TSP 2 DocuSign France
TSA Disclosure statement V 1.0

TSP informations de contact :

La PMA est l'entité à contacter pour toutes questions concernant le présent document :

- 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.

1. OBJET

Les présentes TSA Disclosure Statement, au sens de l'ETSI, ont pour objet de définir les conditions juridiques et techniques aux termes desquelles DocuSign France met à disposition de ses Clients et des Vérificateur de contremarque de temps (aussi appelé UC) le Service d'Horodatage qui permet d'émettre des Contremarque de temps qualifiées au sens eIDAS.

Ce document constitue les conditions générales d'utilisation du service d'horodatage mais ne constitue pas le contrat entre le Client et Docusign.

2. DEFINITIONS

Les termes qui suivent auront la signification définie lorsqu'ils seront utilisés dans le cadre des présentes.

Application utilisatrice : désigne un ensemble d'applications informatiques qui fait appel au Service d'horodatage. Plus particulièrement, ce terme désigne l'ensemble cohérent d'informations et de programmes informatiques ayant pour objet de transmettre des Demandes de contremarque de temps à l'UH.
Autorité de Certification Fille (*ou **AC Fille***) : désigne la (*ou les*) entité(*s*) hiérarchiquement rattachée(*s*) à l'AC Racine et certifiée(*s*) par cette dernière, et qui assure(*nt*) la gestion du cycle de vie des Certificats d'UH.
Autorité de Certification Racine (*ou **AC Racine***) : désigne l'entité de plus haut niveau dans l'Infrastructure à Clés Publiques et qui certifie les AC filles.
Autorité de Certification d'Horodatage (*ACH*) : désigne une entité qui délivre les Certificats électroniques aux UH mises en œuvre par l'AH et rattachées à cette dernière. Cette ACH gère aussi les listes de certificats révoqués pour les certificats d'UH. L'ACH applique sa Politique de Certification (*PC*) pour la gestion des certificats d'UH.
Autorité d'Horodatage (*AH*) : désigne une entité qui a en charge l'application d'au moins une PH en s'appuyant sur une ou plusieurs UH. L'AH délivre des contremarques de temps avec une précision donnée, et à partir de Source de temps choisies.
Calcul d'empreinte numérique : désigne le processus algorithmique qui consiste à obtenir une empreinte numérique à partir d'une donnée électronique.
Certificat(s) d'AC : désigne(*nt*) un(*des*) fichier(*s*) électronique(*s*) émis pour une AC Fille par l'AC Racine.
Certificat(*s*) UH : désigne un Certificat Cachet NCP+ contenant l'identité d'une unique UH émis par une ACH et certifiant du lien entre une identité et la Clé publique de la personne physique titulaire du Certificat.
Certificat d'AC auto signé : désigne un certificat d'AC signé par la clé privée de cette même AC.
Client : désigne l'entité ayant contracté avec Docusign pour bénéficier du Service d'horodatage de DocuSign France uniquement dans le cadre d'utilisation des service de création de signature qualifiée et avancée et de création de cachet avancé vendus par Docusign et mis en œuvre par DocuSign France.
Chemin de certification (*ou **chaîne de confiance**, ou **chaîne de certification***) **:** désigne l'ensemble d'AC où chaque AC est certifiée par une AC d'échelon supérieur. À titre d'illustration, une AC délivrant des certificats à des UH peut elle-même être certifiée par une AC, dite « AC intermédiaire », qui à son tour peut être certifiée par une autre AC intermédiaire, ainsi de suite jusqu'à l'AC de plus haut niveau, auto signée, l'ACR.
Contremarque de Temps : Donnée signée qui lie une représentation d'une donnée à un temps particulier fournit par une UH, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là. Cette contremarque de temps

est signée électroniquement par une UH. Une contremarque de temps permet d'établir la preuve que l'empreinte numérique existe à la date et l'heure qui y figure.

Coordinated Universal Time (*UTC*) : désigne l'échelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF 460-6 (2002): "Standard-frequency and time-signal emissions".

Date et heure d'UH (*temps particulier*) : désigne une date et une heure particulière qui sont créées par l'horloge interne de l'UH. L'horloge interne de cette UH est synchronisée avec des Source(*s*) de temps externe(*s*) afin de créer une date et une heure avec une précision donnée au regard du temps UTC. Dans le cadre de la PH, la date et l'heure d'UH de DocuSign France contenues dans les contremarques de Temps sont la date et l'heure légale française, construite à partir de la synchronisation avec plusieurs sources de temps UTC.

Déclaration des pratiques d'horodatage (*DPH*) : Une DPH identifie les pratiques (*organisations, procédures opérationnelles, moyens techniques et humains*) que l'AH applique dans le cadre de la fourniture de ses services d'horodatage et en conformité avec la ou les PH qu'elle s'est engagée à respecter. Elle n'est pas publique.

Demande de contremarque de temps : désigne la requête qui est soumise par un Client à l'AH pour l'émission d'une contremarque de temps. Cette requête contient l'empreinte numérique de la donnée à horodater.

Données électroniques : désigne un ensemble de données structurées pouvant faire l'objet de traitement(*s*) informatique(*s*) par les applications informatiques du Client. Le calcul de l'empreinte numérique est effectué à partir de cet ensemble de données.

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

Jeton d'horodatage : Voir **contremarque de Temps**.

Liste de certificats révoqués (*LCR*) : désigne la liste signée électroniquement par l'ACH et qui contient l'ensemble des identifiants des certificats d'UH qui ont été révoqués avant leur date d'échéance.

Politique de Certification (*PC*) : désigne l'ensemble de 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 certificats et de toutes les composantes de l'IGC intervenant dans l'ensemble du cycle de vie d'un Certificat.

Les versions applicables des PC des AC sont les versions en vigueurs au jour de l'ouverture du Service et sont consultables à l'adresse web suivante : https://www.docusign.fr/societe/politiques-de-certifications. Les versions successives des PC seront mises à la disposition des Clients et des Vérificateurs sur le site Internet de DocuSign France. Les Clients seront avertis de la modification des PC conformément aux dispositions de l'article 9 de ladite PC.

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

Précision : désigne la différence maximale autorisée entre la date et l'heure UTC fournie par la Source de temps et la date et heure (*Cf. Date et heure d'UH)* de l'horloge de l'UH qui est utilisée pour générer les contremarques de temps.

Prestataire de services d'horodatage (PSHE) : Le règlement eIDAS introduit et définit les prestataires de service de confiance (*PSCO*). Un PSHE est un type de PSCO particulier. Un PSHE se définit comme toute personne ou entité qui est responsable de la génération et de la gestion de contremarques de temps, vis-à-vis de ses abonnés et des utilisateurs de ces contremarques de temps. Un PSHE peut fournir différentes familles de contremarques de temps correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSHE comporte au moins une AH mais peut en comporter plusieurs en fonction de son organisation. Un PSHE est identifié dans les certificats de clés publiques des UH dont il a la responsabilité au travers de ses AH.

Ressource Cryptographique Matériel (*RCM*) : désigne le produit de sécurité comportant une ressource cryptographique matérielle et qui est dédié à la mise en œuvre des fonctions d'horodatage de l'UH, notamment la génération, la conservation et la mise en œuvre de la clé privée de signature de l'UH ainsi que la génération des contremarques de temps.

Service d'horodatage (*ou Service*) : désigne l'ensemble des prestations réalisées par DocuSign France nécessaires à la génération et le cas échéant à la gestion de contremarques de temps.

Source de temps : désigne la composante qui fournit une date et une heure (*temps*) UTC avec une précision donnée (*antenne GPS, onde radio et serveur source de temps NTP*).
Synchronisation : désigne l'opération qui consiste pour une UH à comparer la date et l'heure issue de l'horloge interne à la date et l'heure fournie par une ou des source(*s*) de temps. Cette comparaison sert à maintenir et donc garantir dans le temps que son horloge interne délivre une date et une heure avec un écart maximal correspondant à la précision de l'AH annoncée par rapport au temps UTC.
Système d'horodatage : désigne l'ensemble des UH et des composants d'administration et de supervision utilisés pour fournir des services d'horodatage.
Unité d'Horodatage (*UH*) : désigne l'ensemble de matériels et de logiciels utilisés pour la création de contremarques de temps. L'UH est caractérisée par une identité certifiée, contenu dans un Certificat d'UH, par une AC et une clé unique de signature de contremarques de temps. L'UH construit une date et une heure d'UH qu'elle utilise pour les contremarques de temps qu'elle signe.
UTC(*k*) : Temps de référence réalisé par le laboratoire "k" et synchronisé avec précision avec le temps UTC, dans le but d'atteindre une précision de ±100 ns. Une liste des laboratoires UTC(k) est donné par le document Circular T publié par BIPM (https://www.bipm.org/).
Vérificateur de contremarque de temps : désigne l'entité (*personne ou système*) qui valide une contremarque de temps émise sous une PH et DPH données par une AH donnée afin de s'assurer de l'existence d'une donnée électronique à une date et une heure donnée.
Validation de contremarque de temps : désigne l'action du Vérificateur de contremarque de temps qui consiste à vérifier que la contremarque est valide. La vérification d'une signature électronique de contremarque de temps consiste en les opérations suivantes :

- Vérification de la signature de la contremarque de temps ;
- Vérification et extraction de la date et de l'heure contenues dans la contremarque de temps.
- Identification et extraction du certificat de l'UH 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'UH ayant émis la contremarque de temps.
- Vérification de l'état de validité du certificat de l'UH 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'UH ayant émis la contremarque de temps.

Si l'ensemble de ces opérations est positif, alors la contremarque de temps est considérée comme valide.
Vérification d'une contremarque de temps (UC) : désigne l'action du Vérificateur de contremarque de temps qui consiste à vérifier que la contremarque est valide.

3. HORADATAGE

Un PSCo fournissant des services d'horodatage est appelé l'AH. L'AH est responsable de la fourniture des services d'horodatage comme décrit dans la présente PH. L'AH est responsable du fonctionnement d'une ou plusieurs unités d'UH qui créent et signent en son nom.
L'autorité d'horodatage chargée d'émettre un horodatage est identifiable.
L'horodatage permet d'attester qu'une donnée électronique existe à une date et une heure donnée.
Les dates et heures sont garanties par une AH qui applique la PH décrite dans ce document.
En pratique, l'Application Utilisatrice qui souhaite disposer d'une contremarque de temps élabore une demande de contremarque de temps qui contient une empreinte numérique de la donnée électronique qu'il souhaite faire horodater. Ensuite, l'Application Utilisatrice transmet la demande de contremarque de temps à l'UH. L'UH appose une signature électronique, par l'intermédiaire d'une UH synchronisée par rapport au temps UTC, sur l'empreinte qui lui a été fournie et retourne cette empreinte signée à l'Application Utilisatrice.
La signature générée par l'UH lie de manière sûre l'empreinte numérique, et non la donnée électronique elle-même, à la date et l'heure de génération de la contremarque de temps avec une précision de 1 seconde par rapport au temps UTC.

Une UH est matérialisé par un Certificat d'UH émis par DocuSign France dont l'unicité est garantie par le CN contenue dans le Certificat d'UH.
Cette signature est vérifiable pendant une période qui débute dès la génération de la contremarque de temps et dont la durée est fixée par l'AH dans les présentes PH.
L'AH tient à disposition des Vérificateurs de contremarques de temps, les informations nécessaires à la vérification de la validité des contremarques de temps, parmi celles-ci les informations relatives aux états de validité des certificats d'horodatage (chaîne de certification, LCR, etc).
Les demandeurs de contremarques de temps qui établissent des demandes de contremarques de temps sont authentifiés par l'AH.
Chaque UH signe les contremarques de temps pour le compte de l'AH à l'aide d'une clé privée dont la clé publique correspondante a été certifiée au préalable par l'autorité de certification d'horodatage dénommé ACH. Les UH disposent donc de certificats d'UH qui permettent de les identifier.

4. DESCRIPTION DU SERVICE

DocuSign France utilise le Service d'horodatage qualifié uniquement pour :

- La création de signature ou cachés, au format par exemple PADES-B-LT, sur des documents transmis par les Clients de Docusign en utilisant la plateforme de Docusign.
- Ses besoins internes pour garantir l'intégrité, la date et l'heure et l'origine de données.

L'ACH utilisée est certifiée ETSI 319 411-1 NCP+ et ne sert que pour émettre des Certificat d'UH pour les UHs conformes à la présente PH. L'ACH utilisée est l'AC « Docusign Qualified TimeStamp CA G1 » et les Certificats d'UH possèdent l'OID : 1.3.6.1.4.1.22234.2.14.3.61 avec une clé publique RSA 3072 et utilisation de la fonction d'empreinte SHA-384.

Le format de contremarque de temps standard défini par le [RFC 3161] et le protocole définit dans le [RFC3161] est utilisé pour utiliser les services des UH. Les demandeur de Contremarques de temps ne peuvent le faire qu'en interagissant avec le protocole TLS serveur seulement avec l'UH.
Seul les fonctions d'empreintes suivantes SHA-256, SHA-383 et SHA-512 sont autorisées pour calculer l'empreinte d'une donnée à horodater.
Les Contremarques de temps sont produites en utilisant une empreinte SHA-383.
Le service d'horodatage est normalement disponible suivant un taux de disponibilité de 99,9 % pendant 24 heures par jour par jour et 7 jours par semaine. Le contrat avec le Client donne les engagements de disponibilité précis sur lesquels le PSCo s'engage.
Toutes les contremarques de temps contiennent l'empreinte du Certificat d'UH, le numéro de série du Certificat d'UH et le DN complet de l'ACH qui a émis le Certificat d'UH.

La PH référencée ci-dessous couvre le service qualifié d'horodatage qui est identifié par l'OID de PH suivant :

- 1.3.6.1.4.1.22234.2.6.5.9.

L'OID est inclut dans les Contremarque de temps.

Cette PH est conforme avec les règles identifiées par « ETSI time-stamping identifier, 0.4.0.2023.1.1 (EN 319 421) » dont cet OID est repris dans le TSA Disclosure Statement.

4.1. Synchronisation de l'horloge d'UH avec le temps UTC

DocuSign France s'engage à ce que la Contremarque de temps générée soit synchronisée avec le temps (*UTC*) avec une précision de 1 seconde.
La synchronisation de l'horloge d'UH est maintenue de telle sorte que celle-ci ne puisse normalement dériver en-dehors de l'exactitude déclarée.

De même, DocuSign France s'assure que la synchronisation de l'horloge des UH est maintenue lorsqu'un saut de seconde est programmé.
Toutefois, dans le cas où une désynchronisation avec le temps UTC serait constatée, DocuSign France procèdera immédiatement à une suspension du Service afin de rétablir la synchronisation avec la précision souhaitée.

En tout état de cause, en cas de perte de calibrage qui pourrait affecter les Contremarques de temps, DocuSign France informera l'Application Utilisatrice et les Vérificateurs de contremarque de temps et mettra en place un plan de secours.

4.2. Validité et période opérationnelle des Contremarques de temps

Toute Contremarque de temps est considérée valide à compter de son émission par l'AH, étant précisé que sa validité liée à la validité du Certificat d'UH qui a signé cette Contremarque de temps.
Aussi les Contremarques de temps ont une durée de validité de 5 ans car le Certificat d'UH dure 6 ans et la Clé privée de l'UH n'est utilisable qu'un an.

4.3. Validation des Contremarques de temps

Pendant la durée de validité des certificats d'UH, l'AH s'assure que les UCs peuvent avoir accès à l'information utilisable pour vérifier la signature numérique des Contremarques de temps.
En particulier :

- Les certificats des ACH sont disponibles sur le site internet de DocuSign France : https://www.docusign.com/fr-fr/mentiones-legales/politiques-de-certifications ;
- Les certificats des UH sont joints à la Contremarque de temps si l'Application Utilisatrice le demande dans la demande de contremarque de temps ;
- Les certificats du chemin de certification qui sont utilisables pour valider un certificat d'UH sont publiés par l'ACH ;
- Le Certificat d'AC qui émet les Certificat d'UH est contenu dans la liste de confiance eIDAS de l'ANSSI ;
- Les informations de révocations des certificats d'UH et d'ACH sont publiées par l'AC.
- Vérifier que l'horodatage a été correctement signé et que la clé privée utilisée pour le signer n'a pas été compromise jusqu'au moment de la vérification ;
- Tenir compte des limitations d'utilisation de l'horodatage indiquées par la PH ; et
- Tenir compte de l'usage de la cryptographie et de sa durée de vie en consultant par exemple les standards en la matière publiés par l'ENISA afin de s'assurer que la Contremarque de temps est toujours utilisable et robuste.

Pendant la durée de validité des certificats d'UH et suite à la fin de validité des certificats d'UH, le Vérificateur vérifie régulièrement que les algorithmes et les paramètres cryptographiques qui ont été utilisés le jour de l'émission de la contremarque de temps sont toujours valides.
Suite à la fin de la validité de tous les certificats utilisés pour une Contremarque de temps, le PSCo continuera à publier les informations décrites ci-dessus afin que l'UC puisse toujours continuer à valider les Contremarque de temps.

4.4. Conservation des fichiers d'audit de l'AH

L'AH conserve les fichiers d'audits de son Service d'horodatage pendant une durée de 7 ans minimum après expiration des certificats d'UH.

L'Application Utilisatrice s'engage à informer immédiatement DocuSign France et par écrit de toute utilisation détournée ou non autorisée du Service, et de toute atteinte à la sécurité pouvant en résulter.

5. RESPONSABILITE

Si l'une des parties manque à ses obligations contractuelles, l'autre partie sera en droit d'obtenir dans les conditions définies ci-après, la réparation du préjudice dont elle apportera la preuve.

5.1. Responsabilité du Vérificateur de Contremarque de temps

L'UC est tenu de vérifier les Contremarques de temps comme indiqué dans les présentes TSA DS et la PH et uniquement à l'aide des informations validées par DocuSign France et l'ACH et l'ANSSI. L'UC peux utiliser les Contremarques de temps avec le logiciel Adobe Reader. DocuSign France ne s'engage pas sur un autre outil de vérification sauf si celui-ci a été approuvé par DocuSign France et dûment communiqué auprès du Vérificateur.

5.2. Responsabilité de DocuSign France

Les responsabilités de DocuSign France sont établies dans le contrat entre le Client et Docusign.
L'AH ne saurait être tenue responsable en cas de validation et d'utilisation d'une Contremarque de temps avec une cryptographie qui ne serait plus considéré comme valide par l'ANSSI ou l'ENISA. L'AH émet des Contremarque de temps qui sont valides, au moment de leur émission, d'un point de vue cryptographique par rapport au référentiel de l'ANSSI. L'AH suit les recommandations de l'ANSSI afin de n'émettre que des Contremarque de temps dont la validation des certificats et des signatures repose sur des algorithmes et paramètres cryptographiques qui sont conformes au référentiel de l'ANSSI.

Cependant les attaques évoluent et les référentiels évoluent en conséquence.

Il est également convenu que DocuSign France ne peut être tenue responsable d'éventuels dysfonctionnements sur le poste de l'UC ni dans les logiciels que l'UC utilise pour valider les Contremarques de temps.

De même, la responsabilité de DocuSign France ne s'étend pas au bon fonctionnement (*panne, erreur, incompatibilité, etc*) des logiciels d'Adobe Reader et de son environnement informatique utilisé par le Vérificateur.

6. INDEMNITE

Le sujet des indemnités est traité dans le contrat entre le Client et Docusign.

7. PROTECTION DES DONNEES A CARACTERE PERSONNEL

DocuSign France a mis en place et respecte des procédures de protection des données personnelles pour garantir la sécurité des informations caractérisées comme personnelles dans le cadre du Service d'horodatage. Le Service en tant que tel ne gère pas de données personnelles de l'Application Utilisatrice car il ne reçoit que l'empreinte des données à horodater transmise par l'Application Utilisatrice.
A cet égard, l'AH respecte notamment la législation et la réglementation en vigueur sur le territoire français, en particulier le GDPR.

Toute demande concernant les données personnelles sont à adresser à DocuSign en utilisant l'email privacy@docusign.com.

8. JURIDICTION ET LOI APPLICABLE

Les présentes sont soumises au droit français.
Le contrat entre le Client et Docusign contient les modalités de résolution des litiges.

Signed by:
Maxime Hambersin
9A097E002C47437...