DocuSign

Protect and Sign: Personal Signature (PSM)

Politique de Signature et de Gestion de Preuve (PSGP)

PROTECT AND SIGN: PERSONAL SIGNATURE (PSM) POLITIQUE DE SIGNATURE ET DE GESTION DE PREUVE

Version du document :	V 1.7	**Nombre total de pages :**	24
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	
19/02/2021	V 1.5	EM	Refonte de la PSG pour intégrer tous les services de signature de DocuSign France.	
04/03/2021	V 1.6	EM	Modification information contact PMA et signature CGU pour l'OID 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32 quand DocuSign France est l'AE.	
22/04/2022	V 1.7	EM	Signature by the new PMA	

SOMMAIRE

AVERTISSEMENT 5

1 INTRODUCTION 6

1.1 Présentation générale de la Politique de Signature et de Gestion de Preuves 6
1.2 Identification de la Politique de Signature et de Gestion de Preuve 7
1.3 Entités impliquées 7
1.3.1 Client 7
1.3.2 Utilisateur (Signataire) 8
1.3.3 Autorité d'Enregistrement (AE) 8
1.3.4 DocuSign France 8
1.3.5 DocuSign Inc. 9
1.3.6 Prestataire de Service d'Archivage Electronique (PSAE) 9
1.3.7 Vérificateur 9
1.4 Usages et applications concernés par la PSGP 9
1.5 Gestion de la Politique de Signature et de Gestion de Preuve 10
1.5.1 Entité gérant la Politique de Signature et de Gestion de Preuve 10
1.5.2 Délai de préavis 10
1.5.3 Forme de diffusion des avis 10
1.5.4 Modifications nécessitant l'adoption d'une nouvelle politique 10
1.5.5 Point de contact 10

2 IDENTIFICATION ET AUTHENTIFICATION 11

2.1 Utilisateur 11
2.2 Client 12
2.3 DocuSign France 12

3 DOCUMENT METIER ET ORIGINAL 12

4 PROTOCOLE DE CONSENTEMENT ET DONNEES D'ACTIVATION DE LA SIGNATURE 13

5 HORODATAGE 13

6 STATUT DU CERTIFICAT 14

7 TRANSACTION DE SIGNATURE PSM 14

7.1 Sans DTM 14
7.2 Avec DTM 15

8 MISE A DISPOSITION DU DOCUMENT METIER SIGNE (ORIGINAL) 16

8.1 Avec DTM 16
8.2 Sans DTM 17

9 FICHIER DE PREUVE 17

9.1 Eléments constituant le fichier de preuve 17
9.1.1 Avec DTM 17
9.1.2 Sans DTM 17
9.2 Archivage du fichier de preuve 18
9.2.1 Avec DTM 18
9.2.2 Sans DTM 18
9.3 Lisibilité et pérennité 18

10 VALIDATION ET UTILISATION DE DOCUMENT SIGNE (ORIGINAL) 18

10.1 Validation de signature et utilisation d'un Original 18
10.1.1 Pendant la période de validité des Certificats utilisés 19
10.1.2 Après la période de validité des Certificats utilisés 19
10.2 Vérification des identités 20
10.3 Utilisation du Fichier de preuve et COC 20

11 STIPULATIONS JURIDIQUES 20

12 MESURES DE SECURITE NON TECHNIQUES DES OPERATIONS 20

12.1 DocuSign France 20
12.2 Pour le Client 21
12.3 Pour le PSAE 21

13 MESURES DE SECURITE TECHNIQUES 21

13.1 Pour l'Utilisateur 21
13.2 Pour le Client 21
13.3 DocuSign France 21
13.4 Pour le PSAE 21

14 COMPROMISSION ET PLAN DE CONTINUITE 21

14.1 Compromission 21
14.2 Fin d'activité 22
14.3 Plan de continuité 22

15 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS 22

16 DEFINITIONS 23

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 (noté PSGP) associée au Service « Protect and Sign » (noté PSM) que la société DocuSign FRANCE fournit à ses Clients soit en direct soit en passant par la plateforme de DocuSign (noté DTM).

La présente PSG couvrent les Services de signature, et les preuves associées, suivants :

- Avancée qui sont couverts par les OIDs de Politique de Certification (PC) suivants :
    - SBS EU Advanced (avec DTM uniquement) : 1.3.6.1.4.1.22234.2.14.3.33.
    - SBS EU Advanced with IDV (avec DTM uniquement) : 1.3.6.1.4.1.22234.2.14.3.33.
    - ID check for AES (avec DTM uniquement) : 1.3.6.1.4.1.22234.2.14.3.32 (certifié ETSI 319 411-1 LCP).
    - Client qui est Autorité d'Enregistrement (AE), certifié ETSI, et utilise le Service sans passer par DTM : 1.3.6.1.4.1.22234.2.14.3.32 (certifié ETSI 319 411-1 LCP).
    - Client est AE et utilise le Service sans passer par DTM : 1.3.6.1.4.1.22234.2.14.3.33.
- Qualifiée qui sont couvert par les OIDs de PC suivant :
    - ID check in person for QES (avec DTM uniquement) : 1.3.6.1.4.1.22234.2.14.3.31(certifié ETSI 319 411-2 QCP n-qscd).
    - ID check remote for QES (avec DTM uniquement) : 1.3.6.1.4.1.22234.2.14.3.31 (certifié ETSI 319 411-2 QCP n-qscd).
    - Client qui est Autorité d'Enregistrement (AE), certifié ETSI, et utilise le Service sans passer par DTM : 1.3.6.1.4.1.22234.2.14.3.31 (certifié ETSI 319 411-2 QCP n-qscd).

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 et/ou COC (en fonction du Service) 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 (appelé Originaux).

Lorsque des règles sont spécifiques à un type de Service, alors elles seront identifiées comme suit :

- En précisant si le Service utilise ou pas DTM ;
- Si besoin en indique un nom de Service et/ou un OID de PC comme décrit ci-dessus.

A ce titre, DocuSign FRANCE, en sa qualité de Prestataire de Services de Confiance (PSCO), propose en mode en mode cloud, plusieurs types de Service de signature, comme identifiés ci-dessus, de Document métier par voie électronique avec le cas échéant (en fonction du type de Service) la création de Fichier de preuve associé à l'opération de signature, qui a pour objet :

- La scellement électronique (avec un cachet 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 Document(s) métier(s) (avec et sans DTM) ;
- 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 ou le Client ou DTM en fonction du type de Service ;
- Le recueil du consentement de l'Utilisateur par DocuSign FRANCE ou par le Client en fonction du choix du Client. DocuSign FRANCE met en œuvre soit le Protocole de consentement complet soit une partie technique du Protocole de consentement soit le Client met en œuvre le Protocole de

Consentement (sans DTM seulement) et en ce cas le Client met en œuvre la partie complémentaire du Protocole de consentement ou tout le Protocole de consentement.

- La signature électronique de plusieurs Documents métiers par l'Utilisateur en fonction du type de Service comme identifié ci-dessus.
- L'horodatage qualifié (depuis novembre 2019) avec des Contremarque de temps des Documents métiers immédiatement après la signature ;
- La mise à disposition, par téléchargement par le Client ou par envoi par mail (avec DTM seulement), au Client de l'Original signé et horodaté ;
- La création de Fichiers de preuve scellés et horodatés par DocuSign FRANCE (pour tous les Services sauf SBS EU Advanced with IDV et SBS EU Advanced, en ce cas la preuve de l'opération de signature est fournie par DTM à l'aide du COC) ;
- La mise à disposition du Client d'un accès au Coffre électronique d'archivage pour les Fichiers de preuves et/ou COC et/ou Originaux du Prestataire d'Archivage Electronique (PSAE) si le Client a fait le choix d'utiliser le PSAE de DocuSign France pour archiver ces Fichiers de preuves (pour tous les Services sauf SBS EU Advanced with IDV et SBS EU Advanced et qualifié quand DocuSign France est AE) ;
- La matérialisation des Fichiers de preuve archivés en cas de litige sur demande écrite auprès de DocuSign France (pour tous les Services sauf SBS EU Advanced with IDV et SBS EU Advanced) ;
- La création de Fichier de preuve simplifié sur demande du Client en cas de litige ou de perte du Fichier de preuve originel (pour tous les Services sauf SBS EU Advanced with IDV et SBS EU Advanced et qualifié quand DocuSign France est AE et ID Check for AES).

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

La PSGP est maintenant identifiée par un seul et unique OID : 1.3.6.1.4.1.22234.2.4.6.1.19.

Cette PSGP s'applique indistinctement et englobe tous les autres OIDs précédents suivants : 1.3.6.1.4.1.22234.2.4.6.1.5, 1.3.6.1.4.1.22234.2.4.6.1.6, 1.3.6.1.4.1.22234.2.4.6.1.7 et 1.3.6.1.4.1.22234.2.4.6.1.8 ainsi que tous les Services de signature identifiés ci-dessus.

Les OID sont aussi contenus dans les Fichiers de preuve (et aussi dans le document de mise en production du Client) afin de référencer le présent document.

1.3 Entités impliquées

1.3.1 Client

Le Client désigne l'entité légale, cocontractante de DocuSign France ou de DocuSign Inc. ou d'un partenaire de DocuSign Inc. et responsable de :

- L'Application Client qui génère le Document métier à signer et qui appelle PSM ou DTM pour mettre en œuvre une Transaction. Il est à noter que le Client lorsqu'il utilise DTM peut ne pas utiliser d'Application Client et directement gérer ces Document métier dans DTM qui les fait ensuite signer PSM ;
- 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 (sauf pour les Services SBS EU Advanced with IDV sans manual review, ID Check for AES, ID Check remote for QES et ID Check in person for QES) ;
- La définition d'un Protocole de consentement (seulement pour les Services sans DTM et pour l'OID 1.3.6.1.4.1.22234.2.14.3.33, 1.3.6.1.4.1.22234.2.14.3.32 et 1.3.6.1.4.1.22234.2.14.3.31 uniquement quand le Client est AE).

- Générer, notamment à partir des informations transmises par l'Utilisateur, le Document métier qui sera présenté à l'Utilisateur pour signature.
- Définir une politique d'enregistrement (seulement pour les Services sans DTM et pour l'OID 1.3.6.1.4.1.22234.2.14.3.33 et 1.3.6.1.4.1.22234.2.14.3.32 et 1.3.6.1.4.1.22234.2.14.3.31 uniquement quand le Client est AE et avec DTM pour les services SBS EU Advanced et SBS EU Advanced with IDV avec manual review) ;
- Une Politique d'archivage électronique liée à l'archivage des Fichiers de preuve et COC dans le cadre de la présente PSGP (seulement pour les Services sans DTM et pour l'OID 1.3.6.1.4.1.22234.2.14.3.33 et 1.3.6.1.4.1.22234.2.14.3.32 et 1.3.6.1.4.1.22234.2.14.3.31 uniquement quand le Client est AE et avec DTM pour les services SBS EU Advanced et SBS EU Advanced with IDV). La Politique d'Archivage peut être contenue dans la politique d'Enregistrement ;
- 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 (uniquement pour le Service 1.3.6.1.4.1.22234.2.14.3.33 sans DTM). Dans le cas des niveaux qualifiés, les CGUs du Service doivent être signées par l'Utilisateur (seulement pour les Services 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32 avec DTM). Les CGU sont validés par DocuSign France dans le cadre des services 1.3.6.1.4.1.22234.2.14.3.32 et 1.3.6.1.4.1.22234.2.14.3.31 et elles sont définis et validés par DocuSign France dans les autres cas (sauf pour le Service 1.3.6.1.4.1.22234.2.14.3.33 sans DTM).

1.3.2 Utilisateur (Signataire)

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.

Au cours de cette Transaction, l'Utilisateur manifeste son consentement pour le ou les Documents métiers suivant le Protocole de consentement.

L'Utilisateur est toujours identifié et authentifié par l'Autorité d'Enregistrement (AE). L'identité de l'Utilisateur (nom et prénom du seul signataire) est portée dans le Certificat de signature émis par l'AC.

1.3.3 Autorité d'Enregistrement (AE)

La définition exacte de l'AE est donnée dans les PC qui définissent les règles de gestion d'un Certificat en fonction d'un OID (ceux listés ci-dessus au § 1). En fonction du type de Services, l'AE agît de manière différente comme indiquée dans la PC pour l'OID associé au Service.

Dans tous les cas, l'AE est en charge d'identifier et d'authentifier l'Utilisateur, c'est-à-dire de récupérer et vérifier l'identité de l'Utilisateur ainsi que le numéro de téléphone mobile (si celui-ci est utilisé dans le cadre du Protocol de consentement) et son adresse de courrier électronique de manière sécurisée en lien avec l'identification de l'Utilisateur de façon à s'assurer qu'ils sont liés à l'Utilisateur.

Le Client est AE dans le cas des Services sans DTM pour l'OID 1.3.6.1.4.1.22234.2.14.3.33 et 1.3.6.1.4.1.22234.2.14.3.32 et 1.3.6.1.4.1.22234.2.14.3.31 uniquement quand DocuSign France n'est pas AE et avec DTM pour les services SBS EU Advanced et SBS EU Advanced with IDV en cas de manual review.

1.3.4 DocuSign France

L'entité qui a en charge la création d'un Fichier de preuve permettant d'attester de l'opération de 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 qualifiée), l'intégrité et la validation du Document métier signé (conservation de l'Original dans un fichier de preuve si PSM reçoit le Document métier).

DocuSign France met en œuvre le Protocol de Consentement sauf si le Client le met en œuvre comme détaillé plus loin dans le présent document.

1.3.5 DocuSign Inc.

L'entité qui met en œuvre la plate-forme DTM. Cette plateforme permet de crée le COC qui contient tous les éléments de preuve de la Transaction dans tous les types de Service utilisant DTM et de preuve de signature dans le cas de l'OID 1.3.6.1.4.1.22234.2.14.3.33. Le COC possède un cachet serveur permettant d'identifier la société DocuSign Inc.

1.3.6 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 électronique pour l'archivage des Fichier de preuve et/ou des COC et Document métier garantissant ainsi, en conformité avec les dispositions des articles 1365 et 1366 du Code Civil, leur pérennité et leur intégrité pendant la durée d'archivage définie aux termes du contrat de Service conclus avec le Client.

Le PSAE conserve les données reçues conformément à sa politique et sa pratique d'archivage (ou de préservation).

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

1.3.7 Vérificateur

Le vérificateur est une personne physique (par exemple ; un juge et un expert lors d'un procès, une personne désignée par le Client, 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 ou d'un COC 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 ou du COC.

Le Vérificateur procède à la validation de la signature électronique selon l'ensemble des modalités prévues dans la politique de la PSGP.

1.4 Usages et applications concernés par la PSGP

La présente PSGP 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.

Le Client peut utiliser le Service PSM pour toutes les Transactions métiers de son choix dans les limites fixées dans le contrat de Service, étant précisé que seul le Client apprécie l'adéquation du type de Service (Choisi parmi ceux identifiés aux § 1.1) par rapport à ses besoins juridiques qu'il définit pour chacun des Documents métiers.

Les Signatures électroniques, les Fichiers de preuves et les Fichier de preuves simplifiés créées dans le cadre du Service PSM ainsi que les COC crées par DTM peuvent servir à titre de preuve au même titre qu'un écrit sur support papier, conformément à l'article 1366 du Code Civil, dans la mesure des principes exposés dans de la présente PSGP.

Il est à noter que le Document métier peut être scellé électroniquement à l'aide d'un cachet électronique avancé par DocuSign France au nom du Client ou d'une entité désignée par le Client.

Il est à cet égard précisé que PSM et DTM dans le cadre de la réalisation de ses Services n'interviennent pas sur le contenu des données d'identification du Client et de l'Utilisateur et des Documents métiers.

Les Services identifié au § 1.1 ci-dessus sont regroupés en deux types de niveaux juridiques :

- Avancé : ce qui signifie que la signature ainsi produite est de niveau avancée conformément à l'article 26 du règlement eIDAS.
- Qualifié : ce qui signifie que la signature ainsi produite est de niveau qualifiée conformément à la définition de la signature qualifiée contenue dans l'article 3 du règlement eIDAS et conforment au «

Décret no 2017-1416 du 28 septembre 2017 relatif à la signature électronique » dont l'objet est « Objet : conditions du procédé permettant à une signature électronique de bénéficier de la présomption de fiabilité prévue au deuxième alinéa de l'article 1367 du code civil ».

La valeur juridique dépend donc du type de certificat (référencé par un OID) et des procédures mise en œuvre par l'AE.

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 PSGP au sein de la société DOCUSIGN France est la PMA (Policy Management Authority) de DocuSign France. La PMA 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 du Service 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 en respectant un préavis de trente (30) jours calendaires avant de procéder à tout changement de la présente PSGP susceptible de produire un effet majeur sur lesdits Clients.

DocuSign FRANCE peut modifier la présente politique sans préavis lorsque 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 PSGP, par tous moyens à sa convenance dont notamment le site web de DocuSign France et la messagerie électronique du service client de DocuSign France, 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 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 PMA est l'entité à contacter pour toutes questions concernant la présente PSGP :

- PMA de DocuSign France.
- https://www.docusign.fr/ (Les informations de contacts sont disponibles sur cette page).
- DocuSign France – 9-15 rue Maurice Mallet - 92131 Issy-les-Moulineaux Cedex – France.

Les termes qui sont utilisés dans la présente PSGP avec une majuscule auront la signification décrite dans l'annexe 1 « Définitions ».

2 IDENTIFICATION ET AUTHENTIFICATION

2.1 Utilisateur

L'authentification et l'identification des identités (nom et prénom) des Utilisateurs et la récupération sûre des adresses de courrier électroniques et le cas échéant des numéros de téléphones portables est effectuée par l'AE qui définit les règles et procédures pour construire et vérifier l'identité des Utilisateurs en fonction des types de Services (donc des types de Certificats et donc du choix d'un OID parmi ceux listé au § 1.1 ci-dessus).

Ces règles sont définies dans un document propre à l'AE (politique d'enregistrement). L'AE transmet l'ensemble des informations nécessaires au Service afin de permettre à DocuSign FRANCE de porter l'identité dans les certificats et d'utiliser dans le cadre du Protocole de consentement le cas échéant les adresses de courriers et les numéros de téléphone portable transmis par l'AE.

Par défaut, l'identification et l'authentification de l'Utilisateur est effectuée en premier lieu avant l'opération de signature. Si cette opération d'authentification et d'identification de l'Utilisateur a lieu après l'opération de signature, alors le Client ne doit pas donner le Document métier ainsi signé tant qu'il n'a pas procédé à une authentification et identification de l'Utilisateur valide et qui confirme l'identification de l'Utilisateur. Si cette confirmation ne peut être obtenue alors toutes les copies de l'Original doivent être détruites et non délivrées à l'Utilisateur.

Par conséquent l'Identité de l'Utilisateur portée dans le Certificat Utilisateur et donc dans l'Original (Document métier signé par l'Utilisateur) a une sécurité directement liées à la sécurité des procédures appliquées par l'AE pour ; identifier et authentifier l'Utilisateur à savoir vérifier qu'il possède bien le nom et prénom tel que porté dans le Certificat émis pour l'Utilisateur et récupérer le numéro de téléphone portable et l'adresse de courrier électronique (si requis par le Protocole de consentement et utilisé par l'AC).

Le niveau de sécurité requis pour l'AE et les procédures que l'AE doit appliquer est défini dans les PC qui s'appliquent aux types de Certificats utilisés dans les Services. Au sein des PC, ces règles sont identifiées par les OIDs qui sont donnés au § 1.1. Dans tous les cas, les Autorités de Certification (AC), utilisées pour l'émission de ces Certificats sont sous le contrôle de DocuSign France et gérées dans ces data center et sont listées sur le site suivant https://www.docusign.fr/societe/politiques-de-certifications.

Par défaut le Fichier de preuve émis par DocuSign France, tout comme le COC émis par DTM, ne contient pas les preuves des opérations d'authentification et d'identification de l'Utilisateur (comme par exemple un extrait des informations de la carte nationale d'identité de l'Utilisateur).

En fonction des types de Services, les données de preuves issues de la procédure d'identification et de d'authentification issues de l'AE sont disponibles comme suit :

- Avancée :
    - SBS EU Advanced (avec DTM uniquement) : 1.3.6.1.4.1.22234.2.14.3.33 : auprès du Client seulement.
    - SBS EU Advanced with IDV (avec DTM uniquement) : 1.3.6.1.4.1.22234.2.14.3.33 : auprès du Client seulement qui peut utiliser DTM pour stocker les preuves fournies par le service IDV.
    - ID check for AES (avec DTM uniquement) : 1.3.6.1.4.1.22234.2.14.3.32 (certifié ETSI 319 411-1 LCP) : auprès de DocuSign France qui les mets dans le Fichier de preuve.
    - Client qui est Autorité d'Enregistrement (AE), certifié ETSI, et utilise le Service sans passer par DTM : 1.3.6.1.4.1.22234.2.14.3.32 (certifié ETSI 319 411-1 LCP) : auprès de DocuSign France qui les mets dans le Fichier de preuve et de l'AE.
    - Client est AE et utilise le Service sans passant par DTM 1.3.6.1.4.1.22234.2.14.3.33 : auprès du Client seulement qui peut aussi, si le Client le souhaite, pousser tout ou partie de ces éléments de preuves d'identification dans le Fichier de preuve.
- Qualifiée qui sont couvert par les OIDs de PC suivant :

- ID check in person for QES (avec DTM uniquement) : 1.3.6.1.4.1.22234.2.14.3.31(certifié ETSI 319 411-2 QCP n-qscd) : auprès de DocuSign France qui les mets dans le Fichier de preuve.
- ID check remote for QES (avec DTM uniquement) : 1.3.6.1.4.1.22234.2.14.3.31 (certifié ETSI 319 411-2 QCP n-qscd) : auprès de DocuSign France qui les mets dans le Fichier de preuve.
- Client qui est Autorité d'Enregistrement (AE), certifié ETSI, et utilise le Service sans passer par DTM : 1.3.6.1.4.1.22234.2.14.3.31 (certifié ETSI 319 411-2 QCP n-qscd) : auprès de l'AE ou de DocuSign France qui les mets dans le Fichier de preuve et de l'AE.

2.2 Client

Il est à noter que le Client a la possibilité d'utiliser un cachet électronique, au sens de la définition de cachet électronique contenu à l'article 3 du règlement eIDAS, pour être apposé sur les Document métiers que l'Utilisateur signe. Dans le cadre de tous les Services, DocuSign France n'utilise pour les Clients que des Certificats de cachet électronique au nom d'une entité légale choisit par le Client qui sont certifiés conformé aux standards de l'ETSI 319 411-1 LCP ou 319 411-2 QCP-L (Certificat qualifié de cachet électronique par l'ANSSI). Par conséquent, le nom de l'entité légale contenu dans ces Certificats de cachet électronique est toujours vérifié suivant les standards de l'ETSI et de l'ANSSI en fonction du niveau de Certificat choisi par le Client. Les AC utilisées pour l'émission de ces Certificats de cachet électronique sont sous le contrôle de DocuSign France et sont listées sur le site suivant https://www.docusign.fr/societe/politiques-de-certifications.

2.3 DocuSign France

DocuSign France appose un cachet électronique sur les Fichiers de preuve et les Fichiers de preuve simplifiés qui sont créés dans le cadre de certains types de Service. Ce cachet électronique est géré par une AC sous le contrôle de DocuSign France dans ces data center. Ce Certificat de cachet électronique permet dons d'identifier l'entité légale DocuSign France.

3 DOCUMENT METIER ET ORIGINAL

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 ;
- Déterminer les mesures de sécurité applicables aux Documents métiers pour l'élaboration et le stockage avant son utilisation dans le cadre des Services.
- Déterminer les mesures de sécurité applicables aux Originaux pour l'élaboration et le stockage après son utilisation dans le cadre des Services.
- De gérer la présentation du Document métier à l'Utilisateur en fonction des fonctions de visualisation des Documents métiers disponibles dans les Services ;
- Définir si le Document métier doit être scellé à l'aide d'un cachet électronique au nom du Client (ou une entité légale désignée par le Client).

Le format de Documents signés, donc de l'Original, autorisé est PDF. Le format de Document métier est libre pour les services utilisant DTM dans la mesure où il sera toujours transformé en PDF avant d'être utilisé par les Services. Le format de Document métier est PDF pour tous les services n'utilisant pas DTM.

4 PROTOCOLE DE CONSENTEMENT ET DONNEES D'ACTIVATION DE LA SIGNATURE

Il appartient au Client, ou à toute entité légale désignée par le Client, de définir et choisir le Protocole de consentement et les données d'activation à utiliser dans le Protocole de consentement pour réaliser l'opération de signature en fonction des Utilisateurs, des types de Documents métiers et des types de Transaction uniquement dans le cadre des Services sans DTM et pour les OIDs 1.3.6.1.4.1.22234.2.14.3.33.

Dans le cadre des OIDs 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32 sans DTM, le Client définit, en concertation avec DocuSign France qui valide ou pas, le Protocole de Consentement et les données d'activation à utiliser dans le Protocole de consentement pour réaliser l'opération de signature. Les données d'activation à utiliser dans le Protocole de consentement pour réaliser l'opération de signature sont soit un code OTP envoyé par SMS au numéro de téléphone portable de l'Utilisateur communiquée par l'AE à DocuSign France ou suivant un procédé autorisé pour le QSCD PSM (Cf. https://www.a-sit.at/en/confirmation-evaluation/confirmation-body/downloads/ qui est le certificateur et https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds qui notifie le QSCD « Protect & Sign »).

Pour les services avec DTM, c'est DocuSign France qui définit le Protocole de Consentement et les données d'activation pour l'opération de signature qui sont en fonction du type de Service :

- 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32 : code OTP envoyé par SMS au numéro de téléphone portable de l'Utilisateur communiquée par l'AE à DocuSign France ou procédé autorisé pour le QSCD PSM ;

- 1.3.6.1.4.1.22234.2.14.3.33 : code OTP envoyé par SMS au numéro de téléphone portable de l'Utilisateur communiquée par l'AE à DocuSign France ou code d'accès saisi dans DTM par l'AE et transmis à DocuSign France par DTM et à l'Utilisateur par l'AE.

Le Protocole de consentement est affiché par DocuSign France ou par l'Application Client, 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 » soit en montrant le Document métier dans le Protocole de Consentement soit en indiquant une référence au Document métier dans le Protocole de Consentement que l'Utilisateur aura au préalable visualiser dans l'interface de DTM ou de l'Application Client.

La sécurité de l'activation de l'opération de signature via le Protocole de consentement à l'aide des données d'activation dépend de la sécurité de la procédure utilisée par l'AE pour recueillir, gérer et/ou distribuer les informations de contacts (numéro de téléphone portable, adresse de courrier électronique, …) et/ou moyens de mise en œuvre des données d'activation (code d'accès, token, case à cocher, …) et/ou aux moyens de connexion et d'authentification technique de l'Utilisateur à l'Application Client qui met en œuvre le Protocole de consentement pour une signature à distance et/ou au moyen et procédure d'utilisation du Terminal d'affichage qui affiche le Protocole de consentement à l'Utilisateur pour une signature en face à face en fonction du type de Service.

Le Protocole de consentement doit toujours laisser à l'Utilisateur la possibilité de refuser de signer le Document métier.

5 HORODATAGE

Au moment de chacune des signatures réalisées au nom de l'Utilisateur et d'un scellement avec un cachet électronique au nom du Client par DocuSign FRANCE une Contremarque de temps qualifiée est apposée pour chaque signature.

Les Contremarques de temps sont donc contenues dans l'Original comme le Certificat.

Le Fichier de preuve est aussi cacheté avec en plus une Contremarque de temps qualifiée.

Les dispositions relatives à la génération des Contremarques de temps qualifiées sont décrites dans la politique d'horodatage de DocuSign FRANCE (OID 1.3.6.1.4.1.22234.2.6.5.8) qui est disponible sur le site suivant https://www.docusign.fr/societe/politiques-de-certifications.

6 STATUT DU CERTIFICAT

Le Document métier signé contient toujours l'information du statut du Certificat (donc dans l'Original).

Au moment de chacune des signatures réalisées au nom du Client et de l'Utilisateur par DocuSign FRANCE un jeton OCSP ou la CRL en cours de validité est apposé pour chaque signature.

L'utilisation de l'algorithme RSA 2048 avec la fonction de hachage est SHA-2 est utilisée pour signer les jetons OCSP et CRL apposées sur le Document métier.

Les jetons OCSP et CRL sont émises par les AC de DocuSign France.

7 TRANSACTION DE SIGNATURE PSM

7.1 Sans DTM

Ce chapitre expose le processus de signature d'un Document métier et de constitution du Fichier de preuve de manière générique. La cinématique pour chaque Client est précisée dans le document de mise en production et/ou dans le contrat établi entre le Client et DocuSign FRANCE.

Le Client devra faire autant d'appels au Service PSM qu'il y a de signataires pour signer le Document métier. Chaque appel fait l'objet d'une nouvelle Transaction. 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 configuré dans PSM pour le Service choisit. 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 et ainsi de suite.

Le ou les Document(s) métier, complété de l'identité de l'Utilisateur et des informations utiles pour l'activation de la signature (numéro de téléphone portable …) est ensuite signé par le Connecteur Client afin de fabriquer automatiquement une requête Client.

La requête Client signée est transmise à PSM par l'Application Client soit directement via une session TLS mutuellement authentifiée. Seule l'Application PSM peut extraire les informations qui y sont contenues.

PSM applique un ou plusieurs cachets électroniques de personnes morales sur le Document métier, si le Client en a fait le choix.

L'utilisateur est alors dirigé vers le service PSM qui met en œuvre le Protocole de consentement (Cf. § 4) avec un délai maximum défini par le Client. Dans le cadre des OID 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32 ce délai est définit et validé par DocuSign France.

Une fois que l'Utilisateur a accepté de signer le Document métier conformément aux conditions du Protocole de consentement et en utilisant ces données d'activation de signature, PSM :

- Génère la bi-clé (RSA 2048) de l'Utilisateur, ou utilise une bi-clé pré-générée à l'avance et non utilisée (sauf pour les OID 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32), pour l'Utilisateur dans un HSM (Module cryptographique certifié FIPS 140-2 level 3 ou CC EAL 4+) ;
- Demande la génération du Certificat Utilisateur valables pour cette Transaction UNIQUEMENT en s'adressant à une AC hébergée chez DOCUSIGN FRANCE ;
- Procède à la génération du hash SHA-2 du Document métier ;
- Signe avec la clé Utilisateur le Document métier et pour l'OID 1.3.6.1.4.1.22234.2.14.3.31 les CGUs du Service qui sont transmises par l'Application Client ;

- Détruit la bi-clé Utilisateur générée précédemment ;
- Demande les informations de statut du Certificat et appose une Contremarque de temps qualifiée sur Document métier ainsi signé afin de constituer l'Original ;
- Conserve en base de données les éléments de Transaction (sauf le Document métier et l'Original) à des fins de preuves ;
- Constitue et stocke les éléments du Fichier de preuve qui sont chiffrés dans le système de fichier (AES avec une clé RSA dans un HSM certifié (FIPS 140-2 level 3 ou CC EAL 4+) ;
- Crée une enveloppe contenant l'AR et l'Original que l'Application Client peut télécharger en s'authentifiant en TLS.

Lors de l'appel pour la 1ère Transaction, PSM crée un nouveau Dossier et renvoie l'identifiant de dossier à l'Application Client. Pour les Transactions suivantes, l'Application Client fournit cet identifiant dans la Requête Client, ce qui permet à PSM de lier ces Transactions au même Dossier. Pour le dernier Utilisateur, l'Application Client indique dans la requête Client que la Transaction est la dernière du Dossier. A l'issue de cette Transaction, PSM clôt le Dossier et génère le Fichier de preuve. Tant que le Ficher de preuve n'est pas généré, les Originaux et les éléments permettant de constituer le Fichier de preuve sont conservés chiffrés par PSM. 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, PSM gère l'archivage temporaire du Fichier de preuve stocké chiffré dans le système de fichier. 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 PSM n'en conserve aucune trace. Seules les données minimales (données personnelles des Signataires, identifiant de Transaction, empreinte des Documents, …) sont conservées en base de données, et dans les sauvegardes des bases de données, à titre de preuve pour DocuSign France et permettent de reconstruire un Fichier de preuve simplifié (pendant une période de temps maximale définit dans le contrat avec le Client). L'archivage temporaire est relayé par un archivage électronique de longue durée dans le PSAE choisit par le Client. 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 : PSM archive chez un PSAE choisit par DocuSign France, les Fichiers de preuve permettant ainsi à des Administrateurs habilités du Client d'aller les rechercher dans le coffre électronique du PSAE. C'est DocuSign France qui gère les accès au coffre électronique du Client en accord avec les procédures du PSAE. La liaison entre PSM et le PSAE est sécurisée en TLS. Des procédures de surveillance de l'état des Fichiers de preuve permettent la gestion des reprises sur erreur d'archivage.
- Le Client gère l'archivage du fichier de preuve avec un PSAE de son choix : L'Application Client récupère le Fichier de preuve auprès de PSM lors d'une session TLS mutuelle authentifiée ou alors PSM pousse le Fichier de preuve dans le coffre du PSAE. PSM 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.

7.2 Avec DTM

Ce chapitre expose le processus de signature d'un Document métier et de constitution du Fichier de preuve (sauf pour l'OID 1.3.6.1.4.1.22234.2.14.3.33 pour lequel en ce cas DocuSign France ne génère pas de Fichier de preuve mais le Client possède le COC à titre de fichier de preuve) de manière générique.

Le ou les Document(s) métier et l'identité de l'Utilisateur et des informations utiles pour l'activation de la signature (numéro de téléphone portable, adresse de courrier électronique …) est transmise par l'Application Client ou manuellement par une personne autorisée dans DTM. Il peut y avoir plusieurs signataires en même temps. L'ensemble est associé à un identifiant de Transaction (appelé Enveloppe ID qui est unique et définit et géré par DTM). DTM invite le ou les Utilisateur(s) à signer le ou les Document(s) métier par courrier électronique, saisi par le Client dans DTM, ou suivant l'intégration par interface machine entre l'Application Client et DTM choisit par le Client.

PSM applique un ou plusieurs cachets électroniques de personnes morales sur le Document métier, si le Client en a fait le choix dans DTM. Il est à noter que le cachet électronique peut être apposé avant ou après une signature Utilisateur.

L'utilisateur est alors dirigé vers le service DTM qui lui permet de visualiser le ou les Document(s) métier et ensuite vers PSM qui met en œuvre le Protocole de consentement (Cf. § 4) avec un délai maximum défini par DocuSign France. Pour se faire, PSM procède à la récupération auprès de DTM du début de hash SHA-2 du Document métier ainsi que des informations d'identité et de contacts (numéro de téléphone, adresse de courrier électronique, …) nécessaire à l'activation de la signature de l'Utilisateur et met ensuite en œuvre le Protocole de consentement.

Une fois que l'Utilisateur a accepté de signer le Document métier conformément aux conditions du Protocole de consentement et en utilisant ces données d'activation de signature, PSM :

- Génère la bi-clé (RSA 2048) de l'Utilisateur, ou utilise une bi-clé pré-générée à l'avance et non utilisée (sauf pour les OID 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32), pour l'Utilisateur dans un HSM (Module cryptographique certifié FIPS 140-2 level 3 ou CC EAL 4+) ;
- Demande la génération du Certificat Utilisateur valables pour cette Transaction UNIQUEMENT en s'adressant à une AC hébergée chez DOCUSIGN FRANCE ;
- Complète et signe avec la clé Utilisateur le hash du Document métier et pour l'OID 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32 quand DocuSign France est l'AE les CGUs du Service ;
- Détruit la bi-clé Utilisateur générée précédemment ;
- Demande les informations de statut du Certificat et appose une Contremarque de temps qualifiée sur la signature du hash et ainsi créé la capsule de signature du Document métier ;
- Conserve en base de données les éléments de Transaction récupérer auprès de DTM à des fins de preuves ;
- Retourne à DTM la capsule de signature du Document métier. DTM crée l'Original à partir de la capsule de signature et du Document métier ;
- Uniquement pour les OIDs 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32 : constitue et stocke les éléments du Fichier de preuve qui sont chiffrés dans le système de fichier (AES avec une clé RSA dans un HSM certifié (FIPS 140-2 level 3 ou CC EAL 4+). PSM gère l'archivage temporaire du Fichier de preuve stocké chiffré dans le système de fichier et le pousse ensuite dans le coffre électronique de DocuSign France chez le PSAE.

8 MISE A DISPOSITION DU DOCUMENT METIER SIGNE (ORIGINAL)

Il appartient au Client de mettre en œuvre les moyens et procédures nécessaires pour permettre à disposition pour chaque Utilisateur l'Original conformément à l'article 1375 du Code Civil.

8.1 Avec DTM

Dans les Services avec DTM, c'est la plate-forme DTM qui met à disposition l'Original auprès de l'Application et/ou de l'Utilisateur en fonction de la configuration choisi par le Client (envoie par courrier électronique à

l'Utilisateur, téléchargement dans DTM, récupération par interface machine dans DTM par l'Application Client, …). Pour les OIDs 1.3.6.1.4.1.22234.2.14.3.31, PSM transmets par courrier électroniques les CGUs du Service signés à l'Utilisateur.

8.2 Sans DTM

PSM met à disposition l'Original de l'Application Client qui doit le récupérer. Pour l'OID 1.3.6.1.4.1.22234.2.14.3.31, PSM met à disposition de l'Application Client les CGUs du Service signées qui doit les récupérer. Le Client définit ensuite les modalités de remises de l'Original, et le cas échéant les CGUs du Service signées, auprès des Utilisateurs.

9 FICHIER DE PREUVE

9.1 Eléments constituant le fichier de preuve

9.1.1 Avec DTM

Dans tous les types de Service qui utilisent DTM, DTM produit le COC pour l'ensemble de la Transaction comme décrit ici : https://support.docusign.com/guides/ndse-user-guide-history-coc. Il est à noter que DTM permet aussi d'utiliser un proof service afin de stocker les éléments de preuves de l'identification et de l'authentification de l'Utilisateur issus du service de vérification, comme indiqué ici : https://support.docusign.com/en/guides/ID-Verification-ID-Evidence-Q-A, d'identité de DTM si le Client a pris ce service.

Pour l'OID 1.3.6.1.4.1.22234.2.14.3.33, PSM ne produit pas de Fichier de preuve et en ce cas la preuve de l'opération de signature est apportée par le COC produit par DTM pour chaque Transaction.

Pour l'OID 1.3.6.1.4.1.22234.2.14.3.32 et 1.3.6.1.4.1.22234.2.14.3.31, PSM créé un Fichier de preuve suivant les modalités décrites ci-dessous au § 9.1.2 en y incluant les éléments de preuves de l'identification et authentification de l'Utilisateur créé par l'AE.

9.1.2 Sans DTM

Le Fichier de preuve est constitué des éléments suivants :

- L'OID de la PSGP ;
- Requête Client ;
- Le Document métier soumis, préparé et présenté si transmis par l'Application Client ;
- L'Original ou la capsule de signature si le Document n'a pas été transmis ;
- L'identifiant de Transaction ;
- Les éléments d'identité de l'Utilisateur ainsi que les informations de contacts de l'Utilisateur utilisés pour l'activation de la signature dans le cadre du Protocole de consentement ;
- Les éléments du Protocole de consentement (copie d'écran d'exemple de la page de consentement, case à cocher, …) ;
- Fiche introductive et fiche descriptive qui contient la traçabilité des opérations et la description des éléments constitutifs du Fichier de preuve ;
- Eléments additionnels poussé par l'Application Client ou l'AE.

Le Fichier de preuve est scellé et horodaté électroniquement par DocuSign FRANCE.

9.2 Archivage du fichier de preuve

9.2.1 Avec DTM

Pour l'OID 1.3.6.1.4.1.22234.2.14.3.32 et 1.3.6.1.4.1.22234.2.14.3.31, c'est DocuSign France qui possède le Fichier de preuve et l'archive dans son coffre électronique hébergé par son PSAE. Ce Fichier de preuve est archivé pendant 10 ans. Le Client ne possède pas d'accès technique pour récupérer ce Fichier de preuve. Si le Client souhaite avoir accès à un Fichier de preuve, conformément aux conditions générales du Service, il doit en faire la demande auprès de DocuSign France.

Le Client choisit les modalités et la durée d'archivage du COC. Pour l'OID 1.3.6.1.4.1.22234.2.14.3.31, le COC doit être conservé au moins 7 ans et 10 jours. Il est à noter qu'il est possible de conserver le COC et les Originaux dans DTM ou dans un PSAE connecté à DTM suivant les modalités de durées et suppression définit dans les conditions générales du Service.

Le COC est accessible à l'Utilisateur en fonction de la configuration de DTM choisit par le Client.

9.2.2 Sans DTM

Le Client choisit le PSAE (interne, un PSAE proposé par DocuSign France, …) pour archiver les Fichiers de preuve. La durée de conservation est définie dans le contrat avec le Client. Pour les OIDs 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32 le Fichier de preuve doit être conservés au moins 7 ans et 10 jours par l'AE qu'il y ai eu rétraction ou pas au cours de la Transaction.

Lorsque le Client choisit le PSAE de DocuSign France, alors DocuSign France crée des Administrateurs pour le Client, qui désignent les personnes physiques pour ce rôle, pour la gestion des archives de Fichiers de preuve dans le coffre électroniques. La gestion et l'accès aux archives s'effectue suivant les modalités techniques et les règles de sécurité du PSAE.

L'Utilisateur n'accède pas aux Fichiers de preuve stockés dans le coffre électronique.

9.3 Lisibilité et pérennité

La lisibilité et la pérennité du format de Fichier de preuve sont liées au format de document DOCX (OpenXML) et d'archive de compression 7z/LZMA et au format PDF du COC.

10 VALIDATION ET UTILISATION DE DOCUMENT SIGNE (ORIGINAL)

10.1 Validation de signature et utilisation d'un Original

La Validation de signature d'un Original nécessite la prise de connaissance de la présente PSGP et de ou des PC(s) et de la Politique d'Horodatage afin de comprendre le contexte de la création de signature en fonction des types de Services et des OIDs utilisés. Notamment pour apprécier le niveau de sécurité de l'AE et de l'activation de la signature via le Protocole de consentement.

Le Client définit les moyens disponibles pour le Vérificateur afin qu'il vérifie techniquement les Originaux. Par exemple, utilisation d'un lecteur PDF, d'un service technique de validation du Client ou externe, …

Ce paragraphe définit les principes 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, sauf pour les Service avec DTM et seulement si l'Application Client l'a transmis pour les Services avec DTM, 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 aussi de son contenu.

L'Original au format PDF est autoportant et vérifiable indépendamment par le Vérificateur. Pour la vérification il est nécessaire d'utiliser un logiciel Adobe Reader ou équivalent qui permet de procéder à toutes les vérification techniques (signatures cryptographiques, AC, …).

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 Utilisateur et Client utilisés et Contremarques de temps.
- Supérieure à la durée de validité des Certificats Utilisateur et Client utilisés et Contremarques de temps.

Il donc important de distinguer ces deux périodes pour la Validation d'un Original. Les mesures à prendre par le Client pour permettre la validation d'un Original sont dépendantes de ces 2 périodes.

Le Vérificateur doit appliquer une période de précaution et procéder à des vérifications afin de valider un Original car pour les OIDs 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32 le Certificat de l'Utilisateur est révocable et peut donc être révoqué après l'opération de signature. La révocation n'invalide pas forcément le porté juridique de l'Orignal car ceci dépend en effet des causes de la révocation.

10.1.1 Pendant la période de validité des Certificats utilisés

La validation des signatures (Utilisateur, Client si présente, Contremarque de temps, CRL et OCSP) de l'Orignal et de sa date de création (déterminée grâce à la Contremarque de temps) sont vérifiables pendant la période de validité des Certificats utilisés (Utilisateur, Client et Contremarque de temps) à l'aide des informations fournies par les AC utilisées.

Cette validation technique est à mettre en regard de la sécurité des algorithmes cryptographies comme énoncé par l'ANSSI. DocuSign France n'utilise que des algorithmes en conformité avec les standards de l'ANSSI.

10.1.2 Après la période de validité des Certificats utilisés

Suite à l'expiration de l'AC, par défaut l'AC n'émet plus d'information sur la validité des Certificats émis par cette même AC. Pour l'OID 1.3.6.1.4.1.22234.2.14.3.31, il est à noter que la CRL contient les Certificats Utilisateurs révoqués et expirés et DocuSign France publie pour l'AC expirée une dernière CRL (Cf. PC associée) et la publie sur son site internet.

Suite à la fin de la validité de tous les Certificats utilisés pour un Original (Utilisateur, Client et Contremarque de temps), et si rien n'est convenu entre DocuSign France et le Client pour prolonger leur capacité de vérification, comme l'usage d'un PSAE par exemple qui en fonction du PSAE garantie l'intégrité dans le temps de l'Original, DocuSign France ne s'engage plus sur la capacité de vérification technique 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 sauf pour l'OID 1.3.6.1.4.1.22234.2.14.3.31.

Toutefois DocuSign France peut communiquer sur la robustesse des algorithmes cryptographiques 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 sur l'intégrité de l'Original.

Préalablement à la fin de validité de tous les Certificats, le Client et DocuSign France 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 n'est prévue, il est alors du ressort du Client de définir et de mettre en œuvre les mécanismes de protection permettant de répondre au besoin de conservation (au sens 1366 du code civil) et de validation des signatures des Originaux. De même le Client est averti que la sécurité de l'intégrité de l'Original dépend de la pérennité de la sécurité des algorithme cryptographiques utilisés et que le Client doit suivre les recommandations de l'ANSSI en la matière.

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 le Client.

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.

Les Originaux sont valables au-delà de l'expiration des Certificats qui les protègent à conditions qu'ils soient conservés dans des conditions satisfaisantes l'article 1366 du code civil et qui les préservent des vulnérabilités des algorithmes cryptographiques.

10.2 Vérification des identités

La vérification des identités est effectuée à partir des seuls certificats Utilisateur et Client et du niveau de sécurité des procédures de l'AE. L'AE peut apporter des éléments de preuves supplémentaires en fonction du type de Service utilisé par le Client (par exemple des informations extraites de la pièce d'identité de l'Utilisateur).

10.3 Utilisation du Fichier de preuve et COC

Le Fichier de preuve et le COC est scellé. Par conséquent, il possède des Certificats qui eux aussi expirent comme expliqué ci-dessus dans ce chapitre.

Le Fichier de preuve se valide suivant les mêmes règles définies (Cf. § 10.1 et § 10.2) pour un Original car il est lui aussi scellé et horodaté et les mêmes limites que celles indiquées aux 10.1 et 10.2 s'appliquent.

La sécurité du Fichier de preuve, lorsque les algorithmes cryptographiques ne sont plus sûrs dépend des solutions choisis par le Client pour le conserver intègre au sens 1366 du code civil. En fonction du PSAE choisit par le Client, il est possible de prolonger la sécurité du Fichier de preuve dans le temps malgré l'obsolescence des algorithmes cryptographiques.

Il est à noter que le COC est scellé à chaque téléchargement à partir de DTM. Il sera donc toujours à jour en termes de sécurité algorithmique. Par contre si le Client décide de télécharger et de le conserver dans un PSAE de son choix, les mêmes principes s'appliquent que pour le Fichier de preuve en termes de pérennité.

Le Fichier de preuve et le COC viennent en complément de l'Original afin d'apporter des preuves sur l'opération de signature. Comme indiqué au § 9, dans certains cas le Fichier de preuve et les fonctions DTM peuvent aussi servir à apporter des preuves complémentaires sur l'identification et l'authentification de l'Utilisateur. Ces preuves ainsi constituées dans le Fichier de preuve et le COC sont valables au-delà de l'expiration des Certificats qui les protègent à conditions qu'elles soient conservées dans des conditions satisfaisantes l'article 1366 du code civil et qui les préservent des vulnérabilités des algorithmes cryptographiques.

11 STIPULATIONS JURIDIQUES

Les dispositions de la présente PSGP sont régies par le droit français et le règlement eIDAS.

Les règlement et litiges sont définis dans le contrat avec le Client.

DocuSign France, DocuSign Inc., le PSAE et le Client respectent le règlement RGPD comme indiqué dans les conditions générales des Services et le contrat établit avec le Client.

Les obligations et limites de responsabilité de DocuSign France, DocuSign Inc et du Client sont définies dans les conditions générales des Services et le contrat établit avec le Client.

Les obligations et limites de responsabilité de l'Utilisateur sont définis dans les CGUs.

12 MESURES DE SECURITE NON TECHNIQUES DES OPERATIONS

12.1 DocuSign France

Les mesures de sécurité physiques sont identiques à celles des AC décrites dans les PC (chapitre 5) identifiées par les OID dans les types de Services au § 1.1.

12.2 Pour le Client

Les mesures de sécurité physique à la charge du Client concerne le Connecteur Client (Service sans DTM) et l'Application Client qui est hébergé sur le site informatique d'une entité légale désignée par le Client.

Le Client doit se prémunir des menaces physiques qui viendraient altérer l'intégrité du Connecteur Client (Service sans DTM) et de l'Application Client et des données qu'ils manipulent en déployant des mesures de sécurité conformément aux standards en la matière comme ceux communiqués par l'ANSSI.

De même, le Client s'assure que seuls les personnels autorisés peuvent accéder aux machines qui hébergent le Connecteur Client (Service sans DTM) et l'Application Client.

12.3 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.

13 MESURES DE SECURITE TECHNIQUES

13.1 Pour l'Utilisateur

L'Utilisateur est responsable de la sécurité informatique du Terminal d'affichage qu'il utilise lorsque celui-ci est sous sa responsabilité. Le Termina d'affichage doit être sécurisé suivant les standards en vigueurs en utilisant les règles prescrites par l'ANSSI dans le guide hygiène informatique.

13.2 Pour le Client

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

Le Client doit se prémunir des menaces informatiques qui viendraient altérer l'intégrité du Connecteur Client (Service sans DTM) et de l'Application Client et des données qu'ils manipulent en déployant des mesures de sécurité conformément aux standards en la matière comme ceux communiqués par l'ANSSI.

De même, le Client s'assure par des mesures techniques que seul l'Application Client et les personnels autorisés du Client peuvent mettre en œuvre le Connecteur Client et les Services et ce pour les seules fins de Transaction légitimes au profit du Client et de l'Utilisateur.

13.3 DocuSign France

Les mesures de sécurité techniques sont identiques à celles des AC décrites dans les PC (chapitre 6) identifiées par les OID dans les types de Services au § 1.1.

13.4 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 (ou la politique d'archivage le cas échéant) du PSAE.

14 COMPROMISSION ET PLAN DE CONTINUITE

14.1 Compromission

La gestion de la compromission des Services est identique à celui des AC décrit dans les PC (chapitre 5.7 et 5.8) identifiées par les OID dans les types de Services au § 1.1.

14.2 Fin d'activité

Les modalités de la fin d'activité sont définies dans le contrat avec le Client et dans les PC (chapitre 5.7 et 5.8) identifiées par les OID dans les types de Services au § 1.1.

14.3 Plan de continuité

Le plan de continuité est identique à celui des AC décrit dans les PC (chapitre 5.7 et 5.8) identifiées par les OID dans les types de Services au § 1.1.

15 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits de la PSGP sont réalisés dans le cadre des audits des AC comme définit dans les PC (chapitre 8) identifiées par les OID dans les types de Services au § 1.1.

16 DEFINITIONS

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.

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 Transaction. L'Application du Client héberge le Connecteur Client dans le cas des Services sans DTM.

Application « Protect and Sign (Personal Sign) » (PSM) : 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) est incluse dans le Kit de connexion livré au Client pour installation dans un environnement informatique de son choix.

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 choisit par le Client.

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.

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.

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.

Connecteur Client : désigne le module logiciel (une des composantes de PSM) livré par DocuSign FRANCE dans le Kit de connexion, et qui est installé dans une Application Client en vue de l'utilisation du Service (uniquement pour un Service sans DTM). Le module assure toutes les opérations cryptographiques réalisées nécessaires à l'implémentation de la communication sécurisée avec PSM ainsi que les Requêtes Client.

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.

Document métier : désigne un document électronique créé par le Client sous un format PDF et complété des informations relatives à l'Utilisateur.

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 au travers du Protocole de consentement (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, case à cocher et bouton d'activation, …).

Dossier : 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 ».

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.

Ficher de preuve simplifiée : désigne l'ensemble des données récupérées en base de données permettant de créer une preuve pour une Transaction et contenant moins d'éléments que le Fichier de Preuve. Ce fichier est cacheté et horodaté par DocuSign France et il est au format PDF.

Identifiant de Transaction (OperationId) : 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.

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.

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 et des vérificateurs de Certificat.

Preuve de signature DocuSign (aussi désigné par « certificat de réalisation », « Summary », « certificate of Completion » ou « COC »)" signifie un fichier généré par la demande de signature DocuSign qui contient toutes les informations relatives au signataire, à l'expéditeur du document électronique, à l'identifiant unique DTM de la transaction utilisée pour gérer le document électronique. Un COC dédié associé à chaque document électronique, signataire et expéditeur est généré dans le but de prouver la validité d'une transaction. Le COC est scellé par DocuSign Inc. Le COC est mis à la disposition du client dans DTM.

Protocole de consentement : désigne l'ensemble des règles de recueil de consentement d'un Utilisateur pour un Service à savoir la définition des actions à réaliser par l'Utilisateur sur le Terminal d'affichage pour (i) activer la signature du ou des Document(s) métier proposé(s) par l'Application Client, (ii) visualiser et valider les informations utilisées pour la création de l'identité de l'Utilisateur et les informations pour l'activation de la signature (numéro de téléphone portable par exemple) et (iv) les modalités de visualisation du Document métier ou de sa référence présenté et du message d'acceptation (ou de refus) associé (case à cocher par exemple, bouton accepter ou refuser, …).

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 et le Protocole de consentement.

Transaction : désigne l'échange électronique entre le Client et chaque Utilisateur réalisé au moyen d'un Terminal d'affichage et du Service et au cours duquel le Client propose pour signature, suivant un Protocole de consentement, un ou plusieurs Document(s) métier(s) à un Utilisateur identifié et authentifié par l'AE, afin que l'Utilisateur manifeste son consentement à le(s) signer, ou refuse de le(s) signer. Une Transaction est identifiée de façon unique par un Identifiant de transaction et/ou un enveloppe ID (identifiant DTM).

