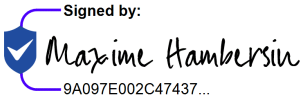
Server Signing Application Service (SSAS) Policy and Practice Statement

Politique de Signature Remote QSCD



POLITIQUE DE SIGNATURE REMOTE QSCD

Version du document :	V 1.1	**Nombre total de pages :**	35
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
12/12/2025	1.0	EM	Passage en v 1.0	
20/05/2026	1.1	EM	Ajout d'un OID pour distinguer les plateformes SSA entre Protect&Sign et CSE software.	

SOMMAIRE

AVERTISSEMENT

Le présent document est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables.

Ces droits sont la propriété exclusive de DocuSign France.

La reproduction, la représentation (hormis la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement de manière expresse par DOCUSIGN FRANCE ou ses ayants-droits, sont strictement interdites.

En outre, l'article L.122-5 du Code de la Propriété Intellectuelle n'autorise d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration.

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

1 INTRODUCTION

1.1 Présentation générale de la Politique de Signature Remote QSCD

Ce document constitue la Politique de Signature (noté PS) associée au Server Signing Application Service (SSAS) pour le service de Remote QSCD, conformément à l'article 29 de eIDAS, que la société DocuSign FRANCE fournit à ses Clients soit en direct soit en passant par la plateforme de DocuSign (noté IAM). La signature ainsi produite est de niveau qualifié conformément à la définition de la signature qualifiée contenue dans l'article 3 du règlement eIDAS.

2 REFERENCES NORMATIVES

La présente PS est élaborée conformément :

- [319 401] : ETSI EN 319 401, "Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers."
- [319 411-1] : ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates, Part 1 : General requirements.
- [319 411-2] : ETSI EN 319 411-2, Electronic Signatures and Infrastructures (ESI) ; Policy and security requirements for Trust Service Providers issuing certificates, Part 2 : Requirements for trust service providers issuing EU qualified certificates.
- [119 431] : ETSI TS 119 431, "Electronic Signatures and Trust Infrastructures (ESI), Policy and security requirements for trust service providers", Part 1 : TSP services operating a remote QSCD / SCDev"
- [419 241-1] : CEN 419 241-1, « Trustworthy Systems Supporting Server Signing - Part 1 : general System Security Requirements »
- [119 312] : ETSI TS 119 312 : Electronic Signatures and Infrastructures (ESI) ; Cryptographic Suites ;
- [CRYPTO] : « European Cybersecurity Certification Group, Sub-group on Cryptography : "Agreed Cryptographic Mechanisms" published by the European Union Agency for Cybersecurity ('ENISA') » ;
- [P&S QSCD] : « Qualified Signature Creation Device (QSCD) Protect & Sign, version 5.14, update 2 » notifié dans la liste de l'EU par l'Autriche (https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd) ;
- [DS QCSD] : « DocuSign QSCD for remote signing version 1.2.0.7» notifié dans la liste de l'EU par les Pays-Bas (https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd) ;
- [Article 29 acte d'implémentation] : « Brussels, 29.7.2025 C(2025) 5044 final, laying down rules for the application of Regulation (EU) No 910/2014 of the European, Parliament and of the Council as regards the management of remote qualified electronic signature creation devices and of remote qualified electronic seal creation devices as qualified trust services » ;
- [Article 24(5)] : "RÈGLEMENT D'EXÉCUTION(UE) 2025/2530 DE LA COMMISSION du 16 décembre 2025 portant modalités d'application du règlement (UE) no910/2014 du Parlement européen et du Conseil en ce qui concerne les exigences applicables aux prestataires de services de confiance qualifiés fournissant des services de confiance qualifiés".

3 DEFINITIONS ET ABREVIATIONS

3.1 Définitions

Application de signature serveur (SSA) : système logiciel qui permet de mettre en œuvre le SAP et de créer le SAD, de gérer et vérifier les Facteurs d'activation, d'authentifier le Signataire, de valider les références des SPIE, d'interagir avec ; le SIC et le remote QSCD pour la mise en œuvre de signature électronique et d'interagir avec l'AC, le service de statut de certificat (CRL et/ou OCSP), l'AE et le service d'horodatage afin de créer une Clé de signature à usage unique et son Certificat associé et de créer une capsule de signature horodatée.

Authentification : un processus électronique qui permet de confirmer l'identification électronique d'un Signataire.

Certificat(s) : désigne(nt) un fichier électronique délivré par l'Autorité de Certification attestant du lien entre une Identité de Signataire et la Clé publique de la personne titulaire du Certificat. Les Certificats utilisés dans le cadre de la présente PS sont des Certificats qualifiés [319 411-2] QCP-N QSCD.

Clé privée : désigne une clé mathématique associée à la Clé publique, qui est secrète et destinée à signer les données électroniques (aussi appelée dans eIDAS Données de Création de Signature Electronique). Les Clés privées ne sont que des Clés de signature à usage unique.

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.

Clé de signature à usage unique : clé publique et clé privée de signature liée, certifiée, utilisée et supprimée sur la base d'une activation unique associée à une Transaction unique.

Composant d'interaction du signataire (SIC) : Composant logiciel et/ou matériel utilisé par le Signataire pour prendre en charge SAP. L'utilisation de ce composant est essentielle au processus SAP et à la création d'une Signature par le remote QSCD. Le SIC est un logiciel et/ou un matériel exécuté dans l'environnement du Signataire et sous son contrôle exclusif. Le SIC participe systématiquement au processus SAP afin d'authentifier le signataire ou de générer le SAD :

- Le SIC peut générer directement le SAD, ou
- Le SIC peut être utilisé pour authentifier le Signataire, et l'assertion permettant d'identifier ce dernier sera utilisée lors de la génération du SAD.

Ce composant peut être, par exemple (ou une combinaison de ceux-ci) :

- Une application exécutée par un navigateur (par exemple, une requête HTTP POST sur TLS),
- Une application exécutée par un appareil mobile (par exemple, un smartphone ou une tablette),
- Un élément sécurisé d'un téléphone portable (par exemple, une carte SIM recevant des SMS),
- Un dispositif cryptographique appartenant au signataire (par exemple, un jeton eID, un jeton électronique ou un jeton FIDO),
- L'Application Client ou le portail IAM de DS ou le SSA peuvent permettre de mettre en œuvre tout ou partie du SIC sachant qu'il permet la mise en œuvre de fonction sous le contrôle du Signataire.

Le SIC assure le lien entre le signataire et l'opération de signature au sein du processus SAP.

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.

Dispositif de création de signature électronique : un dispositif logiciel ou matériel configuré servant à créer une signature électronique.

Dispositif de création de signature électronique qualifié (QSCD) : un dispositif de création de signature électronique qui satisfait aux exigences énoncées à l'annexe II eIDAS.

Dispositif de création de signature électronique qualifié à distance (remote QSCD) : un dispositif de création de signature électronique qualifié qui est géré par un prestataire de services de confiance qualifié conformément à l'article 29 bis de eIDAS, pour le compte d'un Signataire.

Document : désigne un document électronique créé par le Client sous un format PDF et complété des informations relatives au Signataire.

Données d'Activation de Signature (SAD) : Ensemble de données collectées par le SAP, comme les Facteurs d'activation, et utilisées pour créer le SAD sous le contrôle exclusif du Signataire, pour contrôler avec un haut degré de confiance, une opération de signature, dans le cadre d'une Transaction, effectuée par un remote QSCD pour le compte du signataire. Le SAD est créé par le SSA suivant les spécifications des cibles de sécurité des remote QSCD. Les SAD contient entre autres l'Identifiant de Transaction et l'identifiant de l'opération d'authentification de l'Identité du Signataire. Ces deux identifiant peuvent être les mêmes selon le type de Transaction et la plateforme utilisée par l'Application Client (IAM ou sans IAM).

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 ».

Facteur d'activation : désigne les données ou actions associées à un Signataire lui permettant de créer le SAD afin de mettre en œuvre sa Clé privée, via le SAD, au travers du SAP (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, …).

Fichier de preuve : désigne l'historique des opérations réalisées ainsi que les informations sur l'Identité du Signataire dans le cadre d'une Transaction permettant d'assurer la pérennité de la validité du Document signé. Il peut être matérialisé sous forme de fichier électronique scellé et horodaté par le PSCo.

Fournisseur de service d'application de signature serveur (SSASP) : PSCo exploitant un SSAS.

Identifiant de Transaction : désigne un ou plusieurs numéro(s) de référence unique (complété par le cas échéant un identifiant de l'Application Client ou de la plateforme IAM) permettant de lier une Transaction, un Document signé, un Fichier de preuve, un Certificat et un SAD.

Identité : nom(s) et prénom(s) officiel du Signataire tels qu'inscrits sur un titre d'identité officiel (passeport, carte nationale d'identité ou titre de séjour) et collectée et vérifiée par une AE ou un IDP en relation contractuelle avec l'AC.

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.

Module d'activation de signature (SAM) : Logiciel configuré et mis en œuvre dans le QSCD vérifiant et utilisant le SAD afin, avec un haut niveau de confiance, que les Clés privées de signature soient utilisées sous le contrôle exclusif du Signataire.

Service de persistance d'Identité électronique (SPIE) : service mis en œuvre par Docusign composé d'éléments matériels et logiciel qui gère une Identité persistée, et les informations associées à la vérification de l'Identité, suite à une identification du Signataire et est utilisé pour l'Authentification auprès du SSAS via le SAP.

Référence SPIE : données utilisées dans le SSAS comme référence afin de valider les éléments fournis par le SPIE pour authentifier le Signataire.

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 Signataires et des Vérificateurs de Certificat.

Protocole de consentement (SAP) : désigne l'ensemble des règles opérationnelles mises en œuvre par le l'Application Client et/ou SSAS et le QSCD pour :

- le recueil du consentement d'un Signataire à savoir ; la définition des actions à réaliser par le Signataire sur le Terminal d'Affichage pour (i) activer la signature du ou des Document(s) proposé(s) par l'Application Client, (ii) visualiser et valider les informations utilisées pour la création de l'Identité et les informations pour l'activation de la signature (numéro de téléphone portable par exemple) et (iv) les modalités de visualisation du Document ou de sa référence présenté et du message d'acceptation (ou de refus) associé (case à cocher par exemple, bouton accepter ou refuser, …) ; et
- La gestion du SAD, des Facteurs d'activation, la Référence SPIE et l'interaction avec le QSCD.

Le SAP est un protocole permettant la communication entre le signataire (via le SIC), le QSCD et le Système afin de générer la SAD. La conception du SAP inclut au minimum les vérifications suivantes :

- Authentification du Signataire lors de l'utilisation de la Clé privée ;
- Authenticité de la demande de signature venant de l'Application Client ou IAM avec le SAD ;
- Validité et utilisabilité de la Clé privée ;
- Transfert sécurisé de tous les éléments du SAD.

Service d'application de signature serveur (SSAS) : service de confiance composé d'au moins un SSA et d'au moins un remote QSCD permettant de créer une signature électronique pour le compte d'un Signataire.

Signataire : une personne physique qui crée une signature électronique sur ou des Document(s) via le SSAS avec une Identité ;

Système : c'est le TW4S au sens de [419 241-1] qui est composé de QSCD et de SSA et donc de logiciels métiers, système d'exploitation, composants réseaux, … et qui est hébergé chez le PSCo afin de mettre en œuvre le SSAS.

Terminal d'affichage : désigne le terminal (ordinateur personnel, tablette, …) sur lequel le Signataire effectue sa Transaction, et sur lequel est affiché le Document à signer et le SAP. Il permet de mettre en œuvre le SIC.

Transaction : désigne l'échange électronique entre le Client et chaque Signataire réalisé au moyen d'un Terminal d'affichage, d'un SIC et du SSAS et au cours duquel le Client propose pour signature, suivant un SAP, un ou plusieurs Document(s) à un Signataire identifié et authentifié par l'AE ou un IDP, afin que le Signataire 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.

3.2 Abréviations

- AC : Autorité de Certification.
- AE : Autorité d'Enregistrement.
- CC : Critères Communs.
- EAL : Evaluation Assurance Level, norme ISO 15408 (*Critères Communs*) pour la certification des produits de sécurité.
- HTTP : HyperText Transport Protocol.
- ISO : International Organization for Standardization.
- LCR : liste de certificats révoqués.
- OCSP : Online Certificate Status Protocol.
- OID : Object Identifier.
- PC : Politique de Certification.

- PMA : Policy Management Authority.
- PS : Politique de Signature.
- PSGP : Politique de Signature et Gestion de Preuves.
- remote QSCD : Dispositif de création de signature électronique qualifié à distance.
- RSA : Rivest, Shamir, Adleman.
- SAD : Données d'Activation de Signature.
- SAM : Module d'activation de signature.
- SAP : Protocole de consentement.
- SHA : Secure Hash Algorithm (*norme fédérale américaine*).
- SIC : Composant d'interaction du signataire.
- SP : Service de Publication.
- SPIE : Service de persistance d'Identité électronique.
- SSA : Application de signature serveur.
- SSAS : Service d'application de signature serveur.
- SSASP : Fournisseur de service d'application de signature serveur.
- URL : Uniform Resource Locator.

4 GENERAL CONCEPTS

4.1 Documentation applicable

La présente PS suit exactement le sommaire du document [119 431] et est élaboré principalement à partir des exigences définies dans [119 432], [419 241-1] et [319 401].

4.2 Chapitre supprimé

N/A.

4.3 Gestion de la Politique de Signature

4.3.1 SSAS Practice Statement

La présente PS contient également l'information publique du « SSAS Practice Statement », mais le document s'appelle PS. Les informations confidentielles de la practice statement ne sont pas contenues dans la PS. Seuls les auditeurs autorisés par le PSCo peuvent avoir accès aux informations confidentielles de la practice statement.

4.3.2 Politique SSAS

La présente PS couvre les services qualifiés qui sont identifiés par les OIDs de Politique de Certification (PC) suivants :

- AC « DocuSign Premium Cloud Signing CA - G2 » avec l'OID 1.3.6.1.4.1.22234.2.14.3.45 (certifié [319 411-2] QCP n-qscd) avec l'OID de PS 1.3.6.1.4.1.22234.2.4.6.1.20.
- AC « Docusign Qualified CA G1 » avec l'OID 1.3.6.1.4.1.22234.2.14.3.60 (certifié [319 411-2] QCP n-qscd) avec l'OID de PS 1.3.6.1.4.1.22234.2.4.6.1.21.

La présente PS décrit les règles que DocuSign France, ses Clients et les Signataires respectent pour signer électroniquement des Documents et constituer et conserver des Fichiers de preuves relatifs aux Transactions électroniques réalisées entre eux, afin d'être en mesure de démontrer ultérieurement l'existence et l'intégrité de la (ou des) signature(s) des Documents.

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

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

4.3.3 CGU du SSAS

Les CGUs du SSAS sont combinées avec les CGUs de chaque service de gestion de Certificats de signature à distance définies et publiées par l'AC. L'AC et le SSAS sont mis en œuvre par le même PSCo qui est DocuSign France. De plus, comme les Certificats sont associées à des Clés à usage uniques tous deux générés dans le cadre d'une même et unique Transaction, alors le Signataire ne visualise et n'accepte qu'une seule CGU qui sont celles du PSCo.

Il est à noter que dans le cadre de la transition eIDAS v1 vers eIDAS v2 seul l'OID de la PC est indiqué dans les CGUs. Une fois le service qualifié par l'ANSSI, les CGUs seront mises à jour afin de rajouter l'OID de la PS en plus de l'OID de la PC.

4.4 SSAS Composants du service

Pour délivrer les signatures électroniques via le SSAS avec un remote QSCD, le PSCo s'appuie sur les services suivants :

- Service de génération de Clés privée : génère des Clés privées dans la ressource cryptographique du QSCD. La preuve de possession des Clés privées générée est transmise au service d'enregistrement de l'AC (Autorité de Certification) qui délivre le Certificat associé.
- Service d'association de Certificats : associe le certificat généré par le service de génération de certificats de l'AC aux Clés privées correspondantes.
- Service d'association d'Identité : ce service associe une Référence de SPIE ou une Identité, via le SAD et le SAP, aux Clés privées correspondantes afin d'en assurer le contrôle exclusif. Les deux possibilités s'appliquent uniquement dans le cas d'une Clé privée, est assure que l'Identité figurant dans le Certificat est identique à celle du Signataire. Ce service est utilisé pour répondre à l'exigence REG-6.3.1-01 de la norme [319 411-1] pour l'AC émettant les Certificats.
- Service d'activation de signature : vérifie les Facteurs d'activation et le SAD et active la clé de signature correspondante afin de créer une signature.
- Service de suppression des Clés privées : détruit les Clés privées de manière à s'assurer qu'elles ne puissent plus être utilisées.
- SPIE (optionnel) : prépare et fournit ou met à disposition des signataires un compte dans le SPIE.

Ces services sont mis en œuvre grâce à un Système au sens de [419 241-1] qui est composé au moins d'une SSA et d'un remote QSCD.

5 DISPOSITIONS GENERALES RELATIVES A LA DECLARATION DE PRATIQUE ET AUX POLITIQUES

5.1 Exigences particulières pour la SSAS Practice statement

Les exigences cryptographiques sont indiquées dans le chapitre 6 pour les Clés privées.

L'Empreinte du Document à signer est calculé en SHA-256.

Le service SSAS est normalement disponible suivant un taux de disponibilité de 99,9 % pendant 24 heures par jour et 7 jours par semaine. Le contrat avec le Client donne les engagements de disponibilité précis sur lesquels le PSCo s'engage.

5.2 OID du SSAS

La PS est identifiée par l'OID : 1.3.6.1.4.1.22234.2.4.6.1.20 pour la mise en œuvre avec le SSA : Protect & Sign et le [P&S QSCD].

La PS est identifiée par l'OID : 1.3.6.1.4.1.22234.2.4.6.1.21 pour la mise en œuvre avec le SSA : CSE software. Pour cet OID le SSA est uniquement connecté au IAM et le [DS QSCD].

Les OID sont aussi contenus dans les Fichiers de preuve afin de référencer le présent document.

5.3 Entités impliquées

5.3.1 SSASP (PSCo) DocuSign France

Le PSCo est DocuSign France qui met en œuvre le SSAS.

Le PSCo a en charge le choix et l'audit des AC, AE et IPD à utiliser dans le cadre du SSAS.

Le PSCo héberge le SSAS au même endroit que l'AC. La PC de l'AC décrit l'opérateur de service de confiance utilisé.

Le PSCo utilise le même service de publication (SP) que celui de l'AC et la PC décrit ce service de publication.

Le PSCo est géré par la même Policy Management Authority (PMA) telle que décrite dans la PC de l'AC.

DocuSign France met en œuvre la partie du SAP pour interagir avec le Signataire sauf si le Client le met en œuvre comme détaillé dans la PS.

5.3.2 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.

5.3.3 Client

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

- L'Application Client qui génère le Document à signer et qui appelle le SSA directement ou via la plateforme de IAM pour mettre en œuvre une Transaction ;
- L'Identification et de l'authentification des Signataires conformément à sa politique d'enregistrement établie et mise en œuvre lorsque le Client agit sa qualité d'Autorité d'Enregistrement pour l'AC du PSCo ;
- La définition d'un SAP (seulement pour les Services sans IAM et uniquement quand le Client est AE) ;
- Générer le Document qui sera présenté au Signataire pour signature ;
- Dans le cas où le Client utilise le SSAS en mode délégation totale pour de la signature de personne physique et sans utiliser le Fichier de preuve PSM, définir et faire approuver par DocuSign France la partie du SAP et le Fichier de preuve mise en œuvre par le Client ;

- L'élaboration de Conditions Générales d'Utilisation (ou de vente ou de service) à destination des Signataires et qui doivent être référencées dans le Document à signer et/ou le SAP (uniquement pour un usage du SSAS sans IAM).

5.3.4 Autorité d'Enregistrement (AE)

La définition exacte de l'AE est donnée dans les PC de l'AC qui émet le Certificat en fonction de l'OID.

C'est une entité dite « external party » au sens du [119 431] lorsque c'est le Client qui est AE mais pas lorsque c'est le PSCo lui-même qui est AE.

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

5.3.5 IDP

C'est une entité dite « external party » au sens du [119 431]. Dans le cadre du SSAS, seul des IDP au sens prestataire de vérification d'identité à distance sont utilisés et comme définis dans la PC (chapitre PVID).

5.3.6 DocuSign Inc.

L'entité qui met en œuvre la plate-forme IAM.

Docusign permet de mettre en œuvre un SPIE dans le cadre de la pérennisation d'une Identité vérifiée par un IDP certifié (se reporter au § 6.2).

C'est une entité dite « external party » au sens du [119 431].

5.3.7 Vérificateur

Le vérificateur est une personne physique qui a le rôle d'Utilisateur de Certificat au sens de la PC de l'AC et qui réalise la validation d'un Document signé et peux utiliser le cas échéant un Fichier de preuve. Selon le résultat de l'opération de validation, le Vérificateur pourra décider de l'utilisation ou non du Document signé ou de Fichier de preuve.

Le Vérificateur procède à la validation de la signature électronique selon l'ensemble des modalités prévues dans la politique de la [PSGP] pour le Fichier de preuve.

6 REGLES ET MESURES DE SECURITE DU SSASP

6.1 Publication

Le PSCo publie sur le SP de l'AC la présente PS. Les CGUs mentionnées dans la présente PS sont en fait les CGUs de l'AC et sont donc publiées sur le SP de l'AC. Le SP est public et disponible 24 heures par jour et 7 jours par semaine.

En cas de panne du SP, d'interruption de service ou d'autres facteurs indépendants de la volonté du PSCo, ce dernier s'engage à faire tout son possible pour que le service du SP ne soit pas indisponible pendant une durée supérieure à 3 semaines.

6.2 Initialisation de la Clé de signature du Signataire

6.2.1 Génération de la clé

Le SSA associé au [DS QSCD] et au [P&S QSCD] déclenche la génération et l'utilisation de la Clé privée dans la ressource cryptographique matérielle [DS QSCD] suite à la mise en œuvre du SAP sous le contrôle du

Signataire dans le cadre d'une Transaction. Les Clés privées peuvent être générées à l'avance dans le [DS QSCD] une fois qu'il est redémarré en production sans être affectées à un Signataire. Quand le [DS QSCD] est configuré de la sorte, alors le [DS QSCD] les conserve tout le temps à l'intérieure du [DS QSCD] et elles ne peuvent être utilisé que de la même manière que lorsque les Clés privées sont générées en temps réel via le SSA et le SAP et uniquement dans le cadre d'une Transaction. Cette possibilité fait partie des fonctions certifiées critère commun du [DS QSCD].

Le [DS QSCD] est certifié critère commun EAL 4+ augmenté AVA_VAN.5. Cette ressource cryptographique est le [DS QSCD] qui est certifié critère commun conformément au profil de protection [419 221-5] et [419 241-2]. Le remote QSCD et le [DS QSCD] est mis en œuvre, configuré et utilisé conformément à la cible de sécurité et au rapport de certification associés.

La taille des Clés de signature est RSA 3072 bits conformément à [119 312] et [CRYPTO].

Les Clés privées sont générées dans et par le [DS QSCD] et sont donc chiffrées par le [DS QSCD] qui est le seul à pouvoir les utiliser. Seul le SSA est autorisé à récupérer et utiliser la Clé privée en interaction avec le [DS QSCD] et [P&S QSCD].

La cérémonie de personnalisation d'un [DS QSCD] se déroule sous le contrôle d'au moins deux personnes dans des rôles de confiance du PSCo (les mêmes que ceux de l'AC). Elle se déroule dans les locaux du PSCo. Les rôles de confiance attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. Les rôles impliqués dans les cérémonies de clés sont précisés dans les procédures opérationnelles.

À la suite de leur génération, les parts de secrets (*données d'activation de la ressource cryptographique au minimum au nombre de 2*) sont remises à des porteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par le PSCo. Quelle qu'en soit la forme (*papier, support magnétique ou confiné dans une carte à puce ou une clé USB*), un même porteur ne peut détenir trop de parts de secrets d'un même [DS QSCD] qui ferait qu'il ait le contrôle seul du [DS QSCD] à un moment donné (principe du schéma à seuil MofN). Une fois ainsi initialisé les [DS QSCD] sont installés en production dans l'environnement du PSCo sous double contrôle de telle sorte qu'ils ne peuvent ensuite n'être utilisé techniquement que part le SSA et [P&S QSCD] en production.

Le SSAS ne met en œuvre que des Clé privée de type Clé de signature à usage unique qui sont liées à une unique Transaction. Ces Clés privées sont forcément liées à un certificat QCP-N QSCD associé à un Signataire qui a été identifiée et authentifié par une AE ou un IDP utilisé par le PSCo. La génération de la Clé privée et du Certificat associé sont effectués dans le cadre de la même et unique Transaction pour un Signataire dûment identifié et authentifié via le SAP et les Facteurs d'activation. Le SSAS se base sur une assertion signée par l'AE ou l'IDP afin de récupérer les informations du Signataire à lier au Certificat et à la Clé de signature à usage unique dans le cadre d'une Transaction initiée par un Client.

6.2.2 Association entre un SPIE ou une Identité et un Signataire

Le SSAS permet soit ; de lier une Identité de manière temporaire dans le cadre d'une Transaction à une Clé privée et un Certificat, soit de lier une Identité de manière pérenne (pendant 3 ans maximum) à un SPIE qui permet ensuite d'obtenir autant de Certificat et de Clés privée que de Transaction impliquant le Signataire.

Les CGUs sont présentées au Signataire soit par l'AE soit par le SSA dans le cadre de la Transaction et toujours pendant la mise en œuvre du SAP.

6.2.2.1 Identité sans SPIE

Par défaut, le SSAS, suite à l'identification et l'authentification du Signataire par une AE ou un IDP dans le cadre d'une Transaction, authentifie l'assertion signée de l'AE ou de l'IDP, entre en session avec le Signataire, met en œuvre le SAP, authentifie le Signataire en utilisant les Facteurs d'activation et génère le SAD afin de déclencher la génération de la Clé privée, le Certificat associé et la signature PADES associée à la Transaction.

6.2.2.2 Identité avec SPIE

Si le Signataire a fait le choix d'avoir un SPIE fournit par DS (se reporter au § 6.2.4), alors il peut utiliser le SPIE pour prouver son Identité auprès du SSAS en activant le SPIE grâce à une bi-clé technique cryptographique stockée dans son téléphone portable. Cette activation ne peut se produire uniquement dans le cadre d'une Transaction. En ce cas, le SSAS récupère l'Identité transmise via le SPIE dans le cadre de la Transaction, vérifie son authenticité, entre en session avec le Signataire, génère le code OTP par SMS et le transmet au Signataire, met en œuvre le SAP et génère le SAD afin de déclencher la génération de la Clé privée, le Certificat associé et la signature PADES-B-LT associée à la Transaction.

La référence du SPIE correspond à l'identifiant de la vérification d'identité générée par l'IDP et la clé publique à utiliser pour vérifier l'Identité. Le SSASP ne génère pas de référence du SPIE. Le SSASP récupère l'Identité à inclure dans le Certificat du Signataire dans l'assertion fournie par l'IDP lors de la Transaction et la mise en œuvre du SAP par conséquent le Certificat contient l'Identité associé au Signataire.

6.2.2.3 Délégation de l'authentification

Le SSASP peut déléguer tout ou partie de l'authentification du Signataire et de la mise en œuvre du SAP pour la collecte des Facteurs d'activation.

Lorsque le PSCo délègue l'authentification, le signataire est authentifié lors d'un face à face par une AE certifiée [319 411-2] QCP-N QSCD ou un IDP certifié [PVID] ou équivalent par l'ANSSI. L'AE et l'IDP doivent respecter les exigences de [119 461] pour le niveau de sécurité « extended Level of Identity Proofing (LoIP) ».

L'AE et l'IDP doivent récupérer les informations suivantes du titre d'identité du Signataire ; numéro de série, type de titre, pays émetteur, date de validité et date de naissance du Signataire et les transmettre protégées en intégrité, confidentialité et authentification au SSA. Les CGUs utilisées par l'AE sont validées par le PSCo et sont forcément montrées au Signataire lors du SAP. L'AE et l'IDP à date n'utilisent que des titres d'identité acceptés pour l'émission d'un Certificat.

Lorsque le PSCo délègue en plus de l'authentification la mise en œuvre du SAP pour la collecte des Facteurs d'activation alors, l'AE ou l'IDP doivent utiliser une ressource cryptographique EAL 4+ ou FIPS 140–2 level 3 pour signer l'assertion transmise au SSA. Cette assertion permet au SSA d'authentifier le l'AE ou l'IDP et de générer le SAD pour le compte du Signataire.

Le PSCo s'assure régulièrement que l'AE et l'IDP possède toujours les certifications requises indiquées dans ce paragraphe ci-dessus.

6.2.3 Lien entre Certificat, Clé de signature à usage unique et le Signataire

Dans tous les cas, avec ou sans usage de SPIE, le SSA lie la Transaction, le SAD, le Certificat et la Clé privée. Ce lien est dynamique et n'est utilisé que pour la Transaction par conséquent l'intégrité est assuré par le SAD qui est signé. Le lien est créé par le fait que le Signataire est authentifié lors de la Transaction et qu'il transmet ses Facteurs d'activation dans le SAP au SSA lors de cette même Transaction. Le SSA génère ainsi, pour cette seule Transaction, un SAD, au seul profit du Signataire, suite à une authentification réussit dans le SAP du Signataire, une Clé de signature à usage unique et un Certificat associé avec l'Identité.

La Clé privée est protégée comme indiquée au paragraphe 6.2.1 ci-dessus et n'est activable que par le SSA qui a mis en œuvre le SAP comme décrit dans le présent document.

6.2.4 Gestion du SPIE

Le Signataire peut s'il le souhaite utiliser le SPIE immédiatement suite à son Authentification réussi par l'IDP et uniquement au cours d'une Transaction via le service IAM. Lors de la création de son compte dans le SPIE, le service SPIE fait :

- Créer une bi-clé technique sur le téléphone portable du Signataire et enregistrer la clé publique dans le SPIE (DS Wallet) du service SPIE.

- Créer un compte dans la plateforme IAM (email du Signataire et mot de passe).
- Stocke l'assertion signée créée par l'IDP qui contient l'Identité.

Le Signataire peut consulter et supprimer le contenu de son compte dans le SPIE en s'authentifiant auprès du service IDV de DS à tout moment.

Le compte dans le SPIE n'est valable que 3 ans. Au bout de 3 ans le compte dans le SPIE doit être renouvelé lors d'une Transaction et requiert que le Signataire s'authentifie auprès d'un IDP certifié approuvé par le PSCo.

Le Signataire est responsable de la protection de sa bi-clé technique et de son utilisation.

Le SPIE fait l'objet d'un audit PASSI tous les 2 ans sur un périmètre et avec des portés de tests qui sont validés par l'ANSSI.

6.3 Cycle de vie et gestion des Clés de Signature

6.3.1 Activation de signature

Un Transaction commence toujours par un Client qui initie une demande de signature au profit d'un Signataire pour un ou plusieurs Document(s). Le Client utilise une Application Client ou la plateforme IAM afin d'initier la Transaction. L'Application Client et la plateforme IAM sont connectées au SSA de manière sécurisée afin de protéger l'intégrité et la confidentialité des échanges et l'authentification des plateformes. Le Signataire est invité à signer soit à distance soit en présentiel. Le Terminal d'affichage sera alors en session technique avec soit l'Application Client ou soit la plateforme IAM qui à leur tour vont établir une session technique avec l'AE ou l'IDP ou le service SPIE en fonction des scénarii et ensuite avec le SSA.

Avant chaque signature, comme indiqué au paragraphe 6.1.1, le Signataire doit être identifié et authentifié soit par l'AE ou un IDP soit via son compte SPIE et doit nécessairement s'authentifier avec plusieurs Facteurs d'activation, sur le numéro de téléphone portable récupéré par l'AE ou l'IDP, dans le cadre du SAP. L'opération et son résultat d'authentification (identification) seule du Signataire n'est pas suffisante pour activer une signature par le Signataire dans une Transaction. Par conséquent l'activation de la Clé privée est toujours sous le contrôle du Signataire.

L'activation de la Clé privée s'effectue obligatoirement dans le cadre d'une Transaction. Le Signataire est invité à signer un Document et par conséquent à s'authentifier et mettre en œuvre le SAP avec des Facteurs d'activation dans le cadre de cette même Transaction. Le SAP et la Transaction s'effectue toujours au cours d'une session TLS, configuré avec des suites cryptographiques conformes à [119 312] et [CRYPTO] et utilisent toujours des identifiants techniques de session à usage unique et dont la période de validité est bornée dans le temps. Le SAP met en œuvre au moins deux Facteurs d'activation afin d'être assuré que seul le Signataire peut mettre en œuvre la Clé de signature. Le SAP nécessite des actions explicites de la part du Signataire (bouton à cliquer, …). Le SAP établit une session à durée limitée dans le temps qui ne dépasse pas 30 minutes.

Le SSA ne permet pas au Signataire d'avoir accès ; aux assertions signées par l'AE et l'IPD, au système de génération des Facteurs d'activation lorsque ceux-ci sont gérés par le PSCo, à la configuration des [P&S QSCD] et [QSCD], au SAD et manière générale le Signataire ne peut accéder qu'au seul SAP et à son compte dans le SPIE. Le SSA est construite de telle sorte que le Signataire ne puisse activer et utiliser que sa seul Clé privée dans le cadre de la seule Transaction avec laquelle le Signataire est en interaction.

Le ou les Document(s) à signer par un Signataire identifié sont transmis par l'AE ou la plateforme IAM au SSA dans le cadre d'une Transaction et le SSA met en œuvre un SAP en montrant l'identifiant du ou des Document(s) ou le ou les Document(s) à signer dans le SAP. Le SAP n'est mis en œuvre que pour ce ou ces Documents au seul profit du Signataire qui ne peut les signer qu'avec le SAP et les Facteurs d'activation et le SAD associé au Signataire, à la Transaction et au ou ces Documents à signer. La Clé privée n'est donc utilisée que pour le ou les Document(s) issus de la Transaction.

Le SAD résulte d'une interaction sécurisée entre le SAM et le SIC via le SSA et le [P&S QSCD] ou [DS QSCD] et le SAP, afin d'autoriser l'opération de signature dans tous les cas au sein du [DS QSCD]. Le SAD est généré par le SSA suite à la vérification des Facteurs d'activation, dont le code OTP saisi par le Signataire, reçu par le SAP pour une Transaction donnée. Le SSA génère un SAD qui contient les identifiants de Transaction et d'identification du Signataire et la référence au ou aux Document(s) à signer ainsi que la référence à la Clé de Signature associée au Signataire. Le SAD est signé par une bi-clé technique, dont les paramètres sont conformes à [119 312] et [CRYPTO], sous le contrôle du SSA chez le PSCo. Le SAD est transmis au SAM via le SSA pour autoriser l'opération de signature au sein du [DS QSCD] pour une Transaction dédiée et un Signataire identifiée et authentifié en utilisant le SAP.

Les Certificats étant émis en même temps que la Clé privée, ils sont donc considérés par essence même comme valides lors de leur usage. Toutefois, le Signataire tout comme le Client ou l'AE peuvent signaler des attaques ou anomalies à propos du Certificat ou de l'utilisation de la Clé privée et le Certificats peut alors être révoqué (Se reporter au système de révocation de l'AC décrit sans PC).

Le [DS QSCD] et le [P&S QSCD] pour créer la signature utilise l'algorithme d'empreinte SHA-256 conformément à [119 312] et [CRYPTO].

Le SAM est mis en œuvre dans le [DS QSCD].

6.3.2 Destruction des Clés de signature

La Clé privée est toujours détruite immédiatement après l'opération de signature liée à la Transaction et au SAD. Ce n'est pas le Signataire qui est à l'origine de la demande de destruction de la Clé privée mais le processus technique géré par le SSA. Le SSA ne conserve pas les Clés privées et ne les possède que temporairement en mémoire le temps de la Transaction technique et les effaces ensuite et demande au [DS QSCD] d'effacer les Clés privée une fois l'opération de signature terminée.

6.3.3 Sauvegarde et recouvrement de Clé de signature

Les Clés privées ne sont pas sauvegardées ni recouvrables.

6.4 MESURES DE SECURITE NON TECHNIQUES

6.4.1 Général

6.4.1.1 Analyse de risque

Le PSCo réalise une évaluation des risques afin d'identifier, d'analyser et d'évaluer les risques liés au service de confiance SSAS, en tenant compte des aspects commerciaux et techniques.

Le PSCo sélectionne les mesures de traitement des risques appropriées, en tenant compte des résultats de l'évaluation des risques.

Ces mesures de traitement des risques permettent de s'assurer que le niveau de sécurité est proportionné au degré de risque. Le PSCo s'appuie sur la norme ISO 27005 pour l'élaboration de son analyse de risque. Cette analyse est incluse dans l'analyse de risque de gestion des certificats associés car ce sont des Clés de signature à usage unique et les services sont en commun et liés.

Le PSCo détermine les exigences de sécurité et les procédures opérationnelles nécessaires à la mise en œuvre des mesures de traitement des risques choisies, telles que documentées dans le présent document et les procédures opérationnelles pour ce service.

Le Remote QSCD et le SSA, et sa gestion du SAD et du SAP, sont construits suivant une analyse de risque qui prend en compte les menaces suivantes ; deviner en ligne ou hors ligne les identifiants de Transaction, le SAD et le code OTP, dupliquer et rejouer les identifiants de Transaction, le SAD et le code OTP, hameçonnage, écoute clandestine, relecture, détournement de session, attaque de l'homme du milieu, vol d'identifiants, usurpation d'identité et attaques par masquage.

L'analyse des risques est revue chaque année et est validée par la PMA qui en accepte les éventuels risques résiduels identifiés.

6.4.1.2 Politique de signature et PSSI

Le PSCo définit la PS et la PSSI, qui est approuvée par la PMA qui le signe électroniquement, qui décrit l'approche de l'organisation en matière de gestion de la sécurité du service SSAS.

L'entité en charge de l'administration et de la gestion de la PS au sein de la société DOCUSIGN France est la PMA de DocuSign France. La PMA est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PS et de la PSSI.

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 PS.

Toute évolution de la PS et PSSI 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.

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 PS susceptible de produire un effet majeur sur lesdits Clients.

DocuSign FRANCE peut modifier la présente PS sans préavis lorsque ces modifications n'ont aucun impact sur eux. Toutefois il informera le client de la nature de la modification.

Dans les cas de modification soumise à préavis, DocuSign FRANCE avise les Clients des modifications apportées à la présente PS, 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.

Si un changement apporté à la présente PS 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).

La PMA est l'entité à contacter pour toutes questions concernant la présente PS :

- 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 PS avec une majuscule auront la signification décrite dans l'annexe 1 « Définitions ».

Les modifications apportées au présent document sont communiquées aux tiers, le cas échéant uniquement en cas de modification majeure qui impacterait les Clients et les Signataires. L'entité qui audite le PSCo et l'ANSSI sont alertés des changements selon les procédures de l'ANSSI.

Les corrections de fautes d'orthographe ou de frappe qui ne modifient pas le sens de la PS sont autorisées sans avoir à être notifiées. Les modifications impactantes pour les Clients sont gérées conformément au contrat établi avec le client. Les Signataires sont avertis par la mise à jour des CGUs qui sont publiées par le PSCo. Si la PMA estime qu'une modification du présent document modifie le niveau de confiance assuré par les exigences contenues dans le présent document ou par le contenu des procédures opérationnelles, elle peut instituer une nouvelle politique avec un nouvel identifiant d'objet (OID).

La PMA donne un préavis d'1 mois au moins aux composantes du PSCo de son intention de modifier le présent document avant de procéder aux changements et en fonction de l'objet de la modification. Ce délai ne vaut que pour des modifications qui porteraient sur le fond (changement de taille de clé, changement de procédure, changement de Protocole de Consentement délégué, etc) et non sur la forme.

La PS est documentée et complémentée par des procédures opérationnelles confidentielles et est mise en œuvre et maintenue par le programme d'audit interne qui inclus au minimum les sujets suivants ; les règles de sécurité et les procédures opérationnelles, les installations techniques et physiques, les systèmes d'information et les actifs qui servent à mettre en œuvre le SSAS. La présente PS contient également l'information publique du « Practice Statement », mais le document s'appelle PS.

Le PSCo possède aussi une politique de sécurité des systèmes d'information (PSSI) qui est publiée en interne et communiquée à tous les employés concernés du PSCo. La PSSI n'est pas publique et elle vient compléter la PS pour l'aspect opérationnel et organisationnel du PSCo.

La PSSI et l'inventaire des actifs de sécurité de l'information du PSCo sont revus tous les ans ou en cas de modifications importantes afin de s'assurer leur pertinence, leur adéquation et leur efficacité continues. Toutes les modifications de la PSSI sont approuvées par la PMA.

La configuration des systèmes du PSCo est vérifiée tous les ans afin de détecter toute modification qui enfreindrait les politiques de sécurité du PSCo.

6.4.1.3 Gestion des actifs du SSASP

Le PSCo assurer un niveau de protection adéquat de ses actifs, y compris ses actifs informationnels. Les actifs fournis par l'intermédiaire d'un sous-traitant sont protégés conformément aux clauses de la PS qui mentionnent les sous-traitants dans le chapitre 6.

Le PSCo tient un inventaire précis des actifs comme condition préalable à une gestion efficace des vulnérabilités techniques et leur attribuer une classification conforme à l'évaluation des risques.

Pour chaque actif ou groupe d'actifs, l'inventaire contient, le cas échéant :

a) Un identifiant unique ;

b) Une description ;

c) Le propriétaire ;

d) L'emplacement ;

e) Le type (logiciel, matériel, services, installations, systèmes CVC, personnel, documents physiques, etc.) ;

f) Le type d'informations traitées ou stockées et leur classification ;

g) La date et la version de la dernière mise à jour ou du dernier correctif ;

h) Le niveau de classification ; et

i) La fin de vie.

Le PSCo attribue un niveau de classification à chaque actif ou groupe d'actifs, en fonction des exigences de protection de la confidentialité, de l'intégrité, de l'authenticité et de la disponibilité, et conformément à son évaluation des risques et à sa valeur commerciale. Le PSCo s'assure que les exigences de disponibilité de chaque actif, ou groupe d'actifs, classés sont conformes aux objectifs de continuité d'activité tels que décrits dans le plan de reprise d'activité et de continuité des services.

Le PSCo procède à des examens périodiques (une fois par an) des niveaux de classification des actifs.

Le PSCo identifie, documente et met en œuvre les règles d'utilisation acceptable et les procédures de gestion des informations et autres actifs associés.

Le PSCo met en œuvre et documente les procédures à suivre en cas de changement ou de cessation d'activité du personnel interne et externe, des sous-traitants ou autres tiers, notamment la restitution de tous les actifs physiques et électroniques précédemment attribués au PSCo ou qui lui ont été confiés.

Tous les supports de stockage sont gérés tout au long de leur cycle de vie (acquisition, utilisation, transport et élimination) conformément au système de classification et aux exigences de manipulation du PSCo.

Les supports de stockage utilisés dans les systèmes du PSCo sont manipulés en toute sécurité afin de les protéger contre les dommages, le vol, l'accès non autorisé et l'obsolescence.

Les procédures de gestion des supports de stockage sont définies de telle sorte à les protéger contre l'obsolescence et la détérioration pendant la période de conservation des documents.

6.4.2 Mesures de sécurité physiques

Le PSCO contrôle l'accès physique aux composants de son système dont la sécurité est essentielle à la fourniture de ses services de confiance et minimiser les risques liés à la sécurité physique.

L'accès physique aux composants du système du PSCo dont la sécurité est essentielle à la fourniture de ses services de confiance est limité aux personnes autorisées.

Des contrôles sont mis en œuvre pour éviter ; la perte, l'endommagement ou la compromission des actifs et l'interruption des activités ainsi que la compromission ou le vol des informations et des installations de traitement de l'information.

Les composants essentiels au fonctionnement sécurisé du service de confiance sont situés dans un périmètre de sécurité protégé, doté d'une protection physique contre les intrusions, de contrôles d'accès à travers ce périmètre et d'alarmes pour détecter les intrusions.

Les installations chargées de la génération et l'utilisation des Clés de signature sont exploitées dans un environnement qui protège physiquement les services contre toute compromission due à un accès non autorisé aux systèmes ou aux données. D'autres fonctions liées aux opérations de TSP peuvent être prises en charge dans la même zone sécurisée, à condition que l'accès soit limité au personnel autorisé.

6.4.3 Mesures de sécurité procédurales

Le PSCo met en place des comptes spécifiques à utiliser à des fins d'administration de la plateforme et des services pour ; l'installation, la configuration, la gestion ou la maintenance.

Les comptes privilégiés ne sont utilisés que si les privilèges sont nécessaires à l'activité spécifique.

Le PSCo révise les droits d'accès aux comptes privilégiés et administrateurs tous les et les modifie en fonction des changements organisationnels. Le résultat de cette révision, y compris les modifications nécessaires des droits d'accès, est documenté.

Le personnel du PSCo est responsable de ses activités.

6.4.4 Ressources humaines

Le PSCo veille à ce que l'ensemble du personnel, y compris les contractants temporaires, appliquent les règles de sécurité conformément à la PSSI et aux procédures spécifiques du PSCo.

Le PSCo emploie du personnel et, le cas échéant, des sous-traitants possédant l'expertise, la fiabilité, l'expérience et les qualifications nécessaires, et ayant reçu une formation en matière de cybersécurité et de protection des données personnelles, adaptée aux services offerts et à la fonction.

Le PSCo désigne au moins une personne responsable de la sécurité (RSSI) du réseau et de l'information, et qui rend compte à la direction.

Le personnel du PSCo satisfait aux exigences en matière de « connaissances, d'expérience et de qualifications », par le biais de formations et de certifications, d'une expérience pratique, ou d'une combinaison des deux. Ceci devrait inclut des mises à jour régulières (au moins tous les 12 mois) sur les nouvelles menaces et les pratiques de sécurité actuelles.

Le personnel employé par un PSCo comprend les personnes engagées contractuellement pour exécuter des fonctions supports aux services du TSP. Le personnel susceptible de participer à la supervision des services du TSP n'a pas besoin d'être employé du TSP.

Des sanctions disciplinaires appropriées sont appliquées aux personnes qui enfreignent les politiques ou les procédures du PSCo.

Les rôles et responsabilités en matière de sécurité de l'information, tels que définis dans la PSSI, seront consignés dans les descriptions de poste ou dans des documents accessibles à tout le personnel concerné et attribués en conséquence. Les rôles de confiance, indispensables au fonctionnement du PSCo, seront clairement identifiés.

Le personnel du PSCo (temporaire et permanent) a des descriptions de poste définies du point de vue des rôles remplis avec la séparation des tâches et le principe du moindre privilège, déterminant la sensibilité du poste en fonction des tâches et des niveaux d'accès, la vérification des antécédents et la formation et la sensibilisation des employés.

Les opérations et les domaines de responsabilité sont séparés afin de réduire les risques de modification ou d'utilisation abusive non autorisée ou involontaire des actifs du PSCo. Le cas échéant, les fiches de poste distinguent les fonctions générales des fonctions spécifiques au PSCo.

Le personnel met en œuvre des procédures conformément aux exigences du PSCo.

Les rôles techniques et rôle de confiance du PSCo sont similaires aux rôles définis par [319 401] et [419 241-1].

Le personnel d'encadrement possède une expérience ou une formation relative au service de confiance fourni, une connaissance des procédures de sécurité pour le personnel ayant des responsabilités en la matière, ainsi qu'une expérience de la sécurité de l'information et de l'évaluation des risques suffisante pour exercer ses fonctions de gestion.

L'ensemble du personnel du PSCo occupant des rôles de confiance est exempt de tout conflit d'intérêts susceptible de nuire à l'impartialité des opérations du PSCo.

Le personnel du PSCo est formellement nommé aux rôles de confiance par le président du PSCO, la PMA et le RSSI responsable de la sécurité selon les procédures du PSCo. Les rôles de confiance sont acceptés par la personne nommée pour remplir la fonction via la procédure d'attribution des rôles.

Le personnel n'a pas accès aux fonctions de confiance tant que les vérifications nécessaires n'ont pas été complétées.

Lorsque le personnel travaille à distance, le PSCo met en œuvre les mesures de cybersécurité pour protéger les informations consultées, traitées ou stockées en dehors des locaux du PSCo. Le PSCo autorise le travail à distance et a une politique spécifique au télétravail définissant les conditions et restrictions pertinentes en matière de cybersécurité pour les rôles de confiance.

6.4.5 Gestion des données des d'audit

Des mesures techniques et organisationnelles appropriées sont mises en œuvre contre le traitement non autorisé ou illicite de données à caractère personnel, ainsi que contre la perte accidentelle, la destruction ou l'altération de ces données.

Le PSCo enregistre et conserve en les rendant accessibles, pendant une période appropriée, y compris après la cessation de ses activités, toutes les informations pertinentes concernant les données émises et reçues par lui, notamment afin de servir de preuve dans le cadre de procédures judiciaires et d'assurer la continuité du service.

La confidentialité et l'intégrité des données d'audit colletées et archivées concernant l'exploitation des services doit est maintenue.

Les traces d'audits concernant l'exploitation des services sont archivées de manière complète et confidentielle, conformément aux exigences du PSCo.

Les traces d'audit concernant l'exploitation des services sont mises à disposition si nécessaire afin de fournir la preuve du bon fonctionnement des services dans le cadre de procédures judiciaires.

L'heure et la date précise des événements d'audit significatifs liés à l'environnement du PSCo, à la gestion des Clés de signature et à la synchronisation de l'horloge est enregistrée.

L'heure utilisée pour enregistrer les événements dans le journal d'audit (log) est synchronisée avec le temps universel coordonné (UTC) au moins une fois par jour. Afin d'avoir une exactitude temporelle des événements audités, au moins une source de temps convenablement synchronisée avec une source de temps standard est utilisée.

Les enregistrements d'audit concernant les services sont conservés pendant une période appropriée (même période que le Certificat associé à la Clé de signature) pour fournir les preuves judiciaires nécessaires et telle que notifiée dans les conditions générales du PSCo.

Les événements d'audit sont journalisés de manière à ne pas pouvoir être facilement supprimés ou détruits (sauf s'ils sont transférés de manière fiable sur un support à long terme) pendant la période de conservation requise.

Tous les événements de sécurité sont journalisés, y compris les modifications relatives à la politique de sécurité, les démarrages et arrêts du système, les plantages système et les défaillances matérielles, les activités des pares-feux et des routeurs, ainsi que les tentatives d'accès au système du SSAS.

Au minimum, les événements suivants sont journalisés :

- Les événements significatifs liés à l'environnement du SSAS et à la gestion des Clés (génération, utilisation et destruction) ;
- Les événements de signature du Signataire (par exemple : signature réussie avec la clé de signature du signataire et gestion des requêtes de signature) ;
- L'authentification du Signataire pendant le Protocol du Consentement ;
- La gestion du SAD du Signataire par le SSAS ;
- Le démarrage et l'arrêt de la fonction de génération des données d'audit ;
- Les modifications des paramètres d'audit.

Tous les enregistrements d'audit (y compris la journalisation spécifique aux services) contiennent les paramètres suivants :

- La date et l'heure de l'événement ;
- Le type d'événement ;
- L'identité de l'entité (par exemple : utilisateur, administrateur, processus) responsable de l'action ;
- Le succès ou l'échec de l'événement audité.

Les événements d'audit de signature du Signataire inclue le certificat ou une référence non ambiguë au Certificat associé à la Clé de signature. En effet, les traces d'audit du service SSAS et du service d'émission de Certificat peuvent être mutualisées car c'est le même TSP qui gère les deux services. Toutes les tentatives d'accès au SSAS devrait être journalisés.

Le cas échéant, le PSCo, en cas d'échec du transfert des informations d'audit vers un support de stockage externe, conserve les informations d'audit et essaye de nouveau de transférer les informations d'audit.

Les composants gérant l'audit du service SSAS collectent (sans remplacer mais en ajoutant) et maintiennent les traces d'audit et empêchent tout effacement des traces d'audit par leurs interfaces d'accès et d'utilisation. Ces mêmes composants protègent les traces d'audit en intégrité et permettent d'en vérifier l'intégrité.

6.4.6 Gestion des archives

Le PSCo conserve les enregistrements de données d'audit pendant au moins sept ans après que tout certificat basé sur ces enregistrements cesse d'être valide et dans les limites de la législation applicable.

6.4.7 Changement de Clé de signature

Pour chaque Transaction une Clé de signature est générée et dédiée à cette seule Transaction.

6.4.8 Gestion des incidents, vulnérabilités et plan de continuité

6.4.8.1 Surveillance et journalisation

Le PSCo met en place des mécanismes permettant de détecter les incidents de sécurité potentiels et d'y répondre en conséquence, en mettant en œuvre des outils et des processus permettant une surveillance et un enregistrement continus des activités sur le réseau et les systèmes d'information de l'entité.

Les activités de surveillance tiennent compte de la sensibilité des informations collectées ou analysées.

Les activités système anormales indiquant une potentielle violation de sécurité, y compris une intrusion dans le réseau du PSCo, sont détectées et signalées sous forme d'alarmes. Les activités système anormales peuvent inclure des analyses réseau (externes) ou des pertes de paquets.

Le PSCo tient à jour, documente et examine régulièrement les journaux, qui inclut :

a. Le trafic réseau entrant et sortant ;
b. Les activités relatives à l'administration des utilisateurs et à la gestion des permissions, ainsi qu'aux accès (y compris les accès privilégiés) aux systèmes et applications ;
c. Les activités effectuées avec les comptes d'administrateur ;
d. L'évaluation ou les modifications apportées aux fichiers de configuration critiques et aux sauvegardes ;
e. Les journaux relatifs à la sécurité ;
f. L'utilisation et les performances des ressources système ;
g. L'accès physique aux installations, le cas échéant ;
h. L'accès et l'utilisation des équipements et périphériques réseau ; et
i. Les événements environnementaux, le cas échéant.

Les systèmes du PSCo sont surveillés, notamment par la surveillance ou l'examen régulier des journaux d'audit, afin d'identifier les preuves d'activités malveillantes, en mettant en œuvre des mécanismes automatiques pour traiter les journaux d'audit et alerter le personnel en cas d'événements de sécurité critiques potentiels.

6.4.8.2 Réponse sur incidents

Le PSCo établit des procédures d'intervention en cas d'incident, notamment le confinement, la perte et le rétablissement.

Le PSCo se conforme aux obligations de l'ANSSI pour toutes déclarations prévues par les cadres législatifs pertinents en matière d'incidents de sécurité des réseaux et de l'information, y compris les autorités de surveillance et les équipes d'intervention en cas de crise (CSIRT).

Les prestataires de services de télécommunications (PST) doivent informer les parties prenantes des incidents conformément aux plans de communication convenus.

Le PSCo établit et maintient des plans de communication efficaces comprenant la catégorisation des incidents, des procédures d'escalade clairement définies et des protocoles de remontées d'incident standardisés.

Le PSCo s'assure que son personnel possède les compétences nécessaires pour détecter et gérer efficacement les incidents de sécurité.

Le PSCo crée et maintient une documentation complète tout au long du processus de détection et de gestion des incidents.

Le PSCo établit des documentations claires entre les processus de gestion des incidents et de gestion de la continuité des activités afin d'avoir une réponse coordonnée et cohérente lors des incidents.

Le PSCo teste et révise tous les ans, et après chaque incident, les rôles, les responsabilités et les procédures appropriées.

Le TSP remédie à toute vulnérabilité critique non traitée précédemment par le PSCo, dans un délai de 48 heures après sa découverte.

Pour toute vulnérabilité, compte tenu de son impact potentiel, le PSCo fait soit :

- Elaborer et mettre en œuvre un plan d'atténuation de la vulnérabilité ; ou
- Documenter les éléments factuels justifiant sa décision selon laquelle la vulnérabilité ne nécessite pas de correction.

Les procédures de signalement et de réponse aux incidents sont mises en œuvre de manière à minimiser les dommages causés par les incidents et dysfonctionnements de sécurité.

Le PSCo désigne du personnel de confiance chargé d'assurer le suivi des alertes relatives à des événements de sécurité potentiellement critiques et de veiller à ce que les incidents pertinents soient signalés conformément à ses procédures.

6.4.8.3 Remontée d'incident

Le PSCo établit des procédures de notification aux parties concernées, conformément à la réglementation applicable eIDAS et les exigences de l'ANSSI, de toute violation de sécurité ou perte d'intégrité ayant un impact significatif sur le service de confiance fourni et sur les données personnelles qui y sont conservées, dans un délai de 24 heures suivant l'identification de la violation.

Lorsqu'une violation de sécurité ou une perte d'intégrité est susceptible de porter préjudice à une personne physique ou morale bénéficiaire du service de confiance, le PSCo l'en informe également dans les meilleurs délais conformément au contrat entre le PSCo et les personnes impliquées.

Le PSCo établit une procédure simple permettant à son personnel, ses sous-traitants et ses clients de signaler les incidents potentiels de sécurité des réseaux et des systèmes d'information.

Le PSCo communique la procédure de signalement à ses sous-traitants et à ses clients et former son personnel à suivre la procédure de signalement et à s'adresser au point de contact approprié.

6.4.8.4 Évaluation et classification des événements

Le PSCo analyse les événements signalés et évalue leur gravité et le PSCo réévalue et reclasse les événements en fonction de nouvelles informations.

6.4.8.5 Examens post-incident

Le PSCo se tient informé par la veille des vulnérabilités techniques de tous les systèmes d'information qu'il utilise.

Le PSCo évalue son exposition à ces vulnérabilités et prend les mesures appropriées.

Le PSCo identifie la cause première de chaque incident et mène une analyse post-incident, pouvant aboutir à des mesures visant à atténuer le risque de récurrence d'incidents similaires.

Le PSCo s'assure que chaque incident passé a fait l'objet d'une analyse post-incident.

6.4.8.6 Gestion de la continuité de service

Le PSCo définit et maintient un plan de continuité d'activité à mettre en œuvre en cas d'incidents.

En cas d'incident, notamment la compromission d'une clé de signature privée ou de toute autre information d'identification du PSCo, les opérations sont rétablies dans les délais prévus par le plan de continuité d'activité, après avoir traité toute cause du sinistre susceptible de se reproduire (par exemple, une faille de sécurité) par

des mesures correctives appropriées. Parmi les incidents figurent aussi la défaillance de composants critiques du PSCo, notamment : le matériel et les logiciels.

6.4.8.7 Sauvegardes

Le PSCo maintient des copies de sauvegarde des informations et des ressources suffisantes, notamment ses installations, son réseau, ses systèmes d'information et son personnel, conformément à l'évaluation des risques et au plan de continuité d'activité.

Le PSCo définit des plans de sauvegarde prenant en compte au moins les éléments suivants :

a) Les délais de restauration ;

b) La protection de l'intégrité et de l'exactitude des copies de sauvegarde (y compris les données de configuration et les informations stockées dans un environnement de service cloud) ;

c) Le stockage des copies de sauvegarde dans un ou plusieurs lieux sûrs, situés hors du réseau du système sauvegardé et à une distance suffisante pour les protéger de tout dommage en cas de sinistre sur le site principal ;

d) Les contrôles physiques, environnementaux et logiques des copies de sauvegarde, conformément à leur niveau de classification des informations ; et

e) Les procédures de restauration des informations à partir des copies de sauvegarde (y compris les procédures d'approbation).

Le PSCo effectue un contrôle d'intégrité des copies de sauvegarde. Le PSCo teste à intervalles réguliers la restauration des copies de sauvegarde et des redondances et prendre des mesures correctives en cas de problème. Les résultats de ces tests doivent être documentés.

6.4.8.8 Gestion de crise

Le PSCo établi des procédures de gestion de crise portant au moins sur :

a) Les rôles et responsabilités en situation de crise ;

b) Les communications obligatoires et volontaires entre le PSCo et l'ANSSI ; et

c) Les contrôles appropriés pour maintenir la sécurité du réseau et des informations en situation de crise.

Le PSCo met en œuvre une procédure de gestion et d'utilisation des informations reçues du CSIRT national ou, le cas échéant, des autorités compétentes, informations utiles à la gestion de crise.

Le PSCo teste et révise, à intervalles planifiés ou dans le cadre du processus d'analyse post-incident, son plan de gestion de crise.

6.4.9 Fin de service du SSASP

Les perturbations potentielles pour les Signataires et les Vérificateurs de signature sont minimisées suite à la cessation des services du SSASP, et notamment la maintenance continue des informations nécessaires à la vérification de la fiabilité des services de confiance doit être assurée.

En particulier, le PSCo dispose d'un plan de fin de service à jour.

Avant de cesser ses services, le PSCo met en œuvre au moins les procédures suivantes, avant de cesser ses services :

- Le SSASP informe de la cessation les entités suivantes : les Clients du PSCo, autres entités avec lesquels le PSCo a conclu des accords ou entretenu d'autres formes de relations dans le cadre de l'utilisation tu SSASP, notamment les Vérificateurs de signature et l'ANSSI.
- Le PSCo communique l'information relative à la cessation aux autres parties prenantes.
- Le PSCo révoque l'autorisation de tous ses sous-traitants à agir en son nom pour toute fonction relative à l'émission de Signature à usage unique.

- Le PSCo transfère à un tiers de confiance l'obligation de conserver toutes les informations nécessaires pour prouver son fonctionnement pendant une période raisonnable, sauf s'il est démontré qu'il ne détient aucune de ces informations.
- Les clés privées des Signataires PSCo sont détruites ou mises hors service de manière à ce qu'elles ne puissent pas être récupérées.
- Le PSCo, dans la mesure du possible, prend des dispositions pour transférer la fourniture de services de confiance à ses clients existants à un autre PSCo.

Le PSCo prévoit un dispositif permettant de couvrir les coûts liés au respect de ces exigences minimales en cas de faillite ou d'incapacité, pour d'autres raisons, à les assumer lui-même, dans la mesure du possible et dans les limites de la législation applicable en matière de faillite.

Le PSCo précise dans ses procédure internes les modalités de résiliation du service. Celles-ci comprennent :

a) La notification des entités concernées ; et

b) Le cas échéant, le transfert des obligations du PSCo à des tiers.

Le PSCo maintient ou transfère à un tiers de confiance son obligation de mettre à disposition les certificats de la chaîne d'AC et la dernière CRL nécessaire à la validation des Signatures aux parties utilisatrices pendant une période raisonnable.

6.5 Contrôles techniques de sécurité

6.5.1 Gestion des systèmes et de la sécurité

Un PSCo gère sa sécurité pour exploiter un Système fournissant des services de création de signatures à usage unique.

Le Système prend en charge différents rôles techniques disposant de privilèges distincts.

Le Système prend en charge au minimum les rôles techniques suivants :

- Responsable de la sécurité : chargés de l'administration et de la mise en œuvre des politiques et pratiques de sécurité, et ayant accès aux informations relatives à la sécurité.
- Administrateur système : autorisés à installer, configurer et maintenir le Système, mais disposant d'un accès contrôlé aux informations relatives à la sécurité.
- Opérateur système : responsables de l'exploitation quotidienne du Système et autorisés à effectuer des sauvegardes et des restaurations système.
- Auditeur système : autorisés à consulter les archives et les journaux d'audit du Système afin d'auditer le fonctionnement du système conformément à la politique de sécurité.

Les responsables de la sécurité et les administrateurs système sont des utilisateurs système privilégiés. Les opérateurs et auditeurs système disposent de rôles privilégiés, mais ne sont pas autorisés à administrer ou configurer le Système au sens métier SSAS mais pas au sont autorisés au sens système d'exploitation et réseaux du Système.

Le Système prend en charge au minimum les rôles techniques métiers SSAS non privilégiés suivants :

- Signataire : autorisé à utiliser le Système en transmettant le SAD dans le cadre du SAP afin de signer le document ou le DTBS/R, qui peut également être transmis via le SAP.
- SCA : autorisé, pour un Client du PSCo, à envoyer la requête DTBS/R au Système afin qu'elle soit signée par un signataire.
- RA : autorisé à envoyer la demande de certificat de clé publique au Système et une requête de signature.

Un utilisateur privilégié ne peut pas assumer tous les rôles privilégiés et ne devrait pas en assumer plusieurs.

Les utilisateurs associés à des rôles privilégiés ne sont pas associés techniquement par le Système à des rôles non privilégiés. Les utilisateurs associés à des rôles non privilégiés ne sont pas techniquement associés à un rôle privilégié par le Système.

Le Système permet, d'un point de vue droit dans le Système, qu'un utilisateur autorisé à assumer le rôle Responsable de sécurité n'est pas autorisé à assumer le rôle d'auditeur système.

Le Système permet, d'un point de vue droit technique dans le Système, qu'un utilisateur autorisé à assumer le rôle d'Administrateur système et/ou d'Opérateur système n'est pas autorisé à assumer le rôle d'Auditeur système et/ou Responsable de sécurité.

Les personnes faisant partie d'un groupe d'utilisateurs système privilégiés sont nommées et formées par le PSCo.

Seuls les utilisateurs avec un rôle privilégié peuvent avoir si besoin est un accès physique au matériel et peuvent administrer le Système.

Seuls les utilisateurs système privilégiés disposent de privilèges étendus pour administrer le Système via toutes les applications et interfaces pertinentes.

6.5.2 Systèmes et opérations

6.5.2.1 Gestion des opérations

Le PSCo exploite le Système en s'assurant que ses fonctions de gestion opérationnelle sont correctement sécurisées.

Le fabricant du Système reçoit du PSCo des instructions permettant d'assurer :

- Une utilisation correcte et sécurisée du Système ;
- Son déploiement de manière à minimiser les risques de défaillance du système ;
- Sa protection contre les virus et les logiciels malveillants afin de protéger l'intégrité des systèmes et des informations qu'ils traitent.

Le fabricant du Système fournit une documentation système couvrant les responsabilités des quatre rôles privilégiés mentionnés dans le présent document. Cette documentation devrait inclure :

- Un guide d'installation ;
- Un guide d'administration ;
- Un guide d'utilisation.

6.5.2.2 Synchronisation du temps

La création de la signature et la vérification subséquente sont liées au temps ; il est donc nécessaire de s'assurer que le Système est correctement synchronisé avec au moins une source de temps standard UTC(k). Cette exigence est distincte de toute exigence d'horodatage pouvant être mise en place par le PSCo.

Le fabricant du Système indique la précision temporelle du Système et la manière dont elle est obtenue.

Afin d'avoir une précision temporelle des événements audités, une source de temps correctement synchronisée avec une source de temps standard est utilisée.

Afin de vérifier si un Certificat a expiré, une source de temps correctement synchronisée avec le temps UTC(k) est utilisée.

6.5.3 Contrôles de sécurité informatique

L'accès au Système du PSCo est limité aux personnes autorisées.

En particulier :

- Le PSCo gère les accès des Opérateurs, Administrateurs et autres comptes privilégiés, ainsi que des Auditeurs système, en appliquant le principe du moindre privilège lors de la configuration des droits d'accès au Système.
- Des procédures d'identification, d'authentification et d'autorisation multi-facteurs sont mises en œuvre pour les comptes privilégiés.

Le PSCo s'assure que les utilisateurs et les appareils sont authentifiés par des mécanismes d'authentification multi-facteurs avant d'accéder au réseau du PSCo et au Système.

Les données sensibles sont protégées contre toute divulgation ou réutilisation (si besoin est) et les supports de stockage accessibles à des utilisateurs non autorisés. Le Système génère une alerte signalant en temps opportun les événements inhabituels susceptibles d'affecter la capacité du Système à respecter les exigences techniques de sécurité définies dans le présent document.

Un mécanisme d'alerte en cas de détection d'un événement inhabituel est mis en place par le PSCo. L'alerte est déclenchée et notifie les personnes concernées du PSCo. Une alerte peut également permettre de déclencher des actions supplémentaires pour contrer d'éventuelles attaques, telles que la coupure technique du chemin utilisé par une attaque potentielle.

6.5.4 Contrôles de sécurité pendant le cycle de vie

6.5.4.1 Sécurité des opérations

Le PSCo utilise des logiciels et matériels fiables, protégés contre toute modification, et assure la sécurité technique et la fiabilité des processus qu'il met en œuvre.

En particulier :

- Une analyse des exigences de sécurité est réalisée lors de la conception et de la spécification des exigences de développement du Système, afin de d'intégrer de la sécurité dans le Système.
- Des procédures de gestion des changements sont appliquées aux mises en production, aux modifications et aux correctifs logiciels d'urgence pour le Système, ainsi qu'aux modifications de la configuration du Système qui impactent la politique de sécurité du PSCo.
- Les procédures document la gestion des modifications.

L'intégrité des systèmes et des informations de TSP est protégée contre les virus, les logiciels malveillants et non autorisés.

Des procédures sont établies et mises en œuvre pour tous les rôles de confiance et d'administration ayant une incidence sur la fourniture du SSAS.

Le PSCo spécifie et applique des procédures permettant que :

a) Les correctifs de sécurité sont appliqués dans un délai raisonnable après leur mise à disposition ;

b) Les correctifs de sécurité ne sont pas appliqués s'ils introduisent des vulnérabilités ou des instabilités supplémentaires qui l'emportent sur les avantages de leur application ; et

c) Les raisons de la non-application de certains correctifs de sécurité sont documentées.

Le PSCo établit, documente, met en œuvre, surveille et examine les configurations, y compris les configurations de sécurité, du matériel, des logiciels, des services et des réseaux.

Le PSCo surveille les configurations à l'aide d'un ensemble complet d'outils de gestion de systèmes.

Le PSCo examine régulièrement les configurations afin de vérifier les paramètres de configuration, d'évaluer la robustesse des mots de passe et d'analyser les activités réalisées.

6.5.4.2 Chaîne d'approvisionnement

Le PSCo identifie et met en œuvre des processus et des procédures pour gérer les risques de sécurité associés à l'utilisation des produits et services fournis par les fournisseurs, y compris la chaîne d'approvisionnement des systèmes d'information.

Le PSCo définit, documente et met en œuvre des processus et des procédures pour gérer les risques liés à la sécurité de l'information associés à l'utilisation des produits ou services des fournisseurs.

En particulier :

- La politique relative à la chaîne d'approvisionnement identifie et communique le rôle du PSCo au sein de cette chaîne.
- La politique relative à la chaîne d'approvisionnement définit les critères de sélection et de contractualisation des fournisseurs ou prestataires de services.

Ces critères incluent :

- La capacité du fournisseur ou du prestataire de services à respecter les spécifications, les niveaux de risque et de classification de cybersécurité des services, systèmes ou produits du PSCo fournis par le fournisseur ou le prestataire de services ;
- La capacité du PSCo à diversifier ses sources d'approvisionnement et à limiter sa dépendance vis-à-vis d'un fournisseur unique ; et
- Les résultats des évaluations coordonnées des risques de sécurité des chaînes d'approvisionnement critiques.

6.5.4.3 Procédure pour gérer la chaîne d'approvisionnement

Des processus et des procédures sont définis et mis en œuvre pour gérer les risques liés à la sécurité de l'information associés à la chaîne d'approvisionnement des produits et services des technologies de l'information et de la communication (TIC).

Le PSCo définit les exigences de sécurité de l'information applicables à l'acquisition de produits ou de services TIC.

Le PSCo exige que les fournisseurs de services TIC diffusent ses exigences de sécurité tout au long de la chaîne d'approvisionnement s'ils sous-traitent une partie du service TIC fourni au PSCo.

Le PSCo exige que les fournisseurs de produits TIC diffusent les bonnes pratiques de sécurité tout au long de la chaîne d'approvisionnement si ces produits incluent des composants achetés ou acquis auprès d'autres fournisseurs ou d'autres entités.

Le PSCo demande aux fournisseurs de produits TIC de fournir des informations décrivant les composants logiciels utilisés dans les produits.

Le PSCo demande aux fournisseurs de produits TIC de fournir des informations décrivant les fonctions de sécurité mises en œuvre dans leurs produits et la configuration requise pour leur fonctionnement sécurisé.

Le PSCo met en œuvre un processus de surveillance et des méthodes acceptables pour valider la conformité des produits et services TIC aux exigences de cybersécurité énoncées.

Le PSCo met en œuvre un processus d'identification et de documentation des composants critiques pour le maintien de la fonctionnalité des produits ou services.

Le PSCo s'assure que les composants critiques et leur origine sont traçables tout au long de la chaîne d'approvisionnement.

Le PSCo s'assure que les produits TIC livrés fonctionnent comme prévu sans aucune fonctionnalité inattendue ou indésirable.

Le PSCo met en œuvre des processus protégeant l'authentification des composants provenant des fournisseurs et leur conformité à leurs spécifications.

Le PSCo définit des règles de partage d'informations relatives à la chaîne d'approvisionnement et à tout problème ou compromission potentiel entre le PSCo et ses fournisseurs.

Le PSCo régulièrement surveille, examine, évalue et gère les changements apportés aux pratiques de sécurité de l'information et à la prestation de services des fournisseurs.

Le PSCo définit, met en œuvre et communique à toutes les parties intéressées concernées des politiques spécifiques relatives à l'utilisation des services cloud et à la manière dont il entend gérer les risques liés à la sécurité de l'information associés.

6.5.4.4 Responsabilités, contrats avec les fournisseurs et SLA

Lorsque le PSCo fait appel à des tiers, notamment des fournisseurs de services de confiance, pour la prestation de certains de ses services par le biais de la sous-traitance, de l'externalisation ou d'autres accords avec des tiers, il définit la responsabilité dans le contrat avec ses fournisseurs à propos de la conformité à la politique de la chaîne d'approvisionnement, à sa politique de sécurité de l'information et aux exigences définies dans le présent document.

Le PSCo définit la responsabilité des sous-traitants et s'assure que ces derniers sont tenus de mettre en œuvre tous les contrôles requis par le PSCo.

Ces processus et procédures incluent :

a) Ceux qui est mis en œuvre par le PSCo ;

b) Ceux que le PSCo exige du fournisseur pour le début de l'utilisation des produits ou services de ce dernier ; et

c) Ceux que le PSCo exige du fournisseur pour la cessation de l'utilisation des produits et services de ce dernier.

Le PSCo dispose d'un accord et d'une relation contractuelle documentés lorsque la fourniture de services implique la sous-traitance, l'externalisation ou d'autres arrangements avec des tiers afin d'avoir une compréhension claire entre le PSCo et le fournisseur concernant les obligations des deux parties en matière de respect des exigences de sécurité de l'information.

Lorsque le PSCo utilise un composant de service de confiance fourni par un tiers, il doit s'assurer que l'utilisation de l'interface du composant est conforme aux exigences spécifiées par le fournisseur du composant de service de confiance.

Lorsque le PSCo utilise un composant de service de confiance fourni par un tiers, il doit s'assurer que la sécurité et les fonctionnalités requises par le composant de service de confiance sont conformes aux exigences appropriées de la politique et des pratiques applicables.

Le PSCo inclut dans ses contrats de services des « accords de niveau de service » et/ou des mécanismes d'audit afin que les fournisseurs directs et les prestataires de services, y compris les fournisseurs de services de cloud computing, prennent des mesures de sécurité appropriées répondant aux exigences de sécurité du PSCo, conformément à l'évaluation des risques du PSCo.

La conformité aux politiques et exigences de sécurité du PSCo est prise en compte lors du processus de sélection de tout fournisseur direct ou prestataire de services dans le cadre du processus d'approvisionnement.

Les politiques et exigences de sécurité applicables des PSCo sont incluses dans les contrats conclus avec les fournisseurs directs ou prestataires de services.

Le PSCo examine la politique relative à la chaîne d'approvisionnement et surveiller, examiner, évaluer et gérer les changements apportés aux pratiques de cybersécurité des fournisseurs directs ou prestataires de services

à intervalles planifiés ou après un incident lié à la fourniture de services par des fournisseurs directs ou prestataires de services.

Le PSCo établit et tient à jour un registre des fournisseurs et de leurs contrats afin de suivre la gestion et/ou l'archivage des informations du PSCo.

Le PSCo régulièrement examine, valide et met à jour son registre des fournisseurs et de leurs contrats afin de s'assurer de leur validité, de leur adéquation à l'usage prévu et de la présence des clauses de sécurité des informations pertinentes.

6.5.5 Contrôles de sécurité du réseau

Le PSCo protège son réseau et ses systèmes contre les attaques.

Le PSCo segmente ses systèmes en réseaux ou zones en fonction d'une évaluation des risques prenant en compte les relations fonctionnelles, logiques et physiques (y compris la localisation) entre les systèmes et services de confiance.

Le PSCo applique les mêmes contrôles de sécurité à tous les systèmes situés dans la même zone.

Le PSCo limite l'accès et les communications entre les zones à ceux nécessaires à son fonctionnement.

Le PSCo interdit ou désactive explicitement les connexions et services non nécessaires.

Le FST révise régulièrement l'ensemble des règles établies.

Le PSCo maintient tous les systèmes critiques pour son fonctionnement dans une ou plusieurs zones sécurisées.

Le PSCo sépare le réseau dédié à l'administration des systèmes informatiques et son réseau opérationnel.

Le PSCo sépare logiquement les systèmes et réseaux d'administration des autres systèmes et réseaux d'information.

Le PSCo séparer les systèmes de production de ses services des systèmes utilisés pour le développement et les tests (par exemple, les systèmes de développement, de test et de préproduction).

Le PSCo établit la communication entre des systèmes distincts et dignes de confiance uniquement par le biais de canaux de confiance isolés par une séparation logique, cryptographique ou physique des autres canaux de communication et contrôle l'identification de ses points d'extrémité ainsi que la protection des données du canal contre toute modification ou divulgation.

Si un haut niveau de disponibilité de l'accès externe au service de confiance est requis, la connexion réseau externe est redondante afin d'avoir une disponibilité des services en cas de défaillance unique.

Le PSCo effectue régulièrement une analyse de vulnérabilité sur les adresses IP publiques et privées qu'il a identifiées et consigner la preuve que chaque analyse a été réalisée par une personne ou une entité possédant les compétences, les outils, l'expertise, le code de déontologie et l'indépendance nécessaires pour fournir un rapport fiable.

L'analyse de vulnérabilité demandée par est effectuée une fois par trimestre.

Le PSCo protège son réseau et ses systèmes d'information contre les logiciels malveillants et non autorisés au moyen d'un logiciel de détection et de suppression de logiciels malveillants, mis à jour au moins quotidiennement.

Le PSCo met à jour régulièrement son logiciel de détection et de réparation des logiciels malveillants.

Le PSCo réalise un test d'intrusion sur ses systèmes lors de leur mise en service et après toute mise à niveau ou modification de son infrastructure ou de ses applications jugées significative.

Le test d'intrusion est réalisé au moins une fois par an.

Le PSCo consigne les preuves que chaque test d'intrusion a été réalisé par une personne ou une entité possédant les compétences, les outils, l'expertise, le code de déontologie et l'indépendance nécessaires à la production d'un rapport fiable.

Des mécanismes de contrôle (pare-feu, par exemple) protègent les domaines du réseau interne du fournisseur de services de télécommunications contre tout accès non autorisé, y compris l'accès des abonnés et des tiers.

Les pares-feux sont également configurés pour bloquer tous les protocoles et accès non nécessaires au fonctionnement du fournisseur de services de télécommunications.

6.6 Audit de conformité et autres évaluations

Le service SSAS est audité par une entité externe d'audit dans le cadre de la qualification eIDAS. Le SSASP est audité de la même manière et suivant les mêmes règles que celles appliquées par l'AC et décrites dans le chapitre 8 de la PC de l'AC.

6.7 Autres sujets commerciales et juridiques

6.7.1 Frais

Les conditions tarifaires sont établies avec le Client et DocuSign dans le cadre contrat établit avec le Client.

6.7.2 Responsabilité financière

DocuSign France atteste avoir souscrit une assurance Responsabilité Civile Professionnelle concernant les prestations décrite dans ce document.

DocuSign France dispose de ressources financières suffisantes à son bon fonctionnement et à l'accomplissement de sa mission.

En cas de dommage subi par un Client du fait d'un manquement par le SSASP à ses obligations, Docusign pourra être amené à dédommager le Client dans la limite de la responsabilité du PSCo définie dans le contrat établi entre le Client et Docusign.

6.7.3 Confidentialité des informations commerciales

Les mêmes règles que celles de l'AC s'appliques et elles sont décrites dans la PC (se reporter au § 9.3 de la PC).

6.7.4 Confidentialité des informations personnelles

Des mesures techniques et organisationnelles appropriées sont prises pour prévenir tout traitement non autorisé ou illicite des données à caractère personnel et pour prévenir toute perte, destruction ou altération accidentelle de ces données. Les mêmes règles que celles décrites dans la PC de l'AC au chapitre 9.4 s'appliquent.

6.7.5 Droits de propriété intellectuelle

Les mêmes règles que celles décrites dans la PC de l'AC au chapitre 9.5 s'appliquent.

6.7.6 Obligations

Les mêmes règles que celles décrites dans la PC de l'AC au chapitre 9.6 s'appliquent.

Les obligations suivantes viennent s'ajouter :

- La PMS élabore et approuve la PS ;
- L'audit inclus les composants du PSCo qui mettent en œuvre le SSAS ;
- Le PSCo doit faire auditer PASSI le SPIE ;

- Le PSCo n'utilise que des QSCD notifiés par l'EU et à jour dans la liste des QSCD de l'EU ;
- Le PSCO n'utilise que des algorithme conformes aux exigences de [CRYPTO] pour les opérations de signature avec les Clés privées.

6.7.7 Exclusions de garanties

Les exclusions de garanties sont décrites dans les CGUs et le contrat établi entre le Client et Docusign.

6.7.8 Limite de responsabilité

Les limites de responsabilités sont décrites dans les CGUs et le contrat établi entre le Client et Docusign.

6.7.9 Indemnité

Les indemnités sont décrites dans les CGUs et le contrat établi entre le Client et Docusign.

6.7.10 Durée et résiliation

Les mêmes règles que celles décrites dans la PC de l'AC au chapitre 9.10 s'appliquent.

6.7.11 Avis individuels et communications avec les participants

Les mêmes règles que celles décrites dans la PC de l'AC au chapitre 9.11 s'appliquent.

6.7.12 Amendements

Les mêmes règles que celles décrites dans la PC de l'AC au chapitre 9.12 s'appliquent.

6.7.13 Procédures de règlement des litiges

Les procédures de règlement des litiges sont décrites dans les CGUs et le contrat établi entre le Client et Docusign.

6.7.14 Loi applicable

Les lois applicables sont décrites dans les CGUs et le contrat établi entre le Client et Docusign.

Les dispositions de la PS sont régies par le droit français.

6.7.15 Respect de la loi applicable

Le PSCo veille à exercer ses activités de manière légale et digne de confiance.

Le PSCo fournit des éléments de preuve démontrant qu'il satisfait aux exigences légales applicables.

6.7.16 Dispositions diverses

N/A.

6.8 Autres dispositions

6.8.1 Organisationnelle

N/A.

6.8.2 Tests supplémentaires

N/A.

6.8.3 Handicaps

Les services de confiance fournis et les produits destinés aux Signataires utilisés dans le cadre de la fourniture de ces services sont accessibles aux personnes handicapées, dans la mesure du possible.

Les normes d'accessibilité applicables, telles que la norme ETSI EN 301 549 [i.6], sont prises en compte.

6.8.4 Termes et conditions

Le PSCo met les CGUs relatives au SSAS à la disposition de tous les Signataires et des Vérificateurs via son site internet et lors de la mise en œuvre du SAP.

Les CGUs précise au moins les aspects suivants :

- La politique de service de confiance appliquée ;
- Les limitations d'utilisation du service fourni, y compris la limitation de responsabilité pour les dommages résultant d'une utilisation dépassant ces limitations (comme la durée de vie du Certificat) ;
- Les obligations du Signataire ;
- Les informations destinées aux Vérificateurs en référençant la politique de certification applicable ;
- Durée de conservation des journaux d'audit du PSCo ;
- Limitation de responsabilité ;
- Loi applicable ;
- Procédures de réclamation et de règlement des litiges ;
- Évaluation de la conformité du PSCo à la politique ;
- Coordonnées du PSCo ; et
- Engagement relatif à la disponibilité.

Les Signataires et les Vérificateurs sont informés des CGUs précises, y compris les éléments mentionnés ci-dessus, avant la conclusion d'un contrat.

Les CGUs sont communiquées par un moyen durable.

Les CGUs sont rédigées dans un langage facilement compréhensible.

Les CGUs sont disponibles en version électronique sur le site de publication du PSCo.