PSAE et leur attribue les droits d'accès au coffre du PSAE ;
- Identifier les Applications Client du service « Protect and Sign (Personal Sign) » qui mettent en œuvre les Transactions électroniques ;
- (V4) Indiquer quand un dossier est ouvert et quand un dossier est clos ;
- Définir les moyens d'identification et d'authentification des Utilisateurs ;
- Informer les Utilisateurs des conditions d'utilisation du Service et leur présente les Documents métiers objets du consentement pour signature ;
- Préparer les Documents métiers sous format PDF pour intégration des Champs de signature électronique et des Eléments visuels de signature électronique ;
- Conserver les informations sécuritaires liées à la gestion de la signature par ses soins des Documents métiers conformément à la Politique de certification de l'AC émettant les Certificats Client et à la gestion des Enveloppes sécurisées ;
- Définir et formaliser le(s) Protocole de consentement proposé(s) aux Utilisateurs ;
- Définir le contenu attendu des certificats Utilisateur et Client pour les identités électroniques ;
- Sécuriser l'authentification des applications utilisatrices autorisées auprès du Connecteur Client ;
- Garantir la sécurité des données transmises tel que les Documents métiers.
- Respecter la PC Utilisateur et Client applicable ;

- Accepter de se soumettre aux contrôles que l'équipe d'audit de DocuSign France effectue et lui communiquer toutes les informations utiles, conformément aux attentes et besoins de l'AGP ;
- Se conformer à la législation en vigueur en matière de protection des données personnelles ;
- Identifier et autorise les types de Documents métier, les types de Transactions, les types d'Utilisateurs et les types de Protocoles de consentement qui peuvent utiliser le Service « Protect and Sign (Personal Sign) ».

11.1.2 DOCUSIGN FRANCE (AGP)

Les obligations de DocuSign France sont :

- Activer et d'exploiter l'Application « Protect and Sign (Personal Sign) » pour la mise en œuvre du Service « Protect and Sign (Personal Sign) » ;
- Mettre en œuvre les éléments cryptographiques pour la réalisation des signatures au sein de son Centre de production ;
- Générer et de détruire après usage pour signature des Documents métiers, la bi-clé Utilisateur ;
- Générer le Fichier de preuve associé à la Transaction en cours (avant la V4) ou du dossier en cours (V4) ;
- Générer un Accusé réception et le transmettre à l'Application Client ;
- Conserver les documents de mise en production associés au Protocole de consentement choisi par le Client pour chaque Transaction ;
- Contrôler et d'assurer la traçabilité des éléments techniques et organisationnels mis en œuvre pour l'exploitation de la plateforme « Protect and Sign (Personal Sign) » (modifications apportées aux plateformes matériels et logiciels, changement de configuration, gestion des éléments sécuritaires etc.) ;
- Contrôler et de mettre en place des moyens de sécurité des flux échangés entre l'Application « Protect and Sign (Personal Sign) » et les différentes entités (Utilisateur, Client et PSAE) ;
- Mettre à disposition des Clients le Service « Protect and Sign (Personal Sign) » conformément à ses engagements contractuels de qualité de service (disponibilité, maintenance planifiée, …) et à la présente Politique de Signature et de Gestion de Preuve ;
- Publier les certificats d'AC que l'AH utilise pour les contremarques de temps ;
- Publier les certificats d'AC que l'OCSP utilise pour les réponses OCSP ;
- Publier les certificats d'AC qui sont utilisés pour les certificats de personnes morales (Client) pour les applications utilisatrices et pour les certificats Utilisateur ;
- Alerter le Client en cas de compromission de clé privées Utilisateur et Client sous sa responsabilité ;
- Authentifier les demandes de certificat Utilisateur transmises par l'application utilisatrice du Client ;
- Authentifier les demandes de Documents métiers à faire signer par un Utilisateur ;
- Mettre en œuvre l'Application « Protect and Sign (Personal Sign) » et faire signer le Document métier fourni par l'Application Client par l'Utilisateur, identifié par l'AE, suivant le protocole de consentement choisit par le Client ;
- Remettre le Document métier signé à l'Application Client ;
- Se conformer à la législation en matière de protection des données personnelles ;
- Restituer le fichier de preuve en le re-matérialisant sur demande écrite du Client ;

- Pour les niveaux ETSI 101 456 QCP et ETSI 102 042 LCP valider les procédures d'enregistrement, les CGU (ou équivalent), le protocole de consentement et auditer et faire auditer (par un auditeur externe accrédité par un organisme d'audit) le Client et l'AE conformément à la Politique de Certification ETSI.

11.1.3 AE

Les obligations de l'AE sont :

- La coordination des demandes de certificats Utilisateur auprès de l'Application « Protect and Sign (Personal Sign) » ;
- Le respect de la PC Utilisateur ;
- Le respect de la Politique de signature (plus particulièrement de la politique d'enregistrement) du Client ;
- De se conformer à la législation en matière de protection des données personnelles ;
- La vérification des caractéristiques d'identification des Utilisateurs lors de leurs demandes de Certificats Utilisateur ;
- L'établissement et la transmission des demandes de certificats Utilisateur à l'AC après vérification de l'identité de chaque demandeur ;
- La gestion et la protection en confidentialité et en intégrité des données personnelles d'identification des Utilisateurs et des données d'activation ;
- Pour le niveau de sécurité Avancé en face à face :
    - La définition des règles de vérification de la ressemblance entre les informations protées sur le Terminal d'affichage et la signature de l'Utilisateur figurant sur sa pièce d'identité officielle présentée à l'Opérateur d'AE ;
    - La conservation de la copie de la pièce d'identité de l'Utilisateur selon une durée en conformité avec les obligations liées à son activité et la durée de conservation des Fichiers de preuve ;
    - La définition d'une politique de sécurité concernant les postes informatiques, connectés aux Terminal d'affichage mises à disposition des Utilisateurs pour signer, et utilisés par les Opérateurs d'AE sur les lieux de vente pour se connecter et transmettre les données à l'Application Client et à l'Application « Protect and Sign (Personal Sign) » ;
    - Informer et former les AED et avoir la connaissance des Opérateurs d'AE ;
    - S'assurer que les AED respectent la politique d'enregistrement définit par le Client ;
    - Pour les niveaux ETSI 101 456 QCP et ETSI 102 042 LCP définir et appliquer des procédures d'enregistrement conformément à la Politique de Certification ETSI et aux exigences de l'ETSI ;
    - Pour les niveaux ETSI 101 456 QCP et ETSI 102 042 LCP accepter les audits externes et ceux de l'AGP conformément à la Politique de Certification ETSI et aux exigences de l'ETSI.

11.1.4 PSAE

Les obligations sont :

- Générer un accusé réception de PSAE suite à chaque dépôt de Fichier de preuve ;
- Garantir que l'ensemble du Fichier de preuve sera conservé intègre pendant toute la durée de conservation prévue par l'AGP ;

- Définir et met en œuvre un mécanisme d'authentification des requêtes (dépôt et consultation) ;
- Garantir la disponibilité des Fichiers de preuves pour consultation par le moyen de coffre ;
- Garantir une date de réception de dépôt des Fichiers de preuves transmis par l'AGP ;
- Accepter de se soumettre aux contrôles que l'équipe d'audit de l'AGP effectue et lui communiquer toutes les informations utiles, conformément aux intentions de l'AGP afin qu'elle puisse contrôler et vérifier la conformité des opérations avec les pratiques d'archivage du PSAE et la présente PSGP ;
- Documenter ses procédures internes de fonctionnement ;
- Mettre en œuvre les moyens techniques et emploie les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles il s'engage ;
- Authentifier les requêtes (dépôt par AGP et consultation coffre) ;
- Informer sans délai le Client et l'AGP en cas de compromission des archives.

11.1.5 Utilisateur

Les Utilisateurs sont soumis aux obligations suivantes :

- Respecter et se conformer aux informations et conditions de mise en œuvre de la Cinématique de signature qui lui sont communiquées par le Client ;
- S'assurer de la sécurité du terminal d'affichage dont il se sert pour interagir avec l'Application Utilisatrice du Client et DOCUSIGN FRANCE dans le cadre de l'utilisation du Service « Protect and Sign (Personal Sign) » en mode à distance ;
- S'assurer de la sécurité des moyens informatiques (téléphone mobile, Terminal d'affichage, …) que l'Utilisateur utilise pour interagir avec l'Application Utilisatrice du Client et DOCUSIGN FRANCE dans le cadre de l'utilisation du Service « Protect and Sign (Personal Sign) » en mode à distance et en mode face à face ;
- Le cas échéant protéger en confidentialité les Données d'authentification Utilisateur qui lui permettent de mettre en œuvre le Protocole de consentement ;
- Alerter le Client en cas de problème lors de la mise en œuvre du Protocole de consentement ;
- Alerter le Client en cas d'erreur constatée dans le Document signé ou à signer (mauvaise identité, contenu non conforme, …) ;
- Pour les niveaux ETSI 101 456 QCP et ETSI 102 042 LCP accepter et signer les CGU (ou équivalent) conformément à la Politique de Certification ETSI et aux exigences de l'ETSI.

11.1.6 Vérificateur

Les obligations sont :

- Valider les documents électroniques conformément aux règles définies dans la présente PSGP et suivant les règles définies et communiquées par le Client ;
- Respecter la présente PSGP pour les opérations qui lui incombent ;
- Tenir compte des limitations sur l'utilisation de la Contremarque de temps indiquées dans la PH et la PSGP ;
- Respecter les différentes Politiques de certification (PC Utilisateur et PC Client) en tant qu'Utilisateurs de Certificat ;
- Respecter la Politique d'horodatage de l'AH en tant que vérificateurs de Contremarques de temps ;
- Respecter les règles de sécurité définies par le Client pour valider les identités électroniques ;

- Pour les niveaux ETSI 101 456 QCP et ETSI 102 042 LCP vérifier les certificats Utilisateur conformément à la Politique de Certification ETSI et aux exigences de l'ETSI.

11.2 Conformité avec les exigences légales

11.2.1 Exonération des droits

Les exigences définies dans la présente PSGP et ses pratiques doivent être appliquées par les parties telle que définie au § 1.3 dans le respect des stipulations de la présente PSGP sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, ne soit possible.

11.2.2 Loi applicable

Les dispositions de la présente Politique de Signature et de Gestion de Preuve sont régies par le droit français.

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

- 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. » ;
- 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 » ;
- Article 1325 alinéa 5 du code civil « qu'il y ait autant d'originaux que de parties ayant un intérêt distinct (qui s'obligent) » ;
- Ordonnance no 2005-674 du 16 juin 2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique ;
- Loi No 2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure, CHAPITRE II, Lutte contre la cybercriminalité, Article 2 (relatif à l'usurpation d'identité) ;
- Pour les niveaux ETSI 101 456 QCP et ETSI 102 042 LCP, la directive européenne de 1999 définissant un cadre communautaire pour les signatures électroniques.

11.2.3 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 du siège social de DocuSign France, nonobstant pluralité de défendeurs, appel en garantie, procédure de référé ou requête.

11.2.4 Droits de propriété intellectuelle

DOCUSIGN FRANCE et ses éventuels fournisseurs ou sous-traitants conservent tous les droits de propriété intellectuelle (brevet, marque déposée et autres droits) sur les éléments composant le Service « Protect and Sign (Personal Sign) », ainsi que la documentation, les concepts, techniques, inventions, procédés, logiciels ou travaux développés relativement au Service mis à disposition par DOCUSIGN FRANCE, quels que soient la forme, le langage, le support des programmes ou la langue utilisés.

Aucun droit de propriété intellectuelle relatif à l'Application « Protect and Sign (Personal Sign) » n'est conféré au Client. DOCUSIGN FRANCE ne concède au Client qu'un droit non exclusif, personnel et non cessible d'utilisation du Service pour les besoins de son activité dans les conditions définies dans le contrat de services « Protect and Sign (Personal Sign) ».

En conséquence, le Client s'interdit tout agissement ou acte pouvant porter atteinte directement ou indirectement, ou par l'intermédiaire de tiers auxquels il serait associé, aux droits de propriété intellectuelle de DocuSign France sur tout ou partie de l'Application « Protect and Sign (Personal Sign) ».

Tous les droits de propriété intellectuelle relatifs au Service « Protect and Sign (Personal Sign) » de DocuSign France et ses fournisseurs sont protégés par la loi, règlement et autres conventions internationales applicables.

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

11.2.5 Protection des données à caractère personnel

DOCUSIGN FRANCE et le Client respectent la législation et la réglementation en vigueur sur le territoire français, en particulier, la loi modifiée n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Le Client, en sa qualité de responsable de traitement, garantit qu'il a procédé à toute obligation lui incombant en vertu de la loi CNIL précitée, notamment toutes déclarations auprès de la Commission Nationale Informatique et Libertés relatives à la constitution de fichiers et traitements informatiques ainsi que celles devant être réalisées auprès d'organismes d'habilitation, et qu'il a informé les personnes physiques concernées de l'usage qui est fait de leurs données personnelles. A ce titre, le Client garantit DOCUSIGN FRANCE contre tout recours, plainte ou réclamation émanant d'une personne physique dont les données personnelles seraient reproduites ou hébergées via le Service.

En outre, sont considérées comme des données personnelles les causes de révocation des Certificats Client et les dossiers d'enregistrement des demandeurs de Certificats et Utilisateurs notamment leurs données d'identification.

Les données personnelles concernant les Utilisateurs recueillies lors de la demande de certificats et la signature des Documents métiers font l'objet d'un traitement informatique aux seules fin de pouvoir être authentifiés et identifiés par l'AE et les Vérificateurs, de permettre les vérifications nécessaires à la délivrance des certificats Utilisateur, de permettre la construction de l'identité Utilisateur portée dans les certificats Utilisateur et la signature des Documents métiers, et d'apporter les preuves nécessaires à la gestion des certificats des Utilisateurs et la signature des documents métiers.

L'ensemble des données à caractère personnel concernant les Utilisateurs et portées dans les documents demandés par l'AE et l'application utilisatrice sont conservées par l'AE et le PSAE.

Le Client s'engage à se conformer et réaliser, tout au long du Contrat, les formalités et/ou démarches nécessaires au respect de la réglementation en vigueur, notamment celles qui seraient rendues nécessaires par l'évolution technique du Service.

En outre, le Client s'engage à :

- Emettre toute recommandation et/ou conseil ainsi qu'à fournir à DOCUSIGN FRANCE l'assistance nécessaire pour que les Prestations fournies par ce dernier, dans le cadre du Contrat, présentent un niveau de sécurité suffisant concernant les données traitées, notamment pour empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ;
- Mettre en œuvre l'ensemble des moyens nécessaires pour permettre à DOCUSIGN FRANCE de disposer d'un accès au Système Informatique du Client et contrôler l'effectivité des mesures de sécurité mises en œuvre ;
- Déclarer DOCUSIGN FRANCE comme tiers ayant accès aux informations nominatives ainsi traitées ;
- Informer les Utilisateurs que le fait de s'opposer à leur conservation empêche l'obtention d'un certificat Utilisateur et la signature électronique d'un Document métier. En effet, en procédant à une demande de certificat et des demandes de signature de Document métier via le Protocole de

consentement, l'Utilisateur accepte que les données soient conservées aux seuls fins de traitement prévues à cet effet et ce pendant une durée de 10 ans, sauf dérogation aux termes de la politique d'archivage du Client ;

- Informer l'Utilisateur de l'exercice de ses droits au regard de ses données personnelles ;
- Recueillir et traiter les réclamations des Utilisateurs relatives à la collecte ou le traitement de leurs données personnelles.

11.2.6 Effets de la résiliation et survie

La fin de validité de la présente PSGP entraîne la cessation de toutes les obligations de l'AGP au titre de la PSGP en question. Toutefois, les obligations du Client ne sont pas impactées par la fin de validité de la présente PSGP.

11.3 Limites de responsabilité

DOCUSIGN FRANCE, en sa qualité d'AC et d'AGP, garantit le bon fonctionnement des composantes de l'ICP et la conformité de son dispositif de gestion des Certificats et de ses procédures aux dispositions énoncées dans la Politique de certification.

Elle est en outre responsable de l'exploitation du Service qu'elle opère depuis son centre de production en conformité avec les engagements de qualité de service décrits dans le contrat de service conclu avec le Client, et de la publication des LCR.

DOCUSIGN FRANCE n'est responsable de l'exécution défectueuse d'une de ses obligations qu'autant que celle-ci est due à sa faute, sa négligence ou à un quelconque manquement à ses obligations contractuelles ou prévues aux présentes.

DOCUSIGN FRANCE ne saurait être tenue responsable en cas de Validation de signature électronique d'un document avec une identité Utilisateur erronée du fait d'une erreur dans l'Identité Utilisateur créée par l'AE.

DOCUSIGN FRANCE ne saurait être tenue responsable en cas d'attaque réalisée sur la Validation de signature d'un Original ou un fichier de preuve alors même que DocuSign France a utilisé des algorithmes à l'état de l'art et conforment aux recommandations de l'ANSSI ou d'institutions équivalentes. DOCUSIGN FRANCE ne saurait en outre être tenu responsable de l'apparition soudaine et inattendue de vulnérabilités avérées sur des algorithmes utilisés pour signer les Documents métiers et les Fichiers de preuve et qui rendrait de fait caduque la Validation de signature des dits Originaux et Fichiers de preuve.

DOCUSIGN FRANCE ne saurait être tenu responsable d'accès frauduleux au Coffre-fort électronique du Client chez le PSAE du fait de la perte ou la compromission des informations par le Client de ses informations d'accès au dit Coffre-fort.

Le Client est seul responsable de la création des identités Destinataires qu'elle communique à DOCUSIGN FRANCE via l'AE.

Le Vérificateur doit appliquer une période de précaution et procéder à des vérifications afin de valider un Original.

Dans le cadre de l'authentification de l'Utilisateur par DOCUSIGN FRANCE afin de lui proposer de signer un document conformément au Protocole de consentement choisit par le Client et l'utilisation de l'Application « Protect and Sign (Personal Sign) » par l'Application Client, DOCUSIGN FRANCE n'est aucunement responsable de :

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

- 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 Utilisateur, le vol, ou la destruction du courrier électronique contenant la donnée d'authentification Utilisateur ;
- L'utilisation par un tiers, autre que l'Application Client et/ou l'Opérateur d'AE autorisé, du Connecteurs Client et/ou des clés Client associées du fait d'une mauvaise protection de la part de la part du Client et permettant ainsi la création de faux Originaux et Fichier de preuve ;
- La signature électronique du Document métier par un tiers non autorisé, résultant de l'utilisation d'informations erronées communiquées par l'AE et permettant de transmettre les Données d'authentification Utilisateur ;
- L'Utilisation par un tiers autre que l'Utilisateur du téléphone sur lequel l'Utilisateur a reçu la Donnée d'authentification Utilisateur, le vol, ou la destruction du téléphone contenant la donnée d'authentification Utilisateur.

Il est en outre précisé que la Signature électronique des Documents, qui composent le document métier, par les Utilisateurs, n'acquiert de valeur juridique, avec un niveau de sécurité, que par les vérifications qui sont effectuées par l'AE (le Client) et les règles définies par le Client. Dans le cas où la responsabilité de DocuSign France serait engagée en qualité d'Autorité de Certification par un Utilisateur ou un tiers du fait d'un manquement du Client à l'une de ses obligations au titre de son rôle d'Autorité d'Enregistrement, le Client prendra à sa charge toutes les conséquences financières (dépenses, frais de justice, dommages intérêts, etc.) supportées par DOCUSIGN FRANCE au titre d'une décision de justice ou d'une transaction amiable.

Il est toutefois précisé que DocuSign France ne pourra en aucun cas être tenue pour responsable des préjudices indirects ou imprévisibles encourus par le Client, tels que notamment les pertes de chiffre d'affaires, de commandes, de bénéfices, de marge, de clientèle, de revenus réels ou anticipés, de réputation, préjudice d'exploitation, gain manqué ou économie attendu, absence d'atteinte de résultats escomptés, utilisation frauduleuse des données, inexactitude ou corruption de fichiers, en relation ou provenant de l'inexécution ou exécution fautive du Contrat ou inhérents à l'utilisation des Certificats émis par DOCUSIGN FRANCE. Sont également exclus de toute demande de réparation les dommages causés par un événement de force majeure ou cas fortuit.

De plus, DOCUSIGN FRANCE n'est pas responsable des conséquences dommageables inhérentes à l'objet ou au contenu du Document métier signé via le Service « Protect and Sign (Personal Sign) ».

Par ailleurs, DOCUSIGN FRANCE ne pourra être tenue responsable de la qualité de la liaison Internet du Client, ni de la défaillance de l'opérateur de télécommunications en charge de l'accès au réseau Internet ou de toute autre liaison mise en place afin de permettre la mise en ligne du Service.

De même, DOCUSIGN FRANCE n'est pas non plus responsable des dommages résultant de la perte, de l'altération, de la destruction ou de toute utilisation frauduleuse de données, de la transmission accidentelle de virus ou autres éléments nuisibles via Internet.

Il est également convenu que DocuSign France ne peut être tenue responsable d'éventuels dysfonctionnements sur le poste du Client et/ou de l'Utilisateur si ces dysfonctionnements font suite à une utilisation du Service ou à une manipulation du Client non conforme à la Documentation du Service, aux instructions de DocuSign France ou le cas échéant aux formations dispensées par cette dernière.

Le Client est également informé que DocuSign France décline toute responsabilité en cas d'utilisation du Service « Protect and Sign (Personal Sign) » par le Client non conforme aux présentes, notamment dans le cadre de Transactions réalisées en considération d'un droit autre que le droit français et ce en l'absence de transposition par DOCUSIGN FRANCE du Service « Protect and Sign (Personal Sign) » et de la documentation y afférente au droit national concerné.

11.4 Publication d'information

Les informations suivantes sont publiées :

- Politique de Signature et de Gestion de Preuve : https://www.opentrustdtm.com/PC/ ;
- Informations pour les certificats utilisés par l'AGP :
    - Certificats du chemin de confiance : https://www.opentrustdtm.com/PC/ ;
    - Politique de certification de l'AC : https://www.opentrustdtm.com/PC/ ;

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

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

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

12 MESURES DE SECURITE NON TECHNIQUES DES OPERATIONS

12.1 Pour le Service de certification électronique

L'ensemble des mesures applicables au Service de certification électronique utilisé pour la fourniture des différents certificats dans le cadre du Service « Protect and Sign (Personal Sign) » est décrit dans les documents Politiques de certification et Déclaration des Pratiques de Certification de l'Autorité de Certification concernée.

12.2 AGP : Application « Protect and Sign (Personal Sign) »

12.2.1 Mesures de sécurité physique

12.2.1.1 Situation géographique

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

12.2.1.2 Accès physique

Afin de limiter l'accès aux Applications et aux informations de « Protect and Sign (Personal Sign) » et afin d'assurer la disponibilité de la plateforme d'exploitation, DOCUSIGN FRANCE a mis en place un périmètre de sécurité opéré pour ses besoins. La mise en œuvre de ce périmètre permet de respecter les principes de séparation des rôles de confiance telle que prévus pour l'exploitation de son site.

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

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

12.2.1.3 Energie et air conditionné

Afin d'assurer la disponibilité des systèmes informatiques de l'Application « Protect and Sign (Personal Sign) », des systèmes de génération et de protection des installations électriques ont été mis en œuvre par DOCUSIGN FRANCE.

12.2.1.4 Exposition aux liquides

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences du contrat de service « Protect and Sign (Personal Sign) ».

12.2.1.5 Prévention et protection incendie

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

12.2.1.6 Sauvegardes hors site

DOCUSIGN FRANCE réalise des sauvegardes hors site permettant une reprise rapide des fonctions de l'Application « Protect and Sign (Personal Sign) » suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces fonctions.

12.2.2 Mesures de sécurité procédurales

Les mesures de sécurité procédurales portent sur les points suivants :

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

Des précisions sont fournies dans le référentiel documentaire « sécurité & qualité » de DocuSign France.

12.2.3 Procédures de constitution des données d'audit

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

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

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

12.2.3.1 Type d'événements enregistrés

DOCUSIGN FRANCE journalise les évènements concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'Application « Protect and Sign (Personal Sign) » :

- Création / modification / suppression de comptes utilisateur et administrateur des machines (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Evènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;

- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et tentatives non réussies correspondantes.

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

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

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

- Type de l'évènement ;
- Nom de l'exécutant ou référence du système déclenchant l'évènement ;
- Date et heure de l'évènement ;
- Résultat de l'évènement (échec ou réussite).

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

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

- Destinataire de l'opération ;
- Nom du demandeur de l'opération ou référence du système effectuant la demande ;
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'évènement ;
- Toute information caractérisant l'évènement.

12.2.3.2 Processus de journalisation

Les opérations de journalisation sont effectuées au cours du processus considéré.

En cas de saisie manuelle, l'écriture se fera, sauf exception, le même jour ouvré que l'évènement.

12.2.3.3 Procédures de sauvegardes des journaux d'événements

DOCUSIGN FRANCE met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour les composantes de l'Application « Protect and Sign (Personal Sign) », conformément aux exigences de la présente PSGP.

12.2.3.4 Evaluation des vulnérabilités

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

12.2.4 Archivage des données d'exploitation

L'archivage des données permet d'assurer la pérennité des journaux et fichiers constitués par les différentes composantes de l'Application « Protect and Sign (Personal Sign) ».

12.3 Pour le Client

L'ensemble des mesures applicables au Client en matière de sécurité des données d'identité des Utilisateurs et de protection des différents Certificats et clés privées associées utilisés dans le cadre du Service « Protect and Sign (Personal Sign) » est décrit dans un document qui lui est propre.

Le Client applique les mêmes mesures de sécurité pour le système d'information qui héberge l'application Client qui sert à mettre en œuvre la Transaction et l'élaboration des Documents métiers et doit prendre les mesures de sécurité nécessaires pour garantir la sécurité physique des différents systèmes d'information impliqués dans la Transaction, le Connecteur Client et l'Application « Protect and Sign (Personal Sign) » (notamment le Client implémente les mesures de sécurité décrite au § 10.2).

Pour les niveaux ETSI 101 456 QCP et ETSI 102 042 LCP, le Client en qualité d'AE doit respecter les exigences de sécurité décrites et référencées dans la Politique de Certification ETSI.

12.4 Pour le PSAE

L'ensemble des mesures applicables au PSAE en charge de la fourniture des fonctions d'archivage est décrit dans le référentiel documentaire du PSAE.

12.5 Pour le tiers horodateur et l'OCSP

L'ensemble des mesures applicables au tiers horodateur et à la génération de l'OCSP est décrit dans la politique d'horodatage applicable et les documents techniques de DocuSign France (pour l'OCSP).

13 MESURES DE SECURITE TECHNIQUES

13.1 Pour le Service de certification électronique

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

13.2 Pour l'Utilisateur

L'utilisation du Service « Protect and Sign (Personal Sign) » par l'Utilisateur n'impose pas de mesure particulière à appliquer sur le Terminal d'affichage. Il n'y a de ce fait pas d'installation de logiciel ou de scanning du Terminal d'affichage.

Pour l'utilisation du service « Protect and Sign (Personal Sign) » en mode « distant », le Terminal d'affichage utilisé par l'Utilisateur doit être protégé à minima d'un firewall, d'un antivirus et d'un logiciel de détection de malware.

L'Utilisateur s'assure de la sécurité des moyens informatiques (téléphone mobile, …) que l'Utilisateur utilise en plus du Terminal d'affichage pour interagir avec l'Application Client et l'Application « Protect and Sign (Personal Sign) » (mode face à face et mode distant).

Pour l'Utilisation du service « Protect and Sign (Personal Sign) » en mode face à face, le Terminal d'affichage est sous le contrôle de l'Opérateur d'AE.

Pour les besoins de l'utilisation du Service « Protect and Sign (Personal Sign) », il est fait l'hypothèse que le Terminal d'affichage pour la présentation des données fournies possède une ou plusieurs applications de présentation qui :

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

13.3 Pour le Client

Les mesures de sécurité techniques et logiques à la charge du Client concerne le Connecteur Client qui est hébergé sur le site informatique d'une entité légale désignée par le Client.

Pour les besoins de l'utilisation du Service « Protect and Sign (Personal Sign) », le Client doit sécuriser ses mécanismes techniques qui mettent en œuvre cette application selon les règles de l'état de l'art et de la technique applicable à la sécurisation d'un serveur.

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

- le système d'exploitation de la machine hôte doit offrir des contextes d'exécution séparés pour les différentes tâches qu'il exécute ;
- le Client respecte l'état de l'art et de la technique, en particulier les mesures suivantes :
    - La machine hôte est protégée contre les virus ;
    - Les échanges entre la machine hôte et d'autres machines via un réseau ouvert sont contrôlés par au moins un pare feu contrôlant et limitant les échanges ;
    - L'accès aux fonctions d'administration de la machine hôte est restreint aux seuls administrateurs de celle-ci (différenciation compte utilisateur/administrateur) ;
    - L'installation et la mise à jour de logiciels sur la machine hôte est sous le contrôle de l'administrateur ;
    - Le système d'exploitation de la machine hôte refuse l'exécution d'applications téléchargées ne provenant pas de sources sûres ;
    - L'identification et l'authentification des Utilisateurs pour l'accès au système ;
    - La gestion de sessions d'utilisation. La protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
    - La gestion des comptes des Utilisateurs, notamment modification et suppression rapide des droits d'accès ;
    - La protection du réseau contre toute intrusion d'une personne non autorisée ;
    - La protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
    - Les fonctions d'audits (non-répudiation et nature des actions effectuées) ;
    - L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante.

Le Client doit se prémunir des menaces ou des processus informatiques viendraient perturber l'exécution des services du Connecteur Client et par exemple modifier les données (identifiant de Transaction, BLOB, ...) lorsqu'elles sont sous son contrôle. De même, le Client s'assure par des mesures techniques que seul l'Application Client, les personnels autorisés de centre de production de l'Application Client, les Opérateurs d'AE peuvent mettre en œuvre le Connecteur Client et ce pour les seuls fins de Cinématique de signature légitimes au profit du Client et de l'Utilisateur.

Le Client applique les mêmes mesures de sécurité pour le système d'informations qui héberge l'Application Client qui sert à mettre en œuvre la Transaction et l'élaboration des Documents métiers et doit prendre les mesures de sécurité nécessaires pour garantir la sécurité des communications entre ces différents système d'information impliqués dans la Transaction, le Connecteur Client et l'Application « Protect and Sign (Personal Sign) ».

Le Client appliques des mesures particulière pour la gestion, la protection et l'utilisation des clés privées Client utilisées par le Connecteur Client de telle sorte à garantir que seuls des personnelles autorisées y est accès et que leur confidentialité ne puisse être atteinte.

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

Pour l'Utilisation du service « Protect and Sign (Personal Sign) » en mode face à face, le Terminal d'affichage qui est sous le contrôle de l'Opérateur d'AE doit respecter les mesures de sécurité définies par l'AE. Les mesures de sécurité définies par l'AE doivent garantir que la confidentialité et l'intégrité ne sont pas remises en cause lors de l'Utilisation du service « Protect and Sign (Personal Sign) ».

Pour les niveaux ETSI 101 456 QCP et ETSI 102 042 LCP, le Client en qualité d'AE doit respecter les exigences de sécurité décrites et référencées dans la Politique de Certification ETSI.

13.4 Pour l'AGP

Ce chapitre traite de la partie de l'Application « Protect and Sign (Personal Sign) », qui est hébergée sur un système d'informations dédié au sein de DocuSign France et auquel accède le Client pour les besoins de ses Applications web et l'Utilisateur.

13.4.1 Mesures de sécurité de l'outil de signature mis à disposition du Client

Lorsque le Client choisit de mettre en œuvre la Signature électronique embarquée dans le document PDF par l'utilisation de l'Application « Protect and Sign (Personal Sign) », il transmet à DOCUSIGN FRANCE une demande d'apposition de sa Signature dans un champ de signature, s'il souhaite que sa signature soit intégrée dans le document. Cette signature est réalisée au moyen d'un élément de sécurité hardware appelé HSM localisé dans le Centre de production de DocuSign France et accessible dans les mêmes conditions de sécurité que les HSM des Autorités de certification. Le choix et l'utilisation de la bi-clé de signature et du certificat associé au sein du HSM sont régis par le contrôle du Certificat de signature Client enveloppant les données métiers et contenu dans le Fichier de preuve.

13.4.2 Mesures de sécurité de l'outil de signature mis à disposition de l'Utilisateur

Lorsque l'Utilisateur consent au document proposé par le Client conformément au Protocole mis en œuvre par l'Application Client, l'Utilisateur active sous son contrôle, un outil de signature qui utilise une bi-clé générée automatiquement par l'Application « Protect and Sign (Personal Sign) ». Cette bi-clé sera affectée, par le biais de la création d'un Certificat, d'une part à la transaction (identifiant de Transaction) et à l'identité de l'Utilisateur (transférée par le Client) d'autre part. Elle sera ensuite utilisée pour signer le Hash des Données métiers, puis détruite immédiatement après utilisation.

13.4.3 Mesures de sécurité des systèmes informatiques

Le niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'Application « Protect and Sign (Personal Sign) » répond aux objectifs de sécurité suivants :

- Identification et authentification des Utilisateurs pour l'accès au système ;
- Gestion de sessions d'utilisation ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- Gestion des comptes des Utilisateurs, notamment modification et suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;

– Fonctions d'audits (non-répudiation et nature des actions effectuées).

L'Application « Protect and Sign (Personal Sign) » est authentifié par l'Utilisateur à l'aide d'un certificat permettant l'établissement d'une session SSL.

13.4.4 Mesures de sécurité du système durant son cycle de vie

13.4.4.1 Mesures de sécurité liées au développement des systèmes

L'implémentation du système permettant de mettre en œuvre les composantes de l'Application « Protect and Sign (Personal Sign) » est documentée. La configuration du système des composantes de l'Application « Protect and Sign (Personal Sign) » ainsi que toute modification et mise à niveau est documentée et contrôlée.

13.4.4.2 Gestion de la sécurité

Toute évolution significative d'un système ou d'une composante de l'Application « Protect and Sign (Personal Sign) » est documentée et est conforme au schéma de maintenance de l'Application « Protect and Sign (Personal Sign) ».

13.4.5 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'Application « Protect and Sign (Personal Sign) ».

13.5 Pour le PSAE

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

14 COMPROMISSION ET PLAN DE CONTINUITE

14.1 Compromission

L'AGP informe le Client impliquées dans le service des d'événements qui affectent la sécurité des services de l'AGP et de ses Clients.

De même, le Client informe l'AGP de tout usage non autorisés et/ou de la perte des moyens utilisés (bi-clés Connecteur Clients) pour accéder et transmettre des informations Utilisateurs à l'Application.

Le plan de secours développé par l'AGP traite le cas de la compromission réelle ou suspectée de la clé privée du Connecteur client et de compromission de la plate-forme Protect and Sign (Personal Signature).

Dans le cas d'une compromission, réelle ou suspectée, la génération de signature à l'aide de la plate-forme 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 et la compromission écartée.

En cas de compromission d'un Client, les moyens utilisés pour accéder à l'Application Protect and Sign (Personal Signature) du Client seront bloqués afin d'empêcher tout emploi de l'Application Protect and Sign (Personal Signature) à l'aide de ses bi-clés et Connecteur Client.

En cas d'un évènement majeur dans le fonctionnement de la plate-forme qui affecte des documents signés, l'AGP 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.

14.2 Fin d'activité de l'AGP

L'AGP s'engage à informer les acteurs impliqués, notamment le Client, dans le Service, avec un préavis d'au moins 6 mois, de sa décision d'arrêter ses activités de délivrance de signature et de gestion de Fichier de preuve.

Avant que l'AGP ne mette fin au Service, l'AGP ;

- Met fin aux autorisations données aux Clients pour se connecter à la plate-forme Protect and Sign (Personal Signature) en révoquant les Certificat Clients du Connecteur Client ;
- Détruit les clés Clients de signature des Documents qu'elle héberge et met en œuvre au nom du Client et révoque les certificats Clients de signature de Document ;
- Etablit avec le Client un planning de récupération des Fichier de preuve du Client qui sont stockés dans le PSAE de l'AGP (car le Client est le seul à pouvoir accéder à son coffre).

Le Client possède le logiciel Proofviewer et est donc autonome pour la relecture des Fichiers de preuves.

14.3 Plan de continuité

En cas de sinistre dans le centre de production de l'AGP, l'AGP peut activer un site de secours, en fonction des modalités contractuelles établies avec le Client, pour la continuité de service afin d'assurer un niveau de confiance et de disponibilité de service constant pendant et après de tels évènements.

L'AGP décrit ces modalités dans son plan de continuité.

15 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et les évaluations concernent ceux que DocuSign France doit réaliser, ou faire réaliser, afin de s'assurer que l'ensemble de son service est bien conforme à ses engagements affichés dans sa Politique de Signature et de Gestion de Preuve. Les audits couvrent les AE afin de s'assurer de la sécurité de l'implémentation et de l'utilisation du Connecteur Client et de la mise en œuvre du Protocole de consentement par l'Application Client et le cas échéant l'Opérateur d'AE.

Pour les niveaux ETSI 101 456 QCP et ETSI 102 042 LCP, le Client en qualité d'AE est audité annuellement suivant les exigences du programme d'audit définies dans la Politique de Certification ETSI.

15.1 Fréquences et / ou circonstances des évaluations

Les évaluations seront réalisées à la demande du Client ou à l'initiative de DocuSign France.

15.2 Identités / qualifications des évaluateurs

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

15.3 Relations entre évaluateurs et entités évaluées

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

15.4 Sujets couverts par les évaluations

Les contrôles de conformité peuvent porter sur une entité (cf. § 1.3) ou l'ensemble de l'Application Client et visent à vérifier le respect par les entités impliquées des engagements et pratiques définies dans la Politique de Signature et de Gestion de Preuve ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

15.5 Actions prises suite aux conclusions des évaluations

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

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

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

15.6 Communication des résultats

Les résultats des audits sont mis à la disposition du Client sur demande expresse de ce dernier.

16 DEFINITIONS

Accusé Réception DOCUSIGN FRANCE : désigne l'ensemble de données suivantes, signées par DOCUSIGN FRANCE et transmises au Client :

- L'identifiant de dossier (V4 seulement) ;
- L'identifiant de Transaction ;
- Les données d'identification de l'Utilisateur signataire du Document métier ;
- OID de la PSGP ;
- Le hash du Document métier signé par l'Utilisateur ;
- Les hash des Documents métiers signés par l'Utilisateur (V4) ;
- La valeur de la Donnée d'authentification Utilisateur utilisée par l'Utilisateur le cas échéant ;
- Le statut de la transaction en succès ;
- Les données d'informations communiquées par le Client ;
- Les données d'informations saisies par l'Utilisateur sur la page de consentement telles que requises par le Client lors de l'élaboration du Protocole de consentement ;
- La date et l'heure de création de l'AR qui repose sur la date et l'heure de la machine synchronisée avec des sources de temps de confiance (GPS, …).

La signature de l'AR comporte une contre marque de temps (V4).

Accusé Réception PSAE : désigne les données transmises par le Prestataire de Service d'Archivage Electronique suite à chaque dépôt de Fichier de preuve effectué par DOCUSIGN FRANCE pour stockage dans le Coffre-fort électronique mis à disposition du Client. Cet Accusé Réception contient l'empreinte de l'ensemble des Fichiers de preuve déposés auprès du Prestataire de Service d'Archivage Electronique et reçus par ce dernier, ainsi que la date et l'heure du dépôt.

Administrateur(s) : désigne la(les) personne(s) physique(s) désignée(s) par le Client, dans la limite de deux, ayant accès à l'interface web d'accès au Coffre-fort électronique et aux Fichiers de preuve archivés y afférents. La notion d'Administrateur n'est utilisée que lorsque le PSAE est désigné par DOCUSIGN FRANCE.

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

Application Client : application mises en œuvre sous la responsabilité du Client qui lui permet; d'élaborer des Documents métiers et les faire signer par des Utilisateurs suivant une Cinématique de signature. L'Application du Client héberge le Connecteur Client.

Application « Protect and Sign (Personal Sign) » : désigne l'ensemble cohérent d'informations et de programmes informatiques propriété de DocuSign France dont une partie est hébergée et exploitée sur la plateforme « Protect and Sign (Personal Sign) » de DocuSign France et dont l'autre partie (modules logiciels Connecteur Client et Proofviewer) est incluse dans le Kit de connexion livré au Client pour installation dans un environnement informatique de son choix. L'Application « Protect and Sign (Personal Sign) » a pour objet de fournir au Client un service de signature de Document métier en ligne avec génération de Fichier de

preuves et optionnellement d'archivage de Fichiers de preuves associés à des Transactions réalisées en ligne entre le Client et un ou plusieurs Utilisateur(s) (en V4) au moyen d'un Terminal d'affichage.

Archivage : désigne l'opération consistant à assurer la conservation sécurisée, pour une durée à moyen ou long terme, d'Original, quel qu'en soit le support, en vue d'une consultation ultérieure à titre de preuve ou d'information. L'archivage est réalisé par un PSAE.

Archivage électronique : désigne l'ensemble des actions, outils et méthodes mis en œuvre pour réunir, identifier, sélectionner, classer et conserver des Fichier de preuve, sur un support sécurisé, dans le but de les exploiter et de les rendre accessibles dans le temps, que ce soit à titre de preuve (notamment en cas d'obligation légale ou de litige) ou à titre informatif. Le Fichier de preuve archivé est considéré comme figé et ne peut donc être modifié.

Archivage temporaire : l'archivage temporaire est un processus de conservation du Fichier de preuve par DOCUSIGN FRANCE, dans un état de nature à garantir son intégrité, préalable à la mise en Archivage du Fichier de preuve de manière définitive.

Authentification : pour l'émission de certificat Utilisateur, c'est une opération organisationnelle et/ou technique réalisée par une AE de l'AC qui consiste à vérifier les données d'identité de l'Utilisateur qui sont portées dans son certificat Utilisateur. En fonction du niveau de sécurité (en face à face ou à distance), le Protocole de consentement définit l'authentification réalisée par le Client.

Autorité d'Archivage (AA) : désigne l'entité qui a en charge l'application d'au moins une Politique d'archivage (PA) en s'appuyant sur un ou plusieurs Service d'Archivage Electronique (SAE) mise en œuvre par un ou plusieurs PSAE. L'AA définit les règles de gestion du cycle de vie des documents archivés dans le cadre des applications utilisatrices du Client. L'AA est le Client ou toute autre entité légale désignée par le Client.

Autorité de Certification (ou **AC**) : désigne l'un des acteurs de l'Infrastructure à Clés Publiques (ICP) émettant des Certificats sur demande de l'Autorité d'Enregistrement et assurant la gestion de leur cycle de vie, et ce en application des règles et des pratiques déterminées par elle dans ses Politiques de Certification et Déclarations des Pratiques de Certification associées.

Dans le cadre du service « Protect and Sign (Personal Sign) » les AC utilisées sont par défaut celles de DocuSign France. Le Client peut aussi choisir ses AC pour la gestion des certificats de signature du Client et de l'Utilisateur. En ce cas, ses AC sont hébergées par DOCUSIGN FRANCE et sont expressément acceptées et rattachées à la hiérarchie DOCUSIGN FRANCE. De plus, DOCUSIGN FRANCE valide la PC associée à une telle AC.

Autorité d'Enregistrement (ou **AE**) : désigne l'un des acteurs de l'ICP approuvé par l'AC et qui a en charge de : (i) assurer l'identification et l'authentification des Utilisateurs suivant une politique d'enregistrement qu'elle aura préalablement établie et mise en œuvre dans le cadre de ses pratiques commerciales, et dans le respect des Politiques de certification applicables, (ii) désigner et assurer la gestion des Opérateur d'AE, (ii) enregistrer les demandes d'émission, de renouvellement et de révocation des Certificats Utilisateurs, les valider ou les rejeter.

Dans le cadre des présentes, pour le traitement des demandes d'émission de Certificats Utilisateurs, l'Autorité d'Enregistrement est le Client, ou le cas échéant toute autre entité désignée par le Client sous sa responsabilité.

Pour le traitement des demandes d'émission de Certificats Clients, l'Autorité d'Enregistrement est DOCUSIGN FRANCE dans le cas de sa propre Politique de Certification, ou, dans le cas d'une AC Client, toute entité légale agissant sous le contrôle et la responsabilité de l'AC et en conformité avec sa Politique de Certification de cette dernière.

Autorité d'Enregistrement Déléguée : désigne toute entité légale agissant pour le compte de l'Autorité d'Enregistrement, dans le cadre d'une relation contractuelle ou hiérarchique dans laquelle l'AE assume pleinement la responsabilité des missions réalisées par l'AED.

Autorité de gestion de preuve (ou **AGP**) : désigne l'entité qui a en charge la création et de la conservation (pour la conservation uniquement si l'option d'archivage a été souscrite auprès de DocuSign France) d'un Fichier de preuve permettant d'attester de la signature électronique d'un Document métier lors d'une Transaction en ligne conclue entre le Client et un ou des Utilisateur(s), afin d'être en mesure de démontrer ultérieurement l'existence, à partir d'une date et d'une heure certaines, l'intégrité et la validation du document électronique métier signé. Les engagements de l'AGP sont formalisés au travers d'une Politique de Signature et de Gestion de Preuve.

Dans le cadre des présentes, le rôle d'AGP est supporté par DOCUSIGN FRANCE.

Autorité de Signature (AS) : désigne l'entité qui a en charge l'application d'au moins une politique de signature en s'appuyant sur un ou plusieurs portail(s) de signature. Le Client définit la politique de signature.

Le rôle d'AS est pris en charge par le Client, ou le cas échéant toute autre entité désignée par le Client sous sa responsabilité.

Centre de production : désigne l'environnement physique et informatique (logiciels et matériels) sécurisé de DocuSign France, pour la production et la gestion des Certificats électroniques du Client.

Certificat(s) : désigne(nt) un fichier électronique délivré par l'Autorité de Certification attestant du lien entre une identité et la Clé publique de la personne titulaire du Certificat.

Dans le cadre des présentes il est précisé que :

- Le terme « **Certificat Client** » (également dénommé « **Certificat KWS** » avant la V4) désigne l'ensemble de certificats électroniques utilisé par le Connecteur Client pour sécuriser les enveloppes sécurisées :
    - (avant la V4) ces certificats sont aux nombres de 3 : un associé à la personne morale (Client-S) est affecté à la signature par le Client du Document métier, le second (Client-S) a pour fonction de signer la requête Client, et le dernier (Client-S) a pour fonction de déchiffrer l'enveloppe de résultat DOCUSIGN FRANCE ;
    - (V4) ces certificats sont aux nombres de 3 : un associé à la personne morale (Client-S) est affecté par le Client à la signature de la requête Client, un autre (Client-S) a pour fonction d'authentifier l'application Client vis à vis de l'application « Protect and Sign (Personal Sign) » dans le cas où la requête Client est transmise en direct, et le dernier (Client-S) pour déchiffrer l'enveloppe de résultat DOCUSIGN FRANCE dans le cas où elle transite par le poste de l'Utilisateur.
- Le terme « Certificat DocuSign France Client » désigne les 2 certificats électroniques utilisés par l'application « Protect and Sign (Personal Sign) » pour sécuriser les enveloppes sécurisées de résultat. L'un (Client-S) pour signer l'enveloppe de résultat et l'AR, l'autre (Client-S) pour déchiffrer l'Enveloppe de requête Client dans le cas où elle transiterait par le poste de l'Utilisateur ;
- Le terme « **Certificat Utilisateur** » (également dénommé « **Certificat KWA** » avant la V4) désigne les Certificats générés à la volée par DOCUSIGN FRANCE pour le compte de l'Utilisateur, et utilisés pour la signature par l'Utilisateur du Document métier créé, signé et présenté par le Client. Ils ont pour caractéristiques principales d'être à usage unique, dédiés à une Transaction, et de contenir une information unique qui est l'identifiant de Transaction. Chaque Certificat Utilisateur contient des informations telles que l'identité Utilisateur de l'Utilisateur, la clé publique de l'Utilisateur, la durée de vie du Certificat, l'identité du Client en qualité d'AE, et la signature de l'AC qui l'a émis ;

- Le terme « **Certificat Client CDS** » désigne le certificat au nom du Client et dont la clé privée est mise en œuvre par DOCUSIGN FRANCE afin de créer une signature électronique embarquée du Document métier au nom du Client.

Cinématique de signature : désigne un processus qui décrit le type et (V4) le nombre de Documents métiers à signer qui composent un Dossier, le nombre et l'ordre des signataires (le nombre de transactions), ainsi que le Protocole de consentement associé à chaque signature (transaction).

Clé privée : désigne une clé mathématique associée à la Clé publique, qui est secrète et destinée à signer les données électroniques.

Clé publique : désigne une clé mathématique rendue publique et qui est utilisée pour vérifier la signature numérique d'une donnée reçue, qui a été préalablement signée avec une Clé privée.

Coffre-fort électronique : désigne, dans le cadre du Service d'archivage proposé par DOCUSIGN FRANCE, un espace de stockage des Fichiers de preuve hébergé chez le Prestataire de Service d'Archivage Electronique et dans lequel un compartiment est dédié au Client. Cet espace est protégé afin de permettre le seul accès aux Administrateurs désignés par le Client, dans son compartiment dédié, au moyen d'identifiants et mots de passe. Cet espace de stockage ne permet que de consulter et télécharger les Fichiers de preuve ainsi stockés. La suppression d'un Fichier de preuve, lorsqu'il est conservé par un PSAE sous la responsabilité de DocuSign France, n'est possible que sur demande expresse du Client auprès de DocuSign France.

Connecteur Client : (également appelé PSMClient en V4 et module TransID avant la V4) : désigne le module logiciel (une des composantes de l'Application « Protect and Sign (Personal Sign) ») livré par DOCUSIGN FRANCE dans le Kit de connexion, et qui est installé dans une Application Client en vue de l'utilisation du Service. Le module assure toutes les opérations cryptographiques réalisées nécessaires à l'implémentation de la Signature électronique suivant les Protocoles de consentements et les Cinématiques de signature choisis par le Client. Il a également pour rôle de créer la référence unique de la Transaction (l'identifiant de Transaction).

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

Déclaration des Pratiques de Certification (ou **DPC**) : désigne l'énoncé des pratiques utilisées par l'Autorité de Certification pour émettre et gérer le cycle de vie des Certificats.

Document électronique métier: désigne un document électronique créé par le Client sous un format PDF ou XML et complété des informations relatives à l'Utilisateur. Le document métier passe par les statuts successifs suivants :

- Soumis : le document métier est transmis par le Client au service « Protect and Sign (Personal Sign) ». A ce stade, le Document métier peut déjà contenir une ou des signature(s) apposée(s) par le Client et/ou un ou des Utilisateur(s) via « Protect and Sign (Personal Sign) » ;
- Préparé (optionnel) : le document métier est signé par DOCUSIGN FRANCE au nom du Client ;
- Présenté :
    - En cas de souscription d'obligations sous format PDF : le Document métier est présenté à l'Utilisateur sur le Terminal d'affichage. Dans le cas particulier d'un Terminal d'affichage de type tablette, le document est présenté avec uniquement des images de signatures ;
    - En cas de souscription d'obligations sous format XML : le Document métier est présenté à l'Utilisateur à l'identique du document soumis par le Client ;
    - Signé : A l'issu de la signature par l'Utilisateur, et le cas échéant le Client, le Document métier devient un Original (cf. définition Original).

Document de mise en production : désigne le document complété et signé par le Client décrivant ; notamment pour chaque Application métier Client utilisant le Service, le Protocole de consentement, l'AC utilisée, les caractéristiques de l'AE utilisée, les modalités d'émission et de communication du rapport d'activité, les conditions d'accès au Service d'archivage (lorsque le Client y a souscrit), et indiquant la date de mise en production du Service.

Données d'activation : désigne les données ou actions associées à un Utilisateur permettant de mettre en œuvre sa clé privée. Dans le cas d'un Certificat Utilisateur, ces données ou actions sont définies aux termes du Protocole de consentement et sont appelées données d'authentification Utilisateur.

Données d'authentification Utilisateur : désigne la donnée d'activation particulière (par exemple ; mot de passe temporaire envoyé par SMS, mot de passe généré par l'Application Client et transmis par le Client à l'utilisateur, …) qui permet à l'Utilisateur de s'authentifier lors de protocole de consentement et de mettre en œuvre sa clé privée Utilisateur.

Dossier (V4) : désigne un ensemble de Transactions liées par un unique identifiant de Dossier. Un Dossier permet notamment de regrouper l'ensemble des Transactions d'un Document métier multi-signataires. A un Dossier correspond un Fichier de preuve. Un Dossier est à l'état complet lorsque toutes les Transactions qu'il doit contenir sont réalisées.

Empreinte : « désigne le résultat d'une fonction, dit de hachage à sens unique, appelé empreinte. C'est-à-dire le résultat d'une fonction calculant une empreinte d'un message de telle sorte qu'une modification même infime du message entraîne la modification de l'empreinte résultante du calcul ».

Enveloppe sécurisée (anciennement appelé BLOB avant la V4) : désigne un ensemble formaté de données qui contient les éléments propres à une Transaction entre le Client et un ou plusieurs Utilisateurs :

- Requête Client: données signées par le Client via le Connecteur Client transmises par l'Application Client à l'Application « Protect and Sign (Personal Sign) » de façon sécurisée en intégrité et en confidentialité et contenant le Document métier. La transmission s'effectue soit directement (en V4) soit via le Terminal d'affichage ;
- Résultat DOCUSIGN FRANCE: données contenant les données résultats de l'exécution de la Transaction et retournées à l'Application Client par l'Application « Protect and Sign (Personal Sign) ». Elle contient l'Original et l'AR signé.

Fichier de preuve : désigne l'ensemble des éléments créés lors de la réalisation d'une ou plusieurs Transaction associées à un Dossier ainsi que l'historique des opérations réalisées, permettant d'assurer la pérennité de la validité de l'Original.

Format de document : désigne le type de codage algorithmique utilisé pour créer, modifier et visualiser un document électronique (PDF ou XML).

Incident : désigne tout défaut de fonctionnement répétitif et reproductible, apparu dans des conditions normales d'utilisation du Service, exclusivement imputable à tout ou partie de l'Application « Protect and Sign (Personal Sign) », et induisant l'impossibilité totale ou partielle de bénéficier des fonctionnalités du Service définies dans le présent Contrat et dans la documentation associée.

Identifiant de Transaction (également appelé TransNUM avant la V4 ou OperationId en V4) désigne un numéro de référence unique, composé de 64 caractères au plus, généré par le Connecteur Client et permettant de lier un Original, sur lequel est apposée une Signature électronique, à un Utilisateur préalablement identifié par l'Application Client.

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

Identité Utilisateur : désigne un ensemble d'informations (nom(s) et prénom(s)) qui caractérise l'Utilisateur en tant qu'individu de telle 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. Cette identité permet aussi de caractériser le fait que cet individu travaille au sein d'une entité légale. L'identité Utilisateur est contenue dans le Certificat Utilisateur : le nom et prénom de l'Utilisateur seront contenus dans un champ CN et si l'Utilisateur est un professionnel, le nom de la société dans laquelle travaille l'Utilisateur pourra être contenue dans un champ « OU » du certificat Utilisateur.

Pour le niveau de sécurité « Avancé en face à face », une mention explicite «Identité vérifiée en présence physique de l'Opérateur d'Autorité d'Enregistrement » est alors insérée dans le certificat Utilisateur. Des informations permettant de préciser les conditions de cette vérification (identité et authentification de l'Opérateur d'AE, localisation et date précise, etc…) peuvent être transmises pour être ajoutées dans le Fichier de preuve.

Il est précisé qu'une mention explicite « Identité vérifiée en présence physique de l'AE » ou « Identity verified in Face to Face with RA » est insérée dans le certificat Utilisateur.

Cette identité est construite par le Client en qualité d'AE.

Identité- Client de personne morale : ensemble d'informations (nom de l'entité légale, numéro de SIREN, …) qui identifient le Client personne morale pour l'Original et le Fichier de preuve. Cette identité est vérifiable à partir de documents officiels tels qu'un extrait K.BIS ou assimilé.

Infrastructure à Clés Publiques (**ICP**) : désigne un ensemble de moyens organisationnels, techniques (matériels et logiciels), humains, documentaires et contractuels pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques. L'ICP génère, distribue, gère et conserve les Certificats. Chacune des composantes de l'ICP est décrite dans les Politiques de certification définissant le niveau de confiance confié à chacune d'elles.

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

Kit de connexion : désigne les éléments logiciels Connecteur Client et Proofviewer relatifs au Service ainsi que la documentation d'installation et d'utilisation du Service, incluant les prérequis techniques, livrés au Client par DOCUSIGN FRANCE pour la mise en œuvre et l'utilisation du Service.

Liste des Certificats Révoqués (ou **LCR**) : désigne la liste des Certificats révoqués avant leurs dates d'échéance, émise périodiquement, et numériquement signée par l'AC émettrice des Certificats contenus dans la liste.

Opérateur(s) d'AE : désigne(nt) toute personne physique nommée expressément par l'AE ou l'AED pour l'identification et l'authentification en face-à-face des Utilisateurs, en vue de la réalisation de Transactions et la signature électronique de Documents métiers en agence au moyen d'un Terminal d'affichage.

Original : désigne le document électronique métier signé électroniquement et constitue un écrit électronique au sens de l'article 1316-1 du code civil et constitue un exemplaire au sens de l'article1325 aliéna 5. Suivant la cinématique et la version de « Protect and Sign (Personal Sign) » choisies, il est constitué de la manière suivante :

- En cas de signature de Document métier par le seul Utilisateur en mode XML, l'Original est composé :
    - Le Document métier électronique (au format XML ou PDF) ;
    - L'identité électronique du signataire portée dans le Certificat Utilisateur ;

- La valeur de (ou des) signature(s) électronique(s) Utilisateur détachée (document métier au format PDF contenu dans un XML) ou embarquée (document métier au format XML) de l'Utilisateur ;
- Une Contremarque de temps (en V4) ;
- Les ARL de la chaîne de la confiance de l'AC Utilisateur (en V4) ;
- Une validation OCSP pour chaque signature électronique Utilisateur (en V4) ;

– En cas de signature du Document métier par le Client et l'Utilisateur en mode XML, l'Original est composé de :
  - Le Document métier électronique (XML ou PDF) ;
  - L'identité électronique du signataire portée dans le Certificat Utilisateur ;
  - La valeur de (ou des) signature(s) électronique(s) Utilisateur détachée (document métier au format PDF contenu dans un XML) ou embarquée (document métier au format XML) de l'Utilisateur ;
  - La valeur de (ou des) signature(s) électronique(s) Client CDS détachée (document métier au format PDF contenu dans un XML) ou embarquée (document métier au format XML) du Client ;
  - Une Contremarque de temps (en V4) ;
  - Les Listes des Autorités Révoquées (LAR) de la chaîne de la confiance de l'AC Utilisateur (en V4) ;
  - Une validation OCSP pour chaque signature électronique Utilisateur (en V4).

– En cas de signature par le seul Utilisateur en mode PDF, l'Original est composé :
  - Le Document métier électronique au format PDF ;
  - L'identité électronique du signataire portée dans le Certificat Utilisateur ;
  - La valeur de la Signature électronique embarquée de l'Utilisateur ;
  - Une contremarque de temps ;
  - Les LAR de la chaîne de la confiance de l'AC Utilisateur ;
  - Une validation OCSP pour chaque signature électronique Utilisateur ;

– En cas de signature du Document métier par le Client et l'Utilisateur en mode PDF, l'original est composé de :
  - Le Document métier électronique au format PDF ;
  - L'identité électronique du signataire portée par le certificat Utilisateur ;
  - La valeur de la signature électronique Utilisateur embarquée de l'Utilisateur ;
  - La valeur de la signature électronique Client CDS embarquée du Client ;
  - Une Contremarque de temps ;
  - Les ARL de la chaîne de la confiance de l'AC Utilisateur ;
  - Une validation OCSP pour chaque signature électronique Utilisateur.

PDF (*Portable Document Format)* : désigne un format de fichier informatique conforme à la norme ISO 32000 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 d'Archivage : désigne l'ensemble des règles juridiques, fonctionnelles, opérationnelles, techniques et de sécurité que le Client doit établir, mettre en œuvre et respecter pour la gestion du cycle de vie des Fichiers de preuve archivés (durée de conservation, accessibilité des archives, modalités de restitution, de destruction, etc.), afin que l'archivage électronique ainsi mis en place puisse être qualifié de fiable. Cette politique d'archivage est définie par le Client en fonction de ses besoins métiers, notamment en termes de confidentialité et de sécurité, et vient en complément de la politique d'archivage du Prestataire de Service d'Archivage Electronique.

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

Les Politiques de Certification de DocuSign France applicables au Service, et leurs mises à jour successives, sont accessibles sur le site Internet de DocuSign France.

Politique de Certification ETSI : désigne la politique de certification particulière référencée « DMS_Protect and Sign Personal Signature ETSI CP v 1.0 » pour la gestion des certificats d'Utilisateurs suivant les règles ETSI 101 456 et 102 042. Les certificats des Utilisateurs sont émis par une AC particulière dénommée « Cloud Signing Personal Signature CA ».

Politique d'enregistrement : désigne les procédures et les règles définies et mises en œuvre par l'Autorité d'Enregistrement pour identifier, authentifier les Utilisateurs et enregistrer les demandes d'émission, de renouvellement et de révocation des Certificats.

Politique de Signature et de Gestion de Preuve : désigne le document décrivant les processus techniques utilisés par DOCUSIGN FRANCE pour la signature par le Client et un ou des Utilisateurs de Documents métiers conformément au Protocole de consentement, puis la création et la conservation du Fichier de preuve lors de l'utilisation du Service. La PSGP de DocuSign France (OID : 1.3.6.1.4.1.22234.2.4.6.1.5 pour le niveau Avancé pour la signature à distance et 1.3.6.1.4.1.22234.2.4.6.1.6 pour le niveau Avancé pour la signature en face à face) et ses mises à jour successives sont accessibles sur le site Internet de DocuSign France.

Politique de signature : désigne un ensemble de règles établies par le Client pour la création ou la validation d'une signature électronique via l'Application « Protect and Sign (Personal Sign) », 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.

Prestations : désignent les prestations définies dans le contrat signé entre le Client et DOCUSIGN FRANCE et réalisé par DOCUSIGN FRANCE dans le cadre du Service.

Prestataire de Service d'Archivage Electronique (ou **PSAE) :** désigne l'entité mettant à la disposition du Client un Coffre-fort électronique pour l'archivage de ses Originaux et Fichiers de preuve, garantissant ainsi, en conformité avec les dispositions des articles 1316-1 et 1316-4 du Code Civil, leur pérennité et leur intégrité pendant la durée d'archivage. Le PSAE est choisi par DOCUSIGN FRANCE par défaut sauf si le Client souhaite lui-même choisir son PSAE. Si le Client souhaite lui-même choisir son propre PSAE, les prestations d'archivage seront sous la responsabilité du Client, et non plus de DocuSign France.

Prestataire de service de certification (ou **PSCE**) : désigne, lorsque le Client souscrit au Service

d'archivage proposé par DOCUSIGN FRANCE, un acteur de l'ICP chargé de gérer le cycle de vie des Certificats électroniques des Utilisateurs pour le compte d'une ou plusieurs Autorités de Certification. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Il est identifié, dans un certificat dont il a la responsabilité, au travers de son AC qui a émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" dudit certificat.

Prestataire de service de Confiance (ou **PSCO)** : désigne toute personne ou entité offrant des services consistant à la mise en œuvre des fonctions qui contribuent à la sécurité des informations échangées par voie électronique (authentification, signature, confidentialité et horodatage).

Proofviewer : désigne un module logiciel (une des composantes de l'Application « Protect and Sign (Personal Sign) »), propriété de DocuSign France, livré au Client dans le cadre du Kit d'installation, afin de lui permettre de visualiser et de vérifier la signature du Fichier de preuve.

Protocole de consentement : désigne l'ensemble des règles de recueil de consentement pour une application métier donnée utilisant le Service à savoir (i) la définition des actions à réaliser par l'Utilisateur sur le Terminal d'affichage pour signer le Document métier proposé par l'Application Client, (ii) les informations utilisées pour la création de l'identité Utilisateur, (iii) les modalités de contrôle par le Service des informations saisies par l'Utilisateur par comparaison aux informations fournies par le Client pour chaque Transaction, (iv) le type de fichier soumis par le Client à signature (XML/PDF…), (v) les modalités de visualisation du Document métier présenté et du message d'acceptation (ou de refus) associé. La description du protocole de consentement est définie dans le Document de mise en production.

Renouvellement (d'un Certificat Client) : désigne l'opération effectuée en fin de période de validité d'un Certificat qui consiste à générer un nouveau Certificat Client pour le Client.

Révocation (d'un Certificat Client) : désigne l'opération demandée par l'AC ou le Client conformément à la Politique de Certification Client, dont le résultat consiste en la suppression de la garantie de l'AC sur un Certificat donné, avant la fin de sa période de validité.

Service (« Protect and Sign (Personal Sign) ») : désigne le service tel que défini dans les présentes mis à la disposition du Client en mode SaaS. Le Service a pour objet de permettre au Client, à partir de son Application Client, de proposer aux Utilisateurs, via un Terminal d'affichage, un service de signature électronique de Documents métiers en ligne, et de constituer et d'archiver des Fichiers de preuve relatifs aux Transactions conclues.

Service d'archivage : désigne l'ensemble des prestations réalisées par le Prestataire de Service d'Archivage Electronique pour l'archivage de données électroniques consistant en la capture du Fichier de preuve créé et transmis par DOCUSIGN FRANCE, sa conservation dans son format d'origine pendant une durée fixée en fonction du PSAE (DOCUSIGN FRANCE ou un PSAE choisi par le Client).

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

Service d'horodatage : désigne l'ensemble des prestations réalisées par DOCUSIGN FRANCE nécessaires à la génération de Contremarques de temps associées aux Fichiers de preuve, en application de la Politique d'horodatage de DocuSign France et ses mises à jour successives, accessibles sur son site Internet.

Cette Contremarque de temps a pour objet de positionner dans le temps la réalisation et l'acceptation de la Transaction conclue en ligne par l'intermédiaire du Service.

Service d'OCSP (Online Certificate Status Protocol) : désigne le service de vérification de DocuSign France mis à la disposition du Client pour contrôler la validité des Certificats émis.

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

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

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 ayant pour objet d'identifier la personne qui l'appose et de « *manifester le consentement du signataire aux obligations qui découlent de l'acte* » signé.

Signature électronique embarquée : désigne une fonctionnalité ayant pour objet d'intégrer au sein d'un document métier au format PDF la Signature électronique de l'Utilisateur et le cas échéant celle du Client, de sorte que la signature soit indissociable dudit document. Il s'appuie sur un certificat CDS. Cette fonctionnalité additionnelle confère ainsi au document PDF le rôle d'un Original électronique contenant l'ensemble des informations de signature (à savoir : horodatage, identité du signataire, 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 qui le possède, 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 ayant été référencée par ADOBE dans le cadre du programme « CDS ». Les spécificités techniques propres à chacun de ces référencements sont précisées dans la documentation d'installation et d'utilisation du Service remise au Client. Cette fonctionnalité additionnelle est liée au Service de certification choisi expressément par le Client lors de la mise en production du Service.

Dans le cas où le Terminal d'affichage ne permet pas de visualiser la signature électronique CDS, la fonctionnalité de Signature électronique embarquée permet également depuis la version (avant la V4) la création d'une copie fidèle du fichier PDF, sous forme de PDF « mis à plat », qui permette une visualisation identique du contenu sur le Terminal d'affichage. Cette copie fidèle mise à plat est également mis à la disposition du Client, étant précisé que l'Original électronique reste le PDF comportant la Signature électronique embarquée des personnes. L'opération de mise à plat peut être réalisée lors de la visualisation avant signature et lors de la visualisation après signature.

Signature électronique valide : une signature électronique qui satisfait aux opérations de Validation de signature définies dans une Politique de signature par le Client.

Terminal d'affichage : désigne le terminal (ordinateur personnel, tablette, …) sur lequel l'Utilisateur effectue sa Transaction, et sur lequel est affiché le Document métier à signer, le Protocole de consentement (affiché en connexion directe avec DOCUSIGN FRANCE) et le cas échéant le document une fois signé à la fin de la Transaction.

Transaction : désigne l'échange électronique entre le Client et chaque Utilisateur réalisé au moyen d'un Terminal d'affichage et au cours duquel le Client propose pour signature ou pour rétractation, suivant une Cinématique de signature et un Protocole de consentement définie par le Client, un ou plusieurs (V4) Document(s) électronique(s) métier(s) à un Utilisateur préalablement identifié par lui, afin que l'Utilisateur manifeste son consentement à le(s) signer, ou refuse de le(s) signer, ou utilise son droit de rétractation sur une Transaction préalablement réalisée. En (V4), une Transaction est associée à un Dossier. Une Transaction est identifié de façon unique par un Identifiant de transaction.

Utilisateur : désigne la personne physique qui se connecte sur l'Application du Client et qui signe le Document métier qui lui est présenté par l'Application Client via l'Application « Protect and Sign (Personal Sign) » sur Terminal d'affichage, et auquel est associé un Identifiant de transaction unique indiqué dans le

Certificat Utilisateur. L'identité de l'Utilisateur est reconnue et validée préalablement par le Client en sa qualité d'Autorité d'Enregistrement.

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 du Vérificateur de la 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 :

- L'identité portée dans l'Original et le Fichier de preuve utilisé pour la Validation de signature ;
- Que le certificat est signé par une AC reconnue et identifiée par l'AS dans la Politique de Signature pour le type d'Original sur lequel portent la signature et la vérification.

Validation de signature : 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 cryptographique 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.

Vérification cryptographique 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.

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