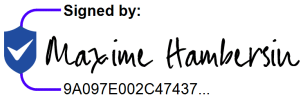
TSP 2 Certificate Policy and Public Certificate Practice Statement : ETSI : Seal and Remote Signature



TSP 2 CERTIFICATE POLICY AND PUBLIC CERTIFICATE PRACTICE STATEMENT : ETSI : SEAL AND REMOTE SIGNATURE

Version du document :	V 1.1	**Nombre total de pages :**	84
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
14/04/2026	1.0	EM	Passage en v 1.0	
01/06/2026	1.1	EM	Intégration des écarts LSTI ; intégration OID signature remote QSCD et précision sur la demande de révocation.	

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

La présente Politique, et statement, de Certification (*PC*) décrit les règles que ; DocuSign France en qualité de PSCo (Prestataire de Service de Confiance), ses Clients, les différentes entités du PSCo DocuSign France et les Porteurs doivent respecter pour assurer la gestion du cycle de vie de Certificats électroniques et de bi-clés associées.

Cette PC couvre deux types de Certificats, à savoir ce destinés :

- À la signature électronique qualifiée, conformément à l'article 3 de [eIDAS v2], de Documents par les Porteurs dans le cadre de Transactions électroniques réalisées entre eux en passant par la plateforme de DocuSign (noté IAM) ;
- À la création de cachet électronique avancé, conformément à l'article 3 de [eIDAS v2], de Documents par les Porteurs dans le cadre de Transactions électroniques réalisées entre eux en passant par la plateforme de DocuSign (noté IAM).

La PC pour les Porteurs qui mettent en œuvre un Certificat qualifié de signature électronique qualifiée le font à distance conformément à 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 v2].

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 ;
- [319 412] :
    - ETSI EN 319 412-1 : Electronic Signatures and Infrastructures (ESI); Certificate Profiles, Part 1: Overview and common data structures.
    - ETSI EN 319 412-2 : Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 2: Certificate profile for certificates issued to natural persons.
    - ETSI EN 319 412-5 : Electronic Signatures and Infrastructures (ESI), Certificate Profiles, Part 5: QCStatements.
- [119 312] : ETSI TS 119 312 : Electronic Signatures and Infrastructures (ESI) ; Cryptographic Suites ;
- [SSAS] : « Server Signing Application Service (SSAS) Policy and Practice Statement, Politique de Signature Remote QSCD, v 1.1 (dont l'OID est 1.3.6.1.4.1.22234.2.4.6.1.21) » ;
- [CRYPTO] : « European Cybersecurity Certification Group, Sub-group on Cryptography : "Agreed Cryptographic Mechanisms" published by the European Union Agency for Cybersecurity ('ENISA') » ;
- [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 28 acte d'implémentation] : « RÈGLEMENT D'EXÉCUTION (UE) 2025/1943 DE LA COMMISSION du 29 septembre 2025 portant modalités d'application du règlement (UE) n o 910/2014 du Parlement européen et du Conseil en ce qui concerne les normes de référence applicables aux certificats qualifiés de signature électronique et aux certificats qualifiés de cachet électronique » ;

- [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” ;
- [Article 24 1 c)] : « RÈGLEMENT D’EXÉCUTION(UE) 2025/1566 DE LA COMMISSION du 29 juillet 2025 portant modalités d’application du règlement (UE) no910/2014 du Parlement européen et du Conseil en ce qui concerne les normes de référence applicables à la vérification de l’identité et des attributs de la personne à laquelle le certificat qualifié ou l’attestation électronique d’attributs qualifiée doit être délivré ».

3 DEFINITIONS ET ABREVIATIONS

3.1 Définitions

Application Client : application mises en œuvre sous la responsabilité du Client qui lui permet d’élaborer des Documents et les faire signer par des Porteurs au cours d’une Transaction. L’Application du Client héberge les secrets de connexion à la plateforme IAM de Docusign.

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.

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.

Compromission : violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de la sécurité de cette clé privée.

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.

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 ».

Entité Légale : désigne la personne morale indiquée dans le Certificat et au nom de laquelle l'UH ou l'US utilise les Certificats Cachet.

Facteur d'activation Signature : désigne les données ou actions associées à un Signataire lui permettant de créer le SAD afin de mettre en œuvre sa Clé privée associé à un Certificat de signature, 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, …).

Facteur d'activation Cachet : désigne les données et actions associées à un CT lui permettant de mettre en œuvre la Clé privée associé à un Certificat de cachet via l'Application Client, ou directement auprès de la plateforme IAM de Docusign.

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 de la plateforme IAM permettant de lier une Transaction, un Document signé ou cacheté et un Certificat.

Identité Signataire : 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 qui est portée dans le Certificat.

Identité Entité Légale : identité de l'Entité Légale tel qu'inscrit sur un document officiel d'enregistrement des Entité Légale (par exemple un KBIS) et qui est portée dans le Certificat.

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

Politique(s) de Certification : désigne(nt) l'ensemble des règles identifiées par un OID et publiées par l'AC, décrivant les caractéristiques générales des Certificats qu'elle délivre. Ce document décrit les obligations et responsabilités de l'AC, de l'AE, des 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.

Représentant Habilité (ou Représentant Légale) : désigne toute personne physique disposant des pouvoirs de représenter une Entité Légale du fait de la loi. Dans le cadre du présent document, une telle personne aura la faculté de procéder à des demandes d'émission, de renouvellement et de révocation de Certificat auprès de l'AE par l'intermédiaire des CT qu'elle aura expressément et personnellement mandatés.

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.

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 entre un Client et un Porteur via la plateforme IAM de Docusign pour signer électroniquement et/ou créer un cachet sur un Document.

Unité d'Horodatage (UH) : désigne l'ensemble de matériels et de logiciels utilisés pour la création de contremarques de temps. L'UH est caractérisée par une identité certifiée par une AC et une clé unique de signature de contremarques de temps. L'UH construit une date et une heure d'UH qu'elle utilise pour les contremarques de temps qu'elle signe.

3.2 Abréviations

- AC : Autorité de Certification.
- AE : Autorité d'Enregistrement.
- CC : Critères Communs.
- CEL : Contact Entité Légale.
- CT : Contact Technique.
- DN : Distinguished Name.
- DPC : Déclaration des pratiques de certification.
- 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.
- 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 Exigences générales applicables

La présente PC suit exactement le sommaire du document [319 411-1] et est élaboré principalement à partir des exigences définies dans [319 441-2], [319 441-1] et [319 401] ainsi que dans les [Article 28 acte d'implémentation], [Article 24(5)] et [Article 24 1 c)].

4.2 Documentation applicable aux services de gestion de Certificat

4.2.1 CA Practice Statement

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

4.2.2 Politique Certification

La présente PC est la PC de Docusign France qui agit en qualité de PSCo pour la gestion des seules AC et Certificats Porteurs émis seulement par les ACs de DocuSign France. Cette PC est élaborée par DocuSign France. Les OIDs contenues dans cette PC sont communiquées dans les Certificats émis et dans les CGUs que les Porteurs doivent accepter et sur le site de publication du PSCo. DocuSign France utilise seulement ses propres OIDs.

La présente PC couvre les types de Certificats suivants :

- Certificat Cachet : de niveau LCP, NPC+ et QCP-L ;
- Certificat Signature : de niveau QCP-N QSCD.

Lorsque des règles sont spécifiques à un type de Certificat et/ou de niveau ETSI, alors elles seront identifiées comme suit :

- Si besoin en indiquant le type de Certificat ; et/ou
- Si besoin en distinguant AC et Porteur ; et/ou
- Si besoin un ou plusieurs OID de PC.

4.2.3 CGU et PDS

Les CGUs sont définies par Docusign pour chaque service de gestion de Certificats et publiées par l'AC. Les CGUs sont des documents distincts de la PC.

De même, l'AC élabore de PDS pour les Certificat QCP-L et QCP-N QSCD qui sont publiées par l'AC.

4.3 Composants du service

Les services de certification sont décomposés dans le présent document en services composants suivants aux fins de la classification des exigences :

- Service d'enregistrement :
    - Certificat cachet : ce service collecte et vérifie les informations d'identification du Contact Technique (CT), et d'Identité Entité Légale, qui demande un certificat, avant de transmettre le résultat au service de génération de certificat ;
    - Certificat Signature : ce service collecte et vérifie les informations d'identification du Porteur, et d'Identité Porteur, qui demande à signer un Document dans le cadre d'une Transaction électronique avant de transmettre le résultat au service de génération de certificat ;
- Service de génération de bi-clé et de Certificat : ce service génère les bi-clés et les Certificats électroniques pour les Porteurs à partir des informations transmises par le service d'enregistrement ;
- Service de remise de publication :
    - Certificat Cachet : ce service remet au CT son Certificat par mail, ou permet au CT de le récupérer ou dans l'application IAM de Docusign et dans tous les cas via le formulaire de demande de Certificat ;
    - Certificat Signature : ce service remet au Porteur (Signataire) son Certificat dans l'application IAM via le Document signé dans le cadre de la Transaction ;
    - Certificat Porteur en général : dans tous les cas les Certificats des Porteurs ne sont pas publiés par l'AC.
    - PDS, PC, Certificats d'AC et CGU : le PSCo publie ces informations sur son site institutionnel ;
- Service de révocation de certificats : ce service traite les demandes de révocation des Certificat et détermine les actions à mener, dont la génération des Liste de Certificats Révoqués (LCR). Les résultats de ce service sont donnés ;
- Service de statut de Certificat : ce service met à disposition des utilisateurs de certificat (UC) les informations nécessaires à l'utilisation des certificats émis par l'AC, ainsi que les informations de validité des certificats issues des traitements du service de gestion des révocations via les mécanismes d'OCSP et de CRL ;
- Service de personnalisation de token : le PSCo ne met pas en œuvre ce type de service.

Les composantes du PSCo mettent en œuvre leurs services conformément à la présente PC et la DPC associée.

Les changements majeurs au sein du PSCo sont notifiés à l'ANSSI.

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

5.1 Exigences générales

La présente PC définit les exigences de sécurité pour tous les services décrits ci-dessus dans la gestion des certificats. La Déclaration des Pratiques de Certification (notée DPC), partie confidentielle, donnera les détails des pratiques des composantes du PSCo dans cette même perspective. La présente PC contient tout de même les descriptifs des services décrits au § 4.3.

Les usages des Certificats sont décrits dans la présente PC.

5.2 Exigences sur la PC

Les exigences sur la PC et les pratiques associées sont décrites dans la présente PC. La présente PC est publiée (Cf. § 6.1).

Les limitations de taille par rapport au RFC 5280 sont indiquées au § 6.2.1.

La structure de la PC suit celle de [319 411-1].

Les algorithmes utilisés sont décrits au § 6.6.

L'usages des clés et des Certificats d'AC et de Porteurs sont décrits au § 6.3.5 et 5.5.

5.3 PC nom et OIDs

Seul des changements majeurs modifiant le niveau de sécurité d'un Certificat ou l'émission d'un même type de Certificat sous une nouvelle AC oblige au changement d'OIDs.

La présente PC, dont le nom est donné en page 1 du présent document, couvre les OIDs suivants :

- AC « Docusign Qualified CA G1 » :
    - ETSI EN 319 411-2 QCP-N QSCD :
    - 1.3.6.1.4.1.22234.2.14.3.60 : Ce profil est mis en œuvre par l'AC et certifié ETSI avec le nouveau profil de certificat et en utilisant le service [SSAS].
- AC « Docusign Advanced Seal CA G1 » :
    - ETSI EN 319 411-1 LCP :
    - 1.3.6.1.4.1.22234.2.14.3.63 : Ce profil est mis en œuvre par l'AC et certifié ETSI avec le nouveau profil de certificat.
- AC « Docusign Qualified Seal CA G1 » :
    - ETSI EN 319 411-2 QCP-L :
    - 1.3.6.1.4.1.22234.2.14.3.64 : Ce profil est mis en œuvre par l'AC et certifié ETSI avec le nouveau profil de certificat.
- AC « Docusign Qualified TimeStamp CA G1 » :
    - ETSI EN 319 411-1 NCP+ :
    - 1.3.6.1.4.1.22234.2.14.3.61 : Ce profil est mis en œuvre par l'AC et certifié ETSI avec le nouveau profil de certificat.

5.4 PSCo composants

5.4.1 Policy Management Authority (PMA)

La PMA est DocuSign France.

La PMA est responsable de l'AC dont elle garantit la cohérence et la gestion du référentiel de sécurité, ainsi que sa mise en application.

Le référentiel de sécurité de l'AC est composé de :

- La présente PC.
- La DPC associée.
- Des conditions générales d'utilisation (CGU), des PDS, et des procédures mises en œuvre par les composantes du PSCo.

La PMA a pour missions principales :

- Valide le référentiel de sécurité composé de la PC et de la DPC.
- Valide l'analyse de risque et homologue les services du PSCo.
- Autorise et valide la création et l'utilisation des composantes du PSCo.
- Suit les audits et/ou contrôle de conformités effectuées sur les composantes du PSCo.
- Décide des actions à mener et veille à leur mise en application.
- Approuver les services délivrés par le PSCo.
- Approuver la PC.
- Approuver la création et la révocation d'AC.
- Approuver le choix de l'ACR et de l'ACI à utiliser pour signer l'AC.
- Approuver les choix cryptographiques pour l'IGC et les clés et les certificats gérés par le PSCo.
- Approuver les standards utilisés. Ce qui garantit le niveau de sécurité et l'acceptation de l'AC par l'ACR.
- Approuver la compatibilité entre la PC et la DPC.
- Approuver le rapport d'audit annuel des composantes du PSCo.
- Approuver les rapports d'audit des entités externes au PSCo réalisés par DocuSign France.
- Approuver les Protocoles de Consentements définis par DocuSign France.
- Garantir la validité et l'intégrité des informations publiées.
- S'assurer qu'un processus de gestion des incidents est mis en œuvre par chaque composante du PSCo et suivre la gestion des incidents.
- Arbitrer les litiges relatifs aux services d'IGC et s'assurer qu'une solution est communiquée auprès des entités concernées.

Les missions plus détailles sont données dans la DPC.

5.4.2 Autorité de Certification (AC)

L'AC, composante technique de PSCo, génère des Certificats et révoque des Certificats à partir des demandes que lui envoie l'AE.

DocuSign France s'appuie sur ses propres capacités d'Opérateur de Service de Certification (OSC) afin de mettre en œuvre l'ensemble des opérations cryptographiques nécessaires à la création et la gestion du cycle de vie des Certificats avec ses propres ACs.

L'AC est mise en œuvre conformément à la présente PC et à la DPC associée qui sont établies par la PMA. Dans la présente PC, l'AC est identifiée par son « Common Name » (*« CN »)* lorsque *de besoin.*

DocuSign France est AC au sens de la responsabilité de gestion du cycle de vie des certificats.

Les AC sont sous la hiérarchie des ACI et ACR de DocuSign France.

5.4.3 Autorité d'Enregistrement (AE) :

L'AE est chargée d'authentifier et d'identifier les Porteurs.

DocuSign France est AE.

La DPC donne les détails de l'organisation de l'AE et des procédures mises en œuvre par l'AE en fonction des types de certificats que l'AE délivre aux Utilisateurs.

Dans tous les cas, l'AE agit conformément à la PC et à la DPC associée qui sont établies par la PMA.

L'AE ne peut pas commencer à délivrer des Certificats sans l'accord préalable de la PMA.

5.4.4 Opérateur de Service de Certification (*OSC*)

L'OSC assure des prestations techniques, en particulier cryptographiques, nécessaires aux services du PSCo, conformément à la présente PC et à la DPC.

L'OSC est techniquement dépositaire de la clé privée de l'AC utilisée pour la signature des Certificats. Sa responsabilité se limite au respect des procédures définies afin de répondre aux exigences de la présente PC et de la DPC des composantes du PSCo.

L'OSC ne peut pas commencer des opérations pour des services du PSCo sans l'accord préalable de la PMA.

Dans la présente PC, son rôle et ses obligations ne sont pas distingués de ceux de l'AC. Cette distinction sera précisée dans la DPC.

Les composantes d'IGC sont opérées de la manière suivante :

- DocuSign France est OSC pour l'AC, l'AE, l'OCSP et le Service de Publication (*SP*).

5.4.5 Service de Publication (*SP*)

Le SP est mis en œuvre par DocuSign France.

Le SP est utilisé pour la mise en œuvre du service de publication (*Se reporter au § 6.1*).
Le SP agit conformément à la PC et à la DPC associée.
Le SP ne peut publier que des informations approuvées par la PMA.

5.4.6 SSASP (PSCo) DocuSign France

Le PSCo est DocuSign France qui met en œuvre le SSAS conformément à [SSAS].

Ce composant est utilisé dans le cadre de la mise en œuvre des Certificat Signature pour la signature qualifiée.

5.4.7 Porteur

5.4.7.1 Certificat Signature

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

Au cours de cette Transaction, le Porteur manifeste son consentement pour le ou les Document(s) 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.

Au sens de l'ETSI est le Subject et le Subscriber.

5.4.7.2 Certificat Cachet

5.4.7.2.1 Technical Contact

Un Contact Technique est une personne nommée et autorisé par un Représentant habilité de l'Entité Légale, ou une personne autorisée par le Représentant Habilité, de l'Entité Légal et qui est autorisée à :

- Remplir les formulaires de demande de Certificat ;
- Vérifier les Certificat ;
- Mettre en œuvre la création de cachet à l'aide de Facteur d'Activation de son choix et sous son contrôle ;
- Procéder le cas échéant aux demandes de révocation des Certificats ;

- Désigner à l'AE le CEL en donnant ces informations de contact pour les opérations de renouvellement de Certificat dans le formulaire de demande de Certificat simplifié (si l'AE met en œuvre le renouvellement simplifiée).

Au sens de l'ETSI est le Subscriber. Le Subject est l'Entité Légal au nom de laquelle le Certificat est émis.

5.4.7.2.2 Contact Entité Légale (CEL)

Désigne une personne physique appartenant à l'Entité Légale et qui est désignée par le CT dans les demandes de renouvellement simplifiée et qui signe les demandes de renouvellement simplifiée. Si le CT est en contrat avec l'Entité Légale mais n'appartient pas à l'Entité Légale alors le CEL est une personne physique différente du CT sinon il n'y a pas besoin de CEL pour un renouvellement.

Les CGU définissent notamment que le CEL doit :

- Effectuer correctement et de façon indépendante les contrôles d'identité des futurs CT de l'entité pour laquelle elle/il est CEL ;
- Vérifier et approuver les demandes de renouvellement simplifiées de Certificat ;
- Respecter les engagements décrits dans les CGU ;
- Respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

Le CEL est définit et autorisé uniquement pour les AC qui ne sont que certifiées ETSI.

Au sens de l'ETSI le CEL est le Subscriber.

5.4.8 Client

5.4.8.1 Certificat Signature

Le Client désigne l'entité, 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 SSAS via la plateforme de IAM pour mettre en œuvre une Transaction ;
- Générer le Document qui sera présenté au Signataire pour signature ;
- Insère les informations de contact du Signataire qui sera partie prenante à la Transaction et par conséquent le Porteur du Certificat.

5.4.8.2 Certificat Cachet

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

- Désigner un CT et le RL et l'Entité Légale pour laquelle un Certificat sera émis par l'AC ;
- Mettre en œuvre l'application Client qui génère le Document sur lequel une création de cachet sera effectué via la plateforme de IAM lors d'une Transaction.

L'Entité Légale détient le nom du service applicatif contenu dans le Certificat.

5.4.9 Prestataire de Vérification d'Identité à Distance (*PVID*)

Le PVID est une entité contractuellement liée à DSF par un Contrat de Service approuvé par la PMA.

Le PVID n'est utilisé que dans l'identification des Porteurs pour un Certificat Signature.

Le PVID définit, met en œuvre et maintient une Politique d'Identification.

Le PVID doit être certifié par l'ANSSI avant d'être utilisé.

Le PVID transmet un bulletin opérationnel au PSCO de manière régulière.

5.4.10 DocuSign Inc.

L'entité qui met en œuvre la plate-forme IAM pour gérer les Transaction.

Docusign permet de mettre en œuvre un service de persistance d'identité électronique dans le cadre de la pérennisation d'une Identité vérifiée par un PVID certifié comme décrit dans [SSAS].

5.4.11 Vérificateur (ou Utilisateur de Certificat UC)

Le vérificateur est une personne physique ou une machine qui réalise la validation d'un Document signé ou cacheté. Dans le cadre d'un Certificat Signature l'UC valide le document comme indiqué dans [SSAS] en qualité de Vérificateur. Dans tous les cas l'UC valide un Certificat en utilisant les règles de validation telles que décrites dans le présent document au § 5.5 et 6.3.5 et en tenant compte obligatoirement des informations les plus récentes sur le statut du Certificat comme fourni par la CRL et l'OCSP.

5.5 Utilisation de Certificat

5.5.1 Domaines d'utilisations applicables

5.5.1.1 Certificat de l'AC

Le certificat de l'AC sert à authentifier les Certificats, les LCR et les Certificats d'OCSP. La clé privée associée au certificat d'AC sert pour :

- La signature de Certificats.
- La signature de CSR.
- La signature de Certificats de répondeurs OCSP.
- La signature de LCR.
- La signature de réponses OCSP uniquement pour le Certificat Signature.

Il est à noter que la clé privée associée au certificat d'OCSP ne sert que pour signer des réponses OCSP comme décrit dans la présente PC.

Un Porteur qui obtient un Certificat émis par l'AC est authentifiable dans le domaine de confiance Adobe AATL.

5.5.1.2 Certificat Signature

Les clés privées associées aux Certificats délivrés aux Porteurs sont exclusivement utilisées par les Porteurs pour signer électroniquement des Documents, et une CSR, dans le cadre de Transaction initiées par des Clients conformément à [SAAS].

Les Certificats émis le sont pour des personnes physique seulement et ne comportent aucune information de rattachement à une quelconque entité légale.

Une telle signature électronique qualifiée apporte, outre l'authenticité et l'intégrité d'un Document ainsi signées, la manifestation du consentement du signataire quant au contenu de ce Document pour l'UC qui utilise le Certificat afin de valider la signature du Document.

5.5.1.3 Certificat Cachet

Les clés privées associées aux Certificats délivrés aux CTs sont exclusivement utilisées pour technique créer des cachet et signer des CSRs.

Un certificat de porteur délivré par l'AC est utilisé par les UC pour :

- Certificat LCP et QCP-L : désigne un Certificat permettant de valider le cachet avancé apposé sur un Document afin d'attester de l'Identité Entité Légale, donc de l'origine du Document, et de l'intégrité du Document émis par l'Entité Légale ;
- Certificat NCP+ : désigne un Certificat permettant de valider les contremarques de temps qualifiées émises seulement par DocuSign France.

5.5.2 Domaines d'utilisations interdits

Les utilisations de Certificats émis par l'AC à d'autres fins que celles prévues au § 5.5.1 ci-dessus ne sont pas autorisées. En pratique, cela signifie que DocuSign France ne peut être en aucun cas tenue pour responsable d'une utilisation autre que celles prévues dans la présente PC.

Les ACs ne sont pas cross certifiées avec des ACs externes au PSCo.

Les Certificats ne peuvent être utilisés que conformément aux lois applicables en vigueur propres à la signature électronique.

Cette PC décrit la gestion du cycle de vie des Certificats de signature et de leurs clés privées associées, elle n'a pas vocation de remplacer une politique de signature ou de création de cachet, qui elle décrit la gestion du cycle de vie des signatures et des créations de cachets.

6 PRATIQUES DU PSCO

6.1 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

La PMA, via le SP institutionnel du PSCo, rend disponibles les informations suivantes :

- La PC : https://www.docusign.com/fr-fr/mentiones-legales/politiques-de-certifications.
- Les certificats de la chaîne de confiance auxquels les AC sont rattachées à savoir : https://www.docusign.com/fr-fr/mentiones-legales/politiques-de-certifications.
- Les conditions générales d'utilisation (*CGU*) sont publiées par la PMA : https://www.docusign.com/fr-fr/mentiones-legales/politiques-de-certifications.
- Certificat Signature : les certificats de l'ACR et de l'AC et du Porteur sont contenus dans le Document signé par le Porteur.
- Certificat Cachet : les Certificats de l'Entité Légale sont contenus dans le formulaire de demande de Certificat (comme établi au § 6.3.1) signé par le CT, le TL et l'AE.

La dernière CRL de chaque AC expirée est mise en ligne de manière durable avec toute la chaîne d'AC dans le site utilisé pour la publication des PC (https://www.docusign.com/fr-fr/mentiones-legales/politiques-de-certifications). Elle sera aussi accessible en ligne en utilisant l'adresse CRL DP tant que l'infrastructure technique le permet.

En cas de panne du SP institutionnel du PSCo, 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.

L'AC publie en production les informations suivantes avec un taux de disponibilité de 99,9% :

- Le PDS est publié pour les certificats qualifiés seulement sont publiées par l'AC en production et l'URL est dans le profil de Certificat.
- LCR : elle est publiée par l'AC en production et son URL est contenu dans le Certificat.

Le SP et le site de publication de l'AC en production sont disponibles 24 heures par jour et 7 jours par semaine avec le taux de disponibilité indiqué ci-dessus pour le SP et le site de publication de l'AC.

Les parties confidentielles de la DPC ne sont pas publiées mais consultable auprès de la PMA sur demande justifiée et après autorisation de la PMA et uniquement dans le cadre d'audit.

Les informations identifiées ci-dessus sont disponibles :

- PC
    - Avant la mise en service initiale du service.

- Dans les meilleurs délais après une mise à jour de PC approuvée par la PMA.

- Certificat d'AC :
  - Avant la mise en service initiale du service.
  - Dans les meilleurs délais après la génération d'un certificat d'AC suivant un renouvellement.

Le SP et l'AC s'assure que les informations sont disponibles et protégées en intégrité contre les modifications non autorisées.

L'ensemble des informations publiques et publiées est libre d'accès en lecture et téléchargement sur Internet et dans un langage compréhensible.

6.2 Identification et authentification

6.2.1 Nommage

Les identités utilisées dans un Certificat sont conformes au RFC 5280 et [319 412], l'AC (Issuer) et le Porteur (subject) sont identifiés par un Distinguished Name (DN).

Certificat Signature :

Dans les profils de certificats, les tailles informations dans le DN ne sont pas celle définies par la RFC 5280 et sont les suivantes :

- Taille DN = maximum 1042 octets.
- Taille C = 2 octets
- Taille OU = maximum 508 octets.
- Taille CN = maximum 512 octets.
- Taille serialNumber = 20 octets maximum
- Taille GN = le GN est limité par le CN et donc l'ensemble GN plus SN respecte la taille du CN.
- Taille SN = le SN est limité par le CN et donc l'ensemble GN plus SN respecte la taille du CN.

Certificat Cachet :

Dans les profils de certificats, les tailles informations dans le DN ne sont pas celle définies par la RFC 5280 et sont les suivantes :

- Taille DN = maximum 1534 octets.
- Taille CN = maximum 512 octets.
- Taille O = maximum 512 octets.
- Taille OI = maximum 508 octets.
- Taille C = 2 octets

6.2.1.1 Nécessité d'utilisation de noms explicites

Les Certificats émis conformément à la présente PC n'ont de sens que si l'Identité qui apparaît dans les Certificats peut être comprise par les UC. Les Identités utilisées permettent d'identifier les AC et les Porteurs comme décrit ci-après.

6.2.1.1.1 AC

Une bi-clé ne peut être liée qu'à un unique CN pour chaque AC.

6.2.1.1.2 Certificat Signataire

Dans tous les cas, l'Identité Signataire portée dans le Certificat est construite à partir d'au moins un des noms et prénoms de son état civil tel que portés sur le document officiel d'identité du Porteur utilisé par l'IDP et l'AE.

Si la représentation formelle du prénom et/ou du nom de famille nécessite une translittération, cette translittération suit l'édition actuelle du document 9303 de l'OACI, partie 3, section 6. A. Translittération des caractères multinationaux à base latine.

Seul des Certificats qui contiennent le nom de l'AE, qui a enregistré le Porteur, dans le champ « OU » du DN peuvent être émis par l'AC.

L'identité utilisée pour les certificats d'AC et de Porteur ne sont ni un pseudonyme ni un nom anonyme.

Les UC peuvent se servir de l'identité incluse dans les Certificats afin d'authentifier les Porteurs. Pour le Porteur, le champ « CN » n'est pas garanti unique.

6.2.1.1.3 Certificat Cachet

Les noms choisis pour désigner l'Entité Légale dans le Certificat sont obligatoirement des noms tels qu'inscrits sur un document officiel d'enregistrement de l'Entité Légale (par exemple un KBIS).

S'agissant de Certificats cachet, les notions d'anonymisation ou de pseudonymisation sont sans objet.

Les UC peuvent se servir de l'identité incluse dans les Certificats afin d'authentifier une Entité Légale émettrice de cachet électronique et une application ou marque particulière en fonction de la valeur du champs CN contenu dans le Certificat.

Pour le Porteur, le champ « CN » n'est pas garanti unique.

6.2.1.2 Unicité des noms

6.2.1.2.1 AC

Les identités des certificats sont uniques au sein du domaine de certification de l'AC.

La PMA assure cette unicité au moyen de son processus d'enregistrement.

6.2.1.2.2 Certificat Signataire

Les DN émis par l'AC dans les Certificats sont uniques au sein du domaine de certification de l'AC. Durant toute la durée de vie de l'AC, un DN attribué à un Porteur ne peut être attribué à un autre Porteur.

A noter que l'unicité d'un Certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de certification de l'AC, mais que ce numéro est propre au Certificat et non pas au Porteur et ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un Porteur donné.

Le serialNumber dans le DN du Porteur est unique et est attribué de manière unique à chaque Certificat émis par l'AC et par conséquent permet de distinguer des homonymies.

En plus de cela afin de lier le Certificat à la personne physique (Porteur), l'AE assure cette unicité au moyen de son processus d'enregistrement et de la valeur unique de l'identifiant de Transaction et de contexte de signature attribués à un Porteur et contenus dans les champs OU du Certificat Porteur. Un identifiant de Transaction et de contexte de signature est associé au Porteur par l'AE et le SSASP (se reporter à [SSAS]) pour chaque Transaction et donc pour chaque Certificat associé à la Transaction.

En cas de différent au sujet de l'utilisation d'un nom pour un certificat, la PMA a la responsabilité de résoudre le différend en question.

6.2.1.2.3 Certificat Cachet

Les DN émis par l'AC dans les Certificats sont uniques au sein du domaine de certification de l'AC. Durant toute la durée de vie de l'AC, un DN attribué à un Porteur ne peut être attribué à un autre Porteur.

A noter que l'unicité d'un Certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de certification de l'AC, mais que ce numéro est propre au Certificat et non pas au Porteur et ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un Porteur donné.

Le Certificat est rattaché de manière non ambigüe à l'Entité Légale via le champ O et OI.

En cas de différend au sujet de l'utilisation d'un nom pour un certificat, la PMA a la responsabilité de résoudre le différend en question.

6.2.1.3 Identification, authentification et rôle des marques déposées

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L. 711-1 et suivants du Code de la propriété intellectuelle (codifié par la loi n° 92-957 du 1er juillet 1992 et ses modifications ultérieures) appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

Le PSCo ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par un Porteur et les Clients des marques déposées, des marques notoires et des signes distinctifs, ainsi que des noms de domaine.

6.2.2 Validation initiale de l'identité

L'AE ne collecte lors des demandes de Certificat que ce qui est strictement nécessaire à :

- L'identification et l'authentification des personnes et Entité Légales ;
- La collecte des informations à inscrire dans le Certificat ;
- L'établissement de preuves d'Identité Signataire et Identité Entité Légale suffisantes pour satisfaire aux exigences de l'utilisation prévue du Certificat.

Les Certificats que le PSCo émet pour lui-même ou pour des personnes qui sont en contrat avec lui (en tant que Porteur) suivent exactement les règles définies dans la présente PC.

L'opérateur d'enregistrement de l'AE qui vérifie l'identité ne doit pas être la personne physique à qui le Certificat est délivré (en tant que Porteur).

6.2.2.1 Certificat Signataire

L'AE vérifie l'identité du Porteur avant l'émission de son Certificat. Pour ce faire, le Porteur est identifié et authentifié à distance par l'IDP, via un processus PVID, au cours de la Transaction qui vérifie l'aspect vivant de la personne physique, le titre officiel d'identité et le lien entre la personne et le titre officiel d'identité. Au cours du processus d'identification, l'IDP récupère les informations suivantes :

- Date et lieu de naissance, référence à un document d'identité reconnu à l'échelle nationale, ou d'autres attributs pouvant être utilisés, dans la mesure du possible, pour distinguer la personne des autres personnes ayant le même nom ;
- Nom complet tel qu'inscrit sur le titre d'identité utilisé par le Porteur ;
- Type de titre officiel d'identité ;
- Numéro de série du titre officiel d'identité ;
- Date de validité du titre officiel d'identité ;
- Numéro de téléphone portable du Porteur qui est l'information de contact du Porteur ;
- Adresse électronique du Porteur qui est l'information de contact du Porteur.

L'AE est responsable de vérifier que l'IDP a collecté les informations requises, qu'elles sont intègres et que c'est l'IDP qui en est à l'origine. L'AE est responsable de collecter et stocker les informations requises afin de pouvoir prouver l'identité portée dans le Certificat ainsi que des informations utilisées par le Porteur pour signer (adresse électronique et numéro de téléphone portable).

Au cours de ce processus d'enregistrement, il est proposé, cela est optionnel, au Porteur de créer un compte dans le service de persistance d'identité de Docusign en utilisant son téléphone portable enregistré comme décrit dans [SSAS]. Ce service permet au Porteur de s'authentifier plus facilement comme expliqué ci-après au § 6.2.3.

Les informations non vérifiées ne sont pas introduites dans les certificats.

6.2.2.2 Certificat Cachet

6.2.2.2.1 Entité Légale

L'AE qui procède à la vérification s'assure que l'Entité Légale existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande du Certificat aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité de l'organisation comprennent le numéro SIREN, le numéro de déclaration de TVA, le DUNS, etc.

L'AE collecte et vérifie les informations suivantes :

- Le nom officiel complet de l'Entité Légale tel qu'enregistre (par exemple le nom de l'Entité Légal tel qu'inscrit sur un KBIS) ;
- L'identifiant officiel de l'Entité Légal (par exemple le numéro de SIREN de l'Entité Légal tel qu'inscrit sur un KBIS) qui sera mis dans le champ OI du Certificat ;
- Le nom, prénom, numéro de téléphone et courriel (qui est l'information de contact du RL et CT) du RL et du CT ;
- La copie de pièce d'identité du CT ;
- La ou les pièces justificatives de l'existence de l'Entité Légale et des informations de l'Entité Légale mises dans le Certificat ;
- Le cas échéant si utilisé, la preuve de délégation du RL auprès d'une personne autorisée à signer à sa place la demande de Certificat.

6.2.2.2.2 CT et RL

L'authentification par l'AE des organisations du RL et du CT repose sur la vérification des informations fournies par le CT dans le cadre de sa demande de Certificat. Ces informations comprennent le nom et l'adresse de l'organisation ainsi que les documents ou les références de l'existence de celle-ci.

L'AE qui procède à la vérification s'assure que l'organisation existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans la demande du certificat aux informations recueillies dans les bases de données officielles de référence.

Les informations susceptibles d'être vérifiées pendant l'authentification de l'identité de l'organisation comprennent le numéro SIREN, le numéro de déclaration de TVA, le DUNS, etc.

Dans tous les cas, la vérification de l'appartenance d'un CT et du RL aux organisations mentionnées dans la demande de Certificat dont il se réclame est effectuée.

Les informations non vérifiées ne sont pas introduites dans les certificats.

De même, la délégation du CT et des personnes autorisées par le RL pour demander le Certificat au nom de l'Entité Légale et le gérer sont obtenues au travers des informations obtenues dans la demande de Certificat.

Le CT et le RL en tant que personne physiques sont identifiées et authentifiées par l'AE à partir des informations contenues dans le dossier de demande de Certificat et la signature de la demande de Certificat. Un nouveau CT requiert un nouvel enregistrement.

Pour les Certificat Cachet de niveau LCP, le RL et la CT signe la demande de Certificat avec le service de signature avancée de DocuSign France qui requiert une identification à distance et une vérification de la pièce d'identité utilisée par le CT et le RL.

Pour les Certificat Cachet de niveau NCP+ et QCP-L :

- Le RL signe la demande de Certificat avec le service de signature avancée de DocuSign France qui requiert une identification à distance et une vérification de la pièce d'identité utilisée par le RL ;
- Le CT signe la demande de Certificat en utilisant le service de signature qualifié de DocuSign France (AC « DocuSign Premium Cloud Signing CA - G2 » utilisant le service avec un PVID certifié par l'ANSSI).

6.2.2.2.3 CEL

L'AE qui procède à la vérification s'assure que le CEL appartient soit à l'Entité Légale du Client et que l'entité à laquelle appartient le CEL existe toujours et est toujours légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies dans le formulaire de demande simplifié aux informations recueillies dans les bases de données officielles de référence et le formulaire de demande initiale de Certificat.

6.2.3 Identification et validation d'une demande de renouvellement des clés

6.2.3.1 Identification et validation pour un renouvellement courant

6.2.3.1.1 AC

Le renouvellement de certificat d'AC s'apparente en situation normale à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales et est approuvé par la PMA.

6.2.3.1.2 Certificat Signature

Pour ce paragraphe, le Porteur est déjà enregistré par l'AE et un premier Certificat lui a été délivré avec succès. Ce paragraphe traite donc d'un nouveau Certificat avec une nouvelle bi-clé pour le Porteur (Cf. § 6.3.7).

L'AE est aussi dans ce cas également responsable, comme pour le premier enregistrement, de la mise à jour, de la collecte et du stockage des informations requises afin de fournir la preuve de l'identité du Porteur inscrite

dans le Certificat pour l'opération de renouvellement. L'AE effectue directement les opérations d'identification et d'authentification du Porteur avant de procéder au renouvellement du Certificat.

L'AE doit vérifier l'existence et la validité du Certificat courant (et non révoqué) à renouveler et que les informations utilisées pour vérifier l'identité et les attributs du Porteur sont toujours valides.

Si les CGU de l'AC ont changées, celles-ci doivent être communiquées au Porteur.

Si tout ou partie des informations du Porteur à mettre dans le Certificat ont changées alors l'enregistrement doit être réalisé avec la procédure telle que définie à l'article 6.2.2 ci-dessus pour l'ensemble des informations ayant changées.

Les informations utilisées pour authentifier le Porteur lors du Protocole de Consentement (*comme l'adresse de courrier électronique et le numéro de téléphone*) ne peuvent être modifiées que par le Porteur après vérification effectuée par l'AE afin d'être sûr que les informations de mise à jour sont liées au Porteur pour le Protocole de Consentement.

En fonction du choix du Porteur, l'AE applique la même procédure que celle décrite pour le Certificat initial (Cf. § 6.2.2) ou requiert que le Porteur s'authentifie avec son service de persistance d'identité comme décrit dans [SSAS].

Cette pratique, permettant d'obtenir un nouveau Certificat sans procéder à l'identification initiale décrite à la section 6.2.2 ci-dessus, est limitée à une durée maximale de 3 ans. Le nombre de Certificats requis par les Transactions nécessitant sa signature n'est pas limité. Le Porteur peut continuer à utiliser le service de persistance d'identité uniquement si l'IDP est toujours certifié et si le titre d'identité utilisée lors de l'identification initiale est toujours approuvé par l'ANSSI.

Après ce délai de 3 ans, le Porteur est tenu de procéder à une nouvelle identification complète comme décrite au § 6.2.2 pour démarrer un nouveau cycle de 3 ans.

Il peut supprimer sa persistance d'identité à tout moment via l'interface de la plateforme DocuSign, en utilisant son compte.

Si le Porteur :

- Souhaite modifier son adresse électronique, son nom ou son numéro de téléphone portable, il doit procéder à une nouvelle identification complète, comme décrit à la section 6.2.2 ci-dessus, afin de démarrer un nouveau cycle de 3 ans avec un nouveau compte dans le service de persistance d'identité.

- Pour avoir un autre compte dans le service de persistance d'identité (par exemple en raison de la perte de sa clé à la suite de la suppression de l'appareil, à une panne…), le Porteur doit effectuer une identification complète initiale comme décrit dans la section 6.2.2 ci-dessus pour commencer un nouveau cycle de 3 ans avec un nouveau compte de persistance d'identité.

6.2.3.1.3 Certificat Cachet

La procédure de renouvellement est identique à celle décrite au § 6.2.2.

Il est possible de procéder à un renouvellement simplifié tant que l'Entité Légale est en relation contractuelles pour le service de cachet avec l'organisation du CT et que l'organisation du CT est en relation contractuelle avec DocuSign pour l'utilisation de service de cachet.

L'authentification de ces demandes de renouvellement simplifiées sont effectuées par l'AE et s'apparente à authentifier le CT et le CEL et leur organisations respectives ainsi que celle du client comme décrit au paragraphe 6.2.2. Une demande de renouvellement simplifiée est signée par le CEL et le CT. Un CEL est requis quand le CT n'appartient pas à l'Entité Légale.

Pour l'instant cette démarche simplifiée n'est pas mise en œuvre.

6.2.3.2 Identification et validation pour un renouvellement après révocation

Pour l'AC ; le renouvellement de certificat s'apparente à un renouvellement de la bi-clé et l'attribution d'un nouveau certificat conformément aux procédures initiales et approuvées par la PMA.

Pour le Porteur, les mêmes procédures que celles décrites au § 6.2.2 s'appliquent.
Un renouvellement en ce cas aussi nécessite une nouvelle bi-clé et un nouveau Certificat.

6.2.4 Identification et validation d'une demande de révocation

6.2.4.1 AC

Les demandes de révocation sont authentifiées par la PMA. La procédure de vérification est identique à celle utilisée pour l'enregistrement initial. La demande de révocation est constituée par un document de nommage signé par la PMA qui est transmis à l'OSC pour mettre en œuvre la cérémonie des clés de révocation.

Il n'y a pas de période de grâce dans le cas d'une révocation d'une AC. La PMA demande la révocation d'un certificat dès lors qu'elle en identifie une cause de révocation comme définie au et la révocation est effectuée dans un délai de 10 jours ouvrés maximum.

En cas de révocation d'un des certificats de la chaîne de certification, le PSCo informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs concernés que leurs Certificats ne sont plus valides.

Pour cela, le PSCo pourra par exemple envoyer des alertes au Client ou publier une information sur le site institutionnel du PSCo.

Ces derniers devront informer les Porteurs en leur indiquant explicitement que leurs Certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide si besoin est en fonction de l'analyse des causes et des impacts dues à la révocation de l'AC.

L'ANSSI est alerté par la PMA immédiatement en cas de révocation d'un des certificats de la chaîne de certification.

L'ANSSI se réserve le droit de diffuser par tout moyen l'information auprès des promoteurs d'applications au sein des autorités administratives et auprès des usagers.

Les Certificats d'AC sont révoqués si une des causes suivantes apparaît :

- L'ACR et/ou l'ACI qui ont émis l'AC est révoquée ou cesse son activité.
- Raison de sécurité invoquée par rapport à l'AC par la PMA ou l'ANSSI.

Les ACR et ACI génère des CRL qui sont valides maximum 1 an.

6.2.4.2 Certificat Porteur : causes possibles d'une révocation

Un Certificat Porteur est révoqué si une des circonstances suivantes arrive :

- L'AC est révoquée.
- Le DN du Porteur est non correctement rempli.
- Le Porteur ou l'AE n'a pas respecter les règles de la PC ou de la DPC.
- La clé privée du Porteur est compromise ou suspectée d'être compromise.
- Le PSCO est informé d'un changement qui impacte la validité du Certificat.

- La cryptographie utilisée pour le Certificat n'est plus considérée comme fiable selon l'ENISA.

6.2.4.3 Certificat Porteur : Origine d'une demande de révocation

Le Porteur peut demander la révocation pour les raisons suivantes :

- Le DN du Porteur est non correctement rempli.
- Le Porteur ou l'AE n'a pas respecter les règles de la PC ou de la DPC.
- La clé privée du Porteur est compromise ou suspectée d'être compromise.

L'AE peut demander la révocation pour les raisons suivantes :

- Le DN du Porteur est non correctement rempli.
- Le Porteur ou l'AE n'a pas respecter les règles de la PC ou de la DPC.
- La clé privée du Porteur est compromise ou suspectée d'être compromise.

La PMA peut demander la révocation pour les raisons suivantes :

- L'AC est révoquée ;
- Le DN du Porteur est non correctement rempli.
- Le Porteur ou l'AE n'a pas respecter les règles de la PC ou de la DPC.
- La clé privée du Porteur est compromise ou suspectée d'être compromise.
- Le PSCO est informé d'un changement qui impacte la validité du Certificat.
- La cryptographie utilisée pour le Certificat n'est plus considérée comme fiable selon l'ENISA.

Le statut d'un Certificat est donné par la CRL et l'OCSP.

6.2.4.4 Délai accordé au Porteur pour formuler la demande de révocation

Dès que le Porteur ou l'AE a connaissance qu'une des causes possibles de révocation de son ressort, est effective, il formule sa demande de révocation sans délai.

6.2.4.5 Demande de révocation Porteur

Pour révoquer un Certificat, seul le Client peut faire une demande d'incident auprès de l'AE. En cas de besoin, c'est au Porteur de se rapprocher du Client pour qu'il déclare l'incident auprès de l'AE.

L'AE authentifie le Client, analyse la remontée d'incident et décide si cela est effectivement une raison de révocation valide.

Si l'incident est effectivement une raison valide de révocation, alors l'AE procède à la demande de révocation. Au préalable l'AE doit faire signer une demande de révocation au Client en utilisant une signature avancé telle que fournie par DocuSign France :

- Certificat Signataire : l'AE demande au Client de fournir l'identifiant de Transaction associé au Certificat et si c'est le Porteur qui demande la révocation une preuve que le Porteur a signalé l'incident soulevé par le Client. L'AE vérifie que le contact du Client est bien un contact déclaré chez Docusign comme Client et que le Client est bien à l'origine de la Transaction dans la Plateforme de Docusign. L'AE utilise les informations de contact du Client pour lui faire signer la demande de révocation ;
- Certificat Cachet : l'AE utilise pour faire signer la demande de révocation, les informations de contact du CT telle que contenues dans la demande de Certificat à révoquer. Si le CT a changé alors il est nécessaire de faire signer un autre CT appartenant à l'entité légale du CT telle que déclarée dans la demande de Certificat. L'authentification est du nouveau CT est effectué par l'AE avec le même niveau de sécurité qu'un enregistrement initiale.

Si ce n'est pas le cas, alors l'AE ne procède pas à la révocation.

6.2.4.6 Délai de traitement par l'AC d'une demande de révocation Porteur

Le service de révocation est disponible uniquement pendant les jours ouvrés du PSCO (Service Client).

Une demande de révocation de Certificat, authentifié et dûment établie par l'AE, et signée par le CT et l'AE (se reporter au § 6.2.4.5), de Certificat est authentifiée et traitée dans un délai inférieur à 24 heures à compter de la signature de la demande de révocation par le CT (se reporter au § 6.2.4.5). La LCR signée, qui a une validité de 6 jours, par l'AC est émise toutes les 12 heures. Par conséquent le statut sera connu pour l'UC par le mécanisme :

- De CRL au plus tard 12 heures après la décision technique de révocation émanant de l'AE ;
- D'OCSP au plus tard quelques secondes après la décision technique de révocation émanant de l'AE.

Si le PSCo ne peut pas respecter le délai de 24H00 pour traiter la demande, la procédure reste malgré tout la même pour traiter la demande de révocation.

Si l'AE ne peut pas traiter la demande en moins de 24H00 alors cela est entièrement tracé par l'AE (raison, action prises et temps total pris pour révoquer le Certificat).

L'AC ne met pas en œuvre le mécanisme dit de révocation à une date future.

Les systèmes du PSCo utilisé pour gérer la révocation sont synchronisé au moins une fois toute les 24H00 avec une source de temps UTC.

6.3 Exigences opérationnelles sur le cycle de vie des Certificats

L'objet du chapitre 6.3.1, 6.3.2, 6.3.3 et 6.3.4 est de décrire le processus de demande d'un premier certificat. La gestion des certificats suivants sont décrits dans les chapitres 6.3.6, 6.3.7 et 6.3.8.

6.3.1 Demande de certificat

6.3.1.1 AC

Une demande de certificat d'AC est effectuée par la PMA. Les ACs sont enregistrées et autorisée par la PMA avant leur émission. Une demande de création d'AC contient :

- L'identifiant de l'AC intermédiaire ou Racine qui signe son certificat d'AC.
- L'identification de l'entité légale qui est AC.
- La CSR de la bi-clé de l'AC ;
- L'ensemble des informations qui composent le certificat d'AC.

Dans tous les cas une demande de certificat est assimilée au document de nommage signé par la PMA.

6.3.1.2 Certificat Signataire

Le Porteur été enregistré conformément à la clause 6.2.2, et l'Identité Signataire a été validée en conséquence.

La demande de Certificat est assimilée à une demande de signature de Document via une Transaction dans la plateforme Docusign comme décrit dans [SAAS]. C'est le Client qui initie cette Transaction et donc la demande de Certificat.

L'AE est responsable de la collecte des informations et de la vérification de la demande de Certificat comme décrite au § 6.2.2.

6.3.1.3 Certificat Cachet

Le Porteur été enregistré conformément à la clause 6.2.2, et l'Identité Signataire a été validée en conséquence.

Une Entité Légale demande au Client de procéder à la demande de Certificat en contactant Docusign. C'est ensuite, l'AE qui envoie le formulaire de demande de Certificat au CT qui la rempli.

L'AE est responsable de la collecte des informations et de la vérification de la demande de Certificat comme décrite au § 6.2.2.

6.3.2 Traitement d'une demande de certificat

La procédure de délivrance du Certificat est liée de manière sécurisée et non ambiguë à l'enregistrement associé, y compris l'identification du Porteur.

6.3.2.1 AC

La PMA est responsable d'identifier, authentifier et traiter la demande de certificat d'AC soumises par le contact administratif. La PMA authentifie les demandes de certificat d'AC (*Cf. § 3.2*) et valide le contenu de la demande de certificat. La PMA autorise ou rejette la création d'un certificat AC.

6.3.2.2 Certificat Signataire

La demande est authentifiée et validée par l'AE comme décrit au § 6.2.2. Le Porteur a 24H00 après une identification réussie avec l'IDP pour signer le Document et donc demander son Certificat en utilisant ses Facteurs d'Activation. Passer ce délai le Porteur doit de nouveau faire une nouvelle identification avec l'IDP.

L'AE authentifie l'IDP utilisé dans le processus d'identification du Porteur (Cf. § 6.2.2). Les communications entre l'IDP, la plateforme Docusign et l'AE sont toutes protégées en confidentialité et intégrité.

L'AE est responsable de vérifier que de la demande de Certificat est exact, autorisée et complète. En cas de rejet de la demande le Porteur en est informé par la plateforme Docusign.

En cas d'approbation de la demande, l'AE :

- Présente le Protocole de Consentement au Porteur afin que le Porteur puisse accepter les CGUs, relire les informations ; nom et prénom qui seront utilisés pour produire son Certificat et email et numéro de téléphone qui seront utilisés par le SSASP.
- Si le Porteur accepte et valide l'ensemble alors le Porteur utilise ses Facteurs d'Activation pour s'authentifier et permettre à l'AE de générer le SAD (Cf. [SSAS]) et de transmettre la demande de Certificat à l'AC.
- Si le Porteur refuse alors le processus s'arrête et le Certificat n'est pas généré.

6.3.2.3 Certificat Cachet

La demande est authentifiée et validée par l'AE comme décrit au § 6.2.2.

L'AE est responsable de vérifier que de la demande de Certificat est exact, autorisée et complète. La demande de Certificat est gérée dans la plateforme Docusign.

LCP et QCP-L : En cas d'approbation de la demande, l'AE :

- Signe la demande de Certificat ;
- Demande à l'AC de générer une bi-clé et une CSR ;
- Insère la CSR dans la demande de Certificat et appose un cachet technique sur la demande de Certificat ;
- Fait signer la demande de Certificat par le RL et le CR comme indiquée au § 6.2.2 ;
- Transmet la demande à l'AC si les RL et CT ont tous deux signés la demande de Certificat.

- Si le RL et ou le CT n'ont pas signé et/ou si la demande de Certificat dépasse les 3 mois alors la demande de Certificat est abandonné et le Certificat n'est pas produit.

NCP+ : En cas d'approbation de la demande, l'AE :

- Le CT a généré une bi-clé lors d'une cérémonie des clés chez l'OSC avec du personnel de confiance ;
- Le CT insère la CSR dans la demande de Certificat ;
- Le CT signe la demande de Certificat comme indiquée au § 6.2.2 ;
- Fait signer la demande de Certificat par le RL comme indiquée au § 6.2.2 ;
- Transmet la demande à l'AE qui vérifie la demande et si les RL et CT ont tous deux signés la demande de Certificat.
- Si le RL et ou le CT n'ont pas signé et/ou si la demande de Certificat dépasse les 3 mois alors la demande de Certificat est abandonné et le Certificat n'est pas produit.

L'ensemble des signatures de l'AE, du RL et du CT ne peut pas dépasser 90 days à partir de la signature de l'AE.

En cas de rejet de la demande, l'AE en informe le Porteur.

6.3.3 Délivrance du certificat

Les numéros de série des Certificats sont aléatoires et ont une longueur exacte de 20 octets.

Les Certificats émis ne dépasse pas la date d'expiration de l'AC émettrice.

La procédure de délivrance du Certificat est liée de manière fiable à la génération de la bi-clé par l'AC.

L'AC prend des mesures contre la falsification des Certificats.

L'AC livre le Certificat de manière sécurisée afin de garantir leur authenticité.

Ce n'est que l'AC qui gère les bi-clés des Porteurs soit via le [SSAS] soit en via l'AE.

Comme expliqué au § 6.2.1, la construction du DN des Certificat Porteur fait qu'un DN ne peut pas être attribué à un autre Porteur.

L'OID (Cf. § 5.3 et § 6.6.1) de PC mis dans les Certificats sont seulement ceux définis par DocuSign France. En plus de ces OIDs, les Certificats contiennent les OIDs d'Adobe afin de pouvoir être utilisé dans les lecteurs Adobe.

6.3.3.1 AC

La PMA transmet la demande de certificat acceptée à l'OSC pour la réalisation de la cérémonie des clés.

Les ACs sont générées pendant une cérémonie des clés dans les locaux de l'OSC.

Le certificat d'AC est signé au cours d'une cérémonie de certification de l'AC dans les locaux de DocuSign France. La cérémonie des clés de l'AC et la cérémonie de certification de l'AC ne sont pas obligatoirement effectuées le même jour. Dans tous les cas, la cérémonie des clés nécessite l'activation des clés d'AC sous multiples contrôles (Cf. § 6.5.1).

La PMA vérifie le contenu du document de nommage des AC, en termes de complétude et d'exactitude des informations présentes. Ce document est utilisé comme base de réalisation de la cérémonie de clés de création des AC.

À la fin de la cérémonie des clés, les clés privées de l'AC n'existent que sous forme de sauvegarde (Cf. § 6.5.2) et sont transférées dans la ressource cryptographique (HSM) de production (Cf. 6.5.2).

6.3.3.2 Certificat Signataire

Si Porteur a été correctement authentifié via le Protocole de Consentement alors l'AC peut générer la bi-clé du Porteur (Cf. [SAAS] et § 6.5.1 du présent document). Les bi-clés sont uniquement gérées par le PSCo et ne sont pas transmises au Porteur.

La bi-clé du Porteur est utilisée par le SSASP pour signer une CSR afin de transmettre la clé publique à certifier à l'AC.

L'AC authentifie le SSASP et signe le certificat. L'ensemble des communications est protégé en intégrité et confidentialité.

Une fois que le Certificat est émis par l'AC, le SSASP peut signer le Document et ensuite permettre à la Plateforme Docusign de remettre le Certificat au Porteur contenu dans le Document signé.

6.3.3.3 Certificat Cachet

Une fois que la demande de Certificat est complète et signé dans les temps, alors l'AC peut produire le Certificat en utilisant la CSR contenue dans la demande de Certificat. L'AC transmet le Certificat à l'AE.

Le Certificat généré est inséré par l'AE dans la demande de Certificat qui est ensuite transmise au CT et RL via la plateforme Docusign sauf pour le Certificat NCP+ qui est directement donné par l'AC au CT.

L'ensemble des communications est protégé en intégrité et confidentialité.

6.3.4 Acceptation du certificat

Les CGU indiquent comment le Porteur accepte les CGUs.

Les CGUs sont l'agreement au sens ETSI qui lie le PSCo et le Porteur, le CT et le RL en fonction du type de Certificat. Les CGUs n'ont pas besoin d'imposer d'exigence auprès du Porteur sur le HSM à utiliser pour générer les bi-clé car c'est le PSCo qui gère le HSM et les bi-clés.

Les CGUs acceptées par le Porteur permettent d'avoir son consentement quant à la conservation par le PSCo et ses sous-traitants des données personnelles et des informations contenues dans la demande de Certificat utilisées lors de l'enregistrement, y compris si celle-ci sont destinées à une autre personne (par exemple CT et RL qui sont différents) et à toute révocation ultérieure (Cf. § 6.4.5 et § 6.4.6), à l'Identité Signataire ou Identité Entité Légale et à tous les attributs spécifiques placés dans le Certificat, et à la transmission de ces informations à des tiers dans les mêmes conditions que celles prévues par la PC en cas de cessation des services du PSCo.

Une fois que le Porteur a le Certificat, le Porteur a un délai fixé dans les CGU pendant lequel il peut contrôler le contenu du Certificat et le cas échéant demander sa révocation en cas d'information erronées dans le Certificat ou si le Certificat est non conforme. Passer ce délai, le Certificat est considéré par le PSCo comme accepté par le Porteur et valide.

Les CGUs imposent au Porteur de vérifier le contenu du Certificat et d'en demander sa révocation si le contenu du Certificat n'est pas conforme ou possède des informations erronées.

6.3.4.1 AC

La PMA vérifie que le certificat d'AC généré contient les informations décrites dans le document de nommage signé. Dès que la PMA confirme l'adéquation entre le certificat généré et le document de nommage, alors la PMA accepte le certificat émis et le témoin de la PMA signe une acceptation officielle du certificat émis. L'AC ne peut pas émettre de Certificat ni de CRL tant que le certificat d'AC n'est pas accepté par la PMA.

6.3.4.2 Certificat Signataire

Avant d'émettre le Certificat, l'AE informe le Porteur des CGU du Certificat (Cf. § 6.9.4) via le Protocole de Consentement. Le CGUs sont publiées sur un serveur en https. Lors du Protocole de Consentement les CGUs sont récupérées directement auprès du PSCo en production qui est sous le seul contrôle du PSCo.

Lors de la mise en œuvre du Protocole de Consentement, l'AE collecte et stocke l'acceptation du Porteur et l'empreinte des CGUs que le Porteur a accepté lors de ce Protocole de Consentement.

6.3.4.3 Certificat Cachet

Avant d'émettre le Certificat, l'AE informe le CT et le RL des CGU du Certificat (Cf. § 6.9.4) via le formulaire de demande de Certificat pour un Certificat Cachet.

Le CGUs sont publiées sur un serveur en https. Le formulaire de demande de Certificat est signé par l'AE ce qui protège l'intégrité des CGU. Le PSCo a le contrôle des formulaires contenant les CGUs et utilisées dans la plateforme Docusign. L'AE conserve le formulaire de demande de Certificat signé par le RL, le CT et l'AE qui contient les CGUs. Le formulaire de demande de Certificat distingue clairement les parties liées au RL, l'Entité Légale et le CT et son entité.

6.3.5 Usage de la bi-clé et du certificat

Les exigences requises par l'ETSI sur le contenu de l'agreement au sens de l'ETSI sont décrites au § 6.9.4 car l'agreement est matérialisé par les CGUs. Les informations à destination de l'UC sont contenues dans la présente PC pour ce concerne ; les utilisations des Certificats et clés privées associées, la validation des Certificats, la disponibilité des informations de statut des Certificats, la compréhension des DN des Porteurs, des OIDs et niveaux de sécurité et les obligations techniques que l'UC doit appliquer lorsqu'il vérifie techniquement un Certificat.

Pour les Certificats Signataire, le sole controle est assuré pour le Porteur comme décrit dans [SSAS].

Pour les Certificats Cachet, le contrôle par l'Entité Légale est assuré par les Facteurs d'Activation, la configuration du Certificat dans la plateforme Docusign, la méthode de connexion entre le PSCo et la plateforme Docusign et les moyens de connexion choisit par le CT à la plateforme de Docusign pour utiliser les clés privées pour créer un cachet.

Il appartient aux UC de vérifier l'état de validité d'un certificat à l'aide de l'ensemble des LCR émises et/ou du service OCSP mise en œuvre par l'AC.

L'usage de Certificat révoqué peut entraîner des conséquences désastreuses pour un UC. L'UC est donc responsable de la vérification du statut du Certificat et des moyens et procédures qu'il décide de mettre en place afin de vérifier le statut d'un Certificat pour une opération de validation de signature.

La CRL émise par l'AC QCP-L et QCP-N QCSD contient les certificats expirés et révoqués et contient l'extension « expiredCertsOnCRL ». Les CRL émises par les AC qui émettent des Certificats QCP-N QSCD et QCP-L contiennent l'extension « ExpiredCertsOnCRL » avec la date pour « start date » correspondante à la date et l'heure du plus ancien certificat de AC.

Il est à noter qu'un certificat non expiré avec un statut révoqué donné par le service OCSP peut avoir un statut valide dans la CRL car l'OCSP est sur base de données de l'AC alors que la CRL est émise toutes les 12 heures. Cette différence d'état ne peut durer qu'au maximum 12 heures (la différence n'existe plus avec la prochaine CRL). Cependant un Certificat expiré, non qualifié et révoqué ne sera plus dans la CRL mais aura un statut révoqué donné par l'OCSP.

Le service OCSP est coupé après la fin de vie de l'AC et seule la dernière LCR est la seule information disponible.

Lorsque l'AC est en fin de vie, alors une dernière CRL est émise par l'AC et est publiée avec une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« *99991231235959Z* »). La dernière CRL n'est émise que lorsque tous les Certificats émis par l'AC concernés par la CRL sont soi révoqués ou expirés. Il est à noter que l'AC ne produit pas de dernière réponse OCSP à l'instar d'une dernière CRL.

Les informations de révocation seront toujours disponibles auprès de l'AC qui publie une CRL. En cas de fin de vie de l'AC ou d'arrêt du Service avec cette AC ou y compris en cas de compromission de clé d'AC, une dernière CRL est générée et archivée chez DocuSign France. Cette dernière CRL est publiée sur le site

internet de DocuSign France jusqu'à expiration du TSP et sur l'URL de distribution de la CRL, contenue dans le Certificat, jusqu'à expiration du dernier Certificat émis par l'AC.

6.3.6 Renouvellement d'un certificat

Le renouvellement de Certificat désigne l'émission d'un nouveau Certificat à un Porteur auquel un Certificat a déjà été délivré par le même PSCo, sans modification des clés publiques du Certificat, ni d'aucune autre information contenue dans le certificat (voir IETF RFC 3647), à l'exception du numéro de série du Certificat, mis à jour conformément à l'IETF RFC 5280. Le renouvellement peut avoir lieu pendant la période de validité du Certificat existant ou après sa date d'expiration (c'est-à-dire après la date indiquée dans le champ « notAfter »). Si le renouvellement a lieu pendant la période de validité du Certificat, la date d'expiration peut être mise à jour.

Si l'AC n'inclut pas de LCR dans le Document, alors l'AC utilise un jeton OCSP dans le Document pour le statut du Certificat.

Ce type d'opération n'est pas autorisé au titre de la présente PC pour les certificats Porteurs mais est autorisée pour l'AC. La procédure pour l'AC est identique à celle utilisée pour l'émission du premier certificat.

6.3.7 Délivrance d'un nouveau certificat par suite de changement de la bi-clé

Le renouvellement de Certificat consiste à émettre un nouveau Certificat avec une nouvelle clé publique pour un Porteur auquel un Certificat a déjà été délivré par le même PSCo (voir IETF RFC 3647). Les attributs du DN et les autres attributs certifiés peuvent être mis à jour. Le renouvellement de Certificat peut avoir lieu pendant la période de validité d'un Certificat existant (y compris un renouvellement à la suite d'une révocation ou avant son expiration), ou après la date d'expiration de l'ancien Certificat (c'est-à-dire après la date indiquée dans le champ « notAfter »). Lorsque le renouvellement a lieu pendant la période de validité de l'ancien Certificat, sa date d'expiration peut être mise à jour.

Dans ce cas la procédure à appliquer pour renouveler un certificat d'AC et de Porteur est décrite dans les § 6.2.2 et 6.2.3 pour l'enregistrement et ensuite 6.3.1, 6.3.2, 6.3.3 et 6.3.4.

6.3.8 Modification du certificat

La modification d'un Certificat désigne l'émission d'un nouveau Certificat pour un Porteur auquel un Certificat a déjà été délivré par le même PSCo, à la suite de modifications d'informations autres que la clé publique du Porteur (voir IETF RFC 3647). Cette modification implique la mise à jour des attributs du DN. Le processus de modification peut intervenir pendant la période de validité du Certificat existant ou après sa date d'expiration (c'est-à-dire après la date indiquée dans le champ « notAfter »). La clé reste inchangée. Si la modification intervient pendant la période de validité du Certificat précédent, sa date d'expiration peut être mise à jour.

Ce type d'opération n'est pas autorisé au titre de la présente PC pour les certificats Porteurs mais est autorisée pour l'AC. La procédure est identique à celle utilisée pour l'émission du premier certificat.

6.3.9 Révocation et suspension des certificats

L'AC ne met pas en œuvre de mécanisme de suspension de Certificat.

L'AC ne met pas en œuvre de mécanisme dit de Delta CRL.

L'AC authentifie l'AE qui fait la demande de révocation. L'ensemble des communications est protégé en intégrité et en confidentialité.

L'AC révoque le Certificat du Porteur, immédiatement après avoir authentifié l'AE, en incluant le numéro de série du Certificat dans la prochaine LCR qui sera émise par l'AC et en changeant le statut du Certificat dans sa base de données.

Une fois la révocation effectuée, le Client est le Porteur (Signataire ou RL et CT en fonction du type de Certificat) sont informé par mail par l'AE de la révocation effective du Certificat Porteur.

Une fois que le Certificat est révoqué l'AC ne peut plus changer son statut.

6.3.10 Fonction d'information sur l'état des certificats

Les ACs mettent toutes en œuvre un service OCSP. Le service OCSP est mis à jour à partir de la base de données de l'AC. Le service OCSP est disponible 24 heures par jours, 7 jours par semaine avec un taux de disponibilité de 99,9 %. La base de données de l'AC est protégée par le PSCO et les réponses OCSP et CRL sont signées par l'AC. Il est à noter que l'AC utilise des serveurs OCSP dédiés mais que l'AC elle-même émet des réponses OCSP lors de l'utilisation de la clé privée du Porteur.

Les informations relatives à l'état de révocation sont mises à disposition au-delà de la période de validité du Certificat au moyen d'au moins une des méthodes utilisées pendant la période de validité du Certificat (CRL ou OCSP) tant que l'AC n'est pas expirée.

La réponse OCSP contient les informations internationales suivantes :

Field	**Requirements**
Version	1
Responder ID	OCSP's public key hash
ProducedAT	Date and time of the OCSP response signature
CertID	Subscriber's certificate serialNumber, Sub-CA issuerKeyHash and Sub-CA issuerNameHash
This Update	Date and time of the verification of the Subscriber's certificate status found in the CA database.
Next Update	Date according to status of certificate: Good: 65 minutes Revoked: 21600 minutes (15 jours) Unknown: 15 minutes.
CertStatus	"Good", "Revoked" or "unknown"
Nonce	Used if and only if the user Application provides a value for this field and reused in full.
extensions	No extension referenced pour les AC LCP et NCP+. Extension « ArchiveCutOff » est utilisée uniquement pour les AC certifiées QCP-N QSCD et QCP-L.

6.3.11 Fin de la relation entre le porteur et l'AC

La fin de relation contractuelle entre DocuSign France et le Client est géré dans le contrat établit entre DocuSign France et le Client.

6.3.12 Séquestre de clé et recouvrement

Les bi-clés des Porteurs et d'AC émis conformément à la PC ne font pas l'objet de séquestre ni de recouvrement.

6.4 Mesures de sécurité physique et procédurales

6.4.1 Mesures de sécurité générales

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 du PSCo, 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.

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.

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 Certification et PSSI

Le PSCo définit la PC 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 PSCo.

L'entité en charge de l'administration et de la gestion de la PC 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 PC 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 PC.

Toute évolution de la PC 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 PC susceptible de produire un effet majeur sur lesdits Clients.

DocuSign FRANCE peut modifier la présente PC 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 PC, 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 PC 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 PC :

- 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 « Définitions ».

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 PC 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 des services du PSCo. La présente PC contient également l'information publique du « Practice Statement », mais le document s'appelle PC.

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 PSCo

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 PC qui mentionnent les sous-traitants.

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 Accès physique

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 du PSCo peuvent être prises en charge dans la même zone sécurisée, à condition que l'accès soit limité au personnel autorisé.

Les équipements du PSCO (gestion de l'AE, génération de bi-clé, génération de Certificat, gestion des révocation et gestion des réponses OCSP) sont protégés contre les accès non autorisés aux données et système et les tentatives d'endommagement. La protection physique permet d'assurer à minima les points suivants :

- La surveillance vidéo des accès aux locaux de l'OSC est assuré 24 heures par jour et 7 jours par semaine ;
- Aucun accès non autorisé n'est possible sur les équipements et les données d'activation ;
- Les supports d'informations papiers et informatiques qui contiennent des informations sensibles en clairs sont stockés dans des endroits sûrs ;
- Les locaux de l'OSC en production qui héberge les composants techniques du PSCo ne sont pas partagés ;
- Les personnes non autorisées sont toujours accompagnées par des personnes autorisées dans les locaux ;
- Un journal des accès entrant et sortant pour les locaux de l'OSC est maintenu et est périodiquement revu de manière indépendante ;
- Au moins deux niveaux de barrières successifs de sécurité sont mis en œuvre pour les accès aux pièces opérationnelles qui contiennent les équipements et les données d'activation ;
- L'accès aux équipements des QSCD (AC, OCSP et Porteur), et leurs données d'activation, requière deux personnes physiques distinctes du PSCo ;
- Tous les équipements, supports, logiciels et données sensibles sont protégées contre le vol et l'accès non autorisé ;
- Les locaux de l'OSC ne permettent de mettre en œuvre que les services du PSCo qu'ils soient qualifiés ou non avec les mêmes procédures et personnels autorisés.

Les locaux d'hébergement de l'ACR et ACI sont totalement distinct des locaux utilisés pour la production et mis en œuvre des services en ligne du PSCo. Les ACR et ACI sont hébergés dans des locaux hors ligne isolés, sous surveillance vidéo et uniquement accessibles par des personnes autorisées et approuvées par la PMA.

Une vérification de sécurité des locaux est effectuée si les locaux ont été laissés sans surveillance. Au minimum, le contrôle est de vérifier ce qui suit :

- L'équipement est dans un état approprié pour le mode de fonctionnement courant ;
- Pour les composants hors ligne, tous les équipements sont arrêtés ;
- Les conteneurs de sécurité (enveloppes inviolables, un coffre-fort, etc) sont correctement fermés ;
- Les systèmes de sécurité physiques (par exemple, des serrures de porte, radars, caméras, etc) fonctionnent correctement ;
- Les locaux sont protégés contre les accès non autorisés.

Les QSCD doivent être désactivés avant leur stockage.

L'OSC dispose de plusieurs arrivé internet.

Lorsqu'ils ne sont pas utilisés, les QSCD et les données d'activation associées sont placés dans des conteneurs sécurisés (coffre, local sécurisé, etc).

Les données d'activation sont soit mémorisées ou enregistrées et stockées d'une manière appropriée à la sécurité du QSCD, et ne doivent pas être stockés avec le QSCD.

Des systèmes de protection de l'alimentation électrique et de génération d'air conditionné sont mis en œuvre par l'OSC afin d'assurer la continuité des services délivrés.

Les accès internet utilisés par les services sont redondés.

Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et ou constructeurs.

Les systèmes de l'OSC sont implantés de telle manière qu'ils ne sont pas sensibles aux inondations et autres projections et écoulements de liquides et sont suffisamment robuste en termes de structure.

Les moyens de prévention et de lutte contre les incendies mis en œuvre par l'OSC permettent de respecter les exigences et les engagements pris par le PSCo dans la présente PC, en matière de disponibilité de ses services.

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.

Le PSCo s'assure que les autorisations d'accès sont modifiées en conséquence lors de la cessation d'emploi ou d'un changement de fonction.

L’accès aux informations et aux fonctions du système d’application est restreint conformément à la politique de contrôle d’accès.

Le système du PSCo fournit des contrôles de sécurité informatique suffisants pour la séparation des rôles de confiance identifiés dans les pratiques du PSCo, y compris la séparation des fonctions d’administration et d’exploitation de la sécurité. En particulier, l’utilisation des utilitaires système est restreinte et contrôlé.

Le personnel du PSCo est identifié et authentifié avant d’utiliser les applications critiques liées au service.

Le personnel du PSCo est responsable de ses activités.

L'émission de certificats par l’ACR et l’ACI est soumise à un double contrôle au moins, exercé par du personnel autorisé et de confiance. Ainsi, une seule personne ne peut signer de certificats d’AC et CRL.

6.4.4 Mesures de sécurité vis-à-vis du personnel

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 PSCo. Le personnel susceptible de participer à la supervision des services du PSCo n'a pas besoin d'être employé du PSCo.

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 [319 411-1] et [319 411-2].

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 exerçant 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 Procédures de constitution des données 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 PSCo.

Le PSCo collecte et stocke les informations suivantes :

- Les traces d'audit techniques liés à la gestion de l'enregistrement, de la gestion des bi-clés et des Certificats (§ 6.2.2, § 6.2.3, § 6.2.4, § 6.3.4, § 6.3.6, § 6.3.7 et § 6.3.8 ;

- Les traces techniques de gestion des CRL et OCSP (Cf. § 6.3.9 et 6.3.10) ;
- Les demandes de Certificats et informations collectées et vérifiées par l'AE et les CGUs comme définies au § 6.3.1 et § 6.3.2 ;
- L'ensemble des Certificats et CRL émis par les AC ;
- Les procédures de validation applicables ainsi que les PC et ensemble du référentiel de sécurité ;
- Les scripts de cérémonies des clés pour les ACR, ACI et AC (génération de bi-clés, génération de certificat et révocation de certificat et gestion des données d'activation des bi-clés) et leurs traces d'audit associées ;
- Les traces de la gestion et configuration des QSCD (AC, OCSP et Porteur) ;
- Les traces de la gestion et de la personnalisation des parts de secret et des données d'activation des QSCD ;
- Les logs techniques de l'infrastructure du PSCo.

Les traces d'audit mentionnées ci-dessus ne sont accessible que par les personnes autorisées du PSCo et selon le principe du besoin d'en connaître.

La DPC donne les dates exactes de conservation des données ci-dessus.

En cas de fin de vie d'une AC, le PSCo continue de conserver les données listées ci-dessus.

6.4.6 Archivage des données

Le PSCo archive les traces d'audit comme définit au § 6.4.5 selon des durées données dans la DPC.

Toutes les traces d'audit liées à la gestion des Certificats et des bi-clés des Porteurs et des AC sont conservées à minima 7 ans après l'expiration du certificat associé.

6.4.7 Changement de clé

La durée de vie d'un certificat d'AC est déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationale ou internationale compétentes en la matière.

Une AC ne peut pas générer de certificats dont la durée de vie dépasse la période de validité de son certificat d'AC. C'est pourquoi, l'AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie la plus longue parmi les Certificats émis. Une nouvelle AC requiert un nouveau certificat d'AC, une nouvelle bi-clé et un nouveau DN d'AC. C'est donc un renouvellement complet d'AC qui est effectué.

Dès qu'une nouvelle AC est générée et auditée et autorisée par la PMA à être utilisée en production, seule celle-ci est utilisée pour générer de nouveaux Certificats de Porteurs.

La précédente AC reste valable pour valider le chemin de certification des anciens certificats émis par la précédente AC et pour l'émission de CRL et de réponse OCSP, jusqu'à l'expiration de tous les Certificats Porteurs émis à l'aide de cette précédente AC. Le Certificat Porteur à une durée de vie fixe qui ne peut pas être changée à cause de la fin de vie de l'AC. Dès que tous les Certificats émis par la précédente AC sont tous expirés alors l'AC entre en fin de vie et une dernière CRL est émise et tous les copies de clés privées de l'AC sont détruites.

Par ailleurs, la PMA se charge de changer l'AC et le certificat correspondant quand la bi-clé cesse d'être conforme aux recommandations de sécurité cryptographique concernant la taille des clés ou si celle-ci est soupçonnée de compromission ou compromise.

La durée de vie des Certificat Porteur est déterminée en cohérence avec les recommandations de sécurité en matière de cryptographie.

6.4.8 Reprise à la suite de compromission et sinistre

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 sou s 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 maintien 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 PSCo 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.

Les données des systèmes du PSCo nécessaires à la reprise des opérations de l'AC sont sauvegardées et stockées dans des lieux sûrs, de préférence distants, permettant au PSCo de reprendre rapidement ses activités en cas d'incident ou de sinistre.

Des copies de sauvegarde des informations et logiciels essentiels sont effectuées régulièrement hors site.

Des moyens de sauvegarde adéquats sont en place pour garantir la récupération de toutes les informations et logiciels essentiels à la suite d'un sinistre ou d'une panne de support.

Les dispositifs de sauvegarde sont testés régulièrement afin de garantir leur conformité aux exigences des plans de continuité d'activité.

Les fonctions de sauvegarde et de restauration sont assurées par les rôles de confiance concernés, spécifiés à l'article 6.4.4.

Si l'analyse des risques identifie des informations nécessitant un double contrôle pour la gestion, par exemple les clés, alors un double contrôle est appliqué à la récupération.

Compromission de la clé d'une AC :

Le plan de continuité d'activité (ou plan de reprise après sinistre) du PSCo traite la compromission, la perte ou la suspicion de compromission de la clé privée d'une AC comme un sinistre.

Les procédures prévues conformément au plan de continuité sont mises en œuvre. Le plan contient l'exigence de révocation des certificats impactés et concernés en les révoquant ainsi que la révoquant de l'AC émettrice.

A la suite à un sinistre, le PSCo doit, dans la mesure du possible, prendre des mesures pour éviter qu'il ne se reproduise.

En cas de compromission (minimum) :

- Le PSCo doit informer de la compromission : tous les abonnés et autres entités avec lesquels le FST a conclu des accords ou entretenu d'autres relations, notamment les parties de confiance et les autres FST.
- Le PSCo met les informations de CRL à la disposition des UC.
- Le PSCo indique que les certificats et les informations relatives à leur révocation, émis à l'aide de cette clé d'autorité de certification (AC), peuvent ne plus être valides.
- Le PSCo révoque le certificat d'AC qu'il a émis lorsqu'il est informé de la compromission d'une telle AC.

Compromission d'algorithme :

- Si l'un des algorithmes ou paramètres associés utilisés par le PSCo ou son Porteur devient inadéquat pour l'usage prévu restant, le PSCo en informera tous les Clients avec lesquelles il a conclu un accord ou entretenu d'autres relations et les UCs.
- Si l'un des algorithmes ou paramètres associés utilisés par le PSCo ou ses Porteurs s'avère insuffisant pour l'usage prévu restant, le PSCo procédera à la révocation de tout Certificat concerné.

6.4.9 Fin de vie de l'AC ou de l'AE

Les perturbations potentielles pour les Porteurs et les UCs sont minimisées à la suite de la cessation des services du PSCo, et notamment la maintenance continue des informations nécessaires à la vérification de la fiabilité des services de confiance est assurée.

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

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

- Le PSCo 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 PSCo, notamment les UCs 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 utilisée dans le service arrêté.
- Avant que le PSCo n'arrête le service, 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. Ces informations concernent ; les traces d'enregistrement (§ 6.2.2, § 6.3.1 et § 6.3.4), les CRL, les Certificats et leur statut (§ 6.3.10) et les traces d'audit (§ 6.4.5 et § 6.4.6). Cela inclut les statuts des Certificats non expirés.
- Les clés privées des Signataires et/ou des composantes du PSCo affectées par la cessation sont détruites et mises hors service de manière 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 Certificats aux parties utilisatrices pendant une période raisonnable.

6.5 Mesures DE SECURITE techniques

6.5.1 Génération et installation de bi-clés

Le PSCo définit des procédures pour la gestion de toutes les clés et des algorithmes que le PSCo utilise.

Le PSCo génère les clés de l'ACR, ACI et AC, y compris celles utilisées par les services de révocation et d'enregistrement, de manière sécurisée afin que la clé privée reste secrète.

En particulier :

- La génération de la bi-clés de l'AC et la certification ultérieure de la clé publique sont effectuées dans un environnement physiquement sécurisé (voir la clause 6.4.2) par du personnel occupant des fonctions de confiance (voir la clause 6.4.4).
- La bi-clé de l'AC utilisée pour la signature des certificats est créée sous un double contrôle au minimum.
- Le nombre de personnes autorisées à effectuer la génération de la bi-clé de l'AC est réduit au minimum et est autorisé par la PMA.
- La génération de la bi-clé de l'AC est effectuée à l'aide d'un algorithme conforme [CRYPTO] pour les besoins de signature de l'AC.
- La longueur de clé et l'algorithme sélectionnés pour la clé de signature de l'AC sont conformes aux spécifications de [CRYPTO] pour les besoins de signature de l'AC.

Avant l'expiration de son certificat d'AC utilisé pour la signature des Certificat, le PSCo applique les règles du § 6.4.7et si le service se poursuit, la nouvelle AC est également générée et diffusée conformément au présent document.

Les opérations décrites ci-avant sont effectuées avec un intervalle approprié entre la date d'expiration du certificat et le dernier Certificat signé, afin de permettre à toutes les parties ayant des relations avec le PSCo (Client, Porteur, UCs, …) d'être informées de ce changement de clé et de mettre en œuvre les opérations requises pour éviter tout désagrément ou dysfonctionnement. Ceci ne s'applique pas au PSCo si le PSCo cessera ses activités avant la date d'expiration de son propre certificat de signature.

Le PSCo disposer d'une procédure documentée pour la génération de bi-clés d'AC, d'ACR et d'ACI. Cette procédure indique à minima :

- a) les rôles participant à la cérémonie (internes et externes à l'organisation) ;
- b) les fonctions à remplir par chaque rôle et les différentes phases de cette tâche ;
- c) les responsabilités pendant et après la cérémonie ; et
- d) les éléments de preuve à recueillir concernant la cérémonie.

Le PSCo produit un rapport de cérémonie, composer de plusieurs documents, attestant que la cérémonie, telle que décrite ci-dessus, a été réalisée conformément à la procédure établie et que l'intégrité et la confidentialité de la paire de clés ont été garanties.

Le rapport de la cérémonie de génération de clés doit inclure au moins les informations suivantes :

a) Les rôles des participants à la cérémonie (internes et externes à l'organisation) ;

b) Les fonctions exercées par chaque rôle et les phases dans lesquelles elles ont été exercées ;

c) Les responsabilités pendant et après la cérémonie ;

d) Les preuves recueillies lors de la cérémonie ;

e) La date de la cérémonie ;

f) Un inventaire des clés générées, comprenant au moins les informations suivantes pour chaque clé :

   a. Un identifiant unique ;

   b. L'algorithme, la taille de la clé et l'empreinte de la clé publique (SHA256 minimum) ;

g) L'identifiant unique et le modèle du dispositif cryptographique sécurisé (par exemple, un module de sécurité matériel) utilisé pour cette génération cérémonie.

h) L’algorithme de génération de clés et les paramètres configurés dans le dispositif cryptographique sécurisé lors de la cérémonie de génération de clés, par exemple, le mode de fonctionnement, le générateur de nombres aléatoires utilisé et les autres paramètres cryptographiques.

Si le PSCo prévoit de conserver des clés pré-générées pour une utilisation ultérieure, celles-ci sont clairement identifiées comme telles dans l’inventaire.

Si le PSCo conserve des clés pré-générées pour une utilisation ultérieure, il s'assure que :

- La bi-clé pré-générée par l'algorithme et les paramètres de génération de clés initialement utilisés (par exemple, un générateur de nombres aléatoires) et le dispositif initialement utilisé pour la génération de clés (par exemple, un module de sécurité matériel) sont toujours considérés comme adaptés à l'usage prévu au moment de la mise en service de la bi-clé ; et
- La bi-clé pré-générée est toujours considérée comme cryptographiquement sûre pour l'usage prévu au moment de son installation (c'est-à-dire sa certification par l'ACR ou l’ACI). Pour ce faire, il convient de comparer l'algorithme et la longueur de la clé les informations enregistrées pour la clé à utiliser lors de la cérémonie de génération de clés correspondante aux recommandations actuelles spécifiées dans [CRYPTO] pour l'usage prévu de la clé.

Si la bi-clé n'est plus jugée adaptée à l'usage prévu, elle n’est pas utilisée et elle est détruite.

Ce rapport est signé comme suit :

- Pour l’ACR et l’ACI : par la personne de confiance responsable de la sécurité de la cérémonie de gestion des clés du PSCo (par exemple, le responsable de la sécurité) et par une personne de confiance indépendante de la direction du prestataire (un notaire ou un auditeur accrédité eIDAS) comme témoin que le rapport de cérémonie reflète fidèlement le déroulée de la cérémonie de gestion des clés.
- Pour les AC : par la personne de confiance responsable de la sécurité de la cérémonie de gestion des clés du prestataire (par exemple, le responsable de la sécurité) comme témoin que le rapport de cérémonie reflète fidèlement le déroulée de la cérémonie de gestion des clés.

Les AC QCP-N QSCD et QCP-L sont contenues dans la TL de l’ANSSI et les AC LCP et NCP+ sont signées par une ACI contenue dans le magasin d’Adobe. De plus les ACR, ACI et AC sont publiées en production et via le SP.

Pour tous les types de Certificat Porteurs, c'est le PSCo qui génère les bi-clés des Porteurs. Ces bi-clés sont générées à l'aide d'un algorithme reconnu comme adapté aux usages identifiés dans la présente PC pendant la période de validité du Certificat. Les bi-clés sont d'une longueur de clé et compatibles avec un algorithme de clé publique conforme à [CRYPTO].

Le PSCo génère, gère et stocke les bi-clés des Porteurs de manière sécurisé.

Lorsque les bi-clés des Porteurs ne sont plus utiles, alors le PSCo supprime les bi-clés et toutes les copies de la clé privée du Porteur. Les bi-clés des Certificats Signature sont détruits immédiatement après leur utilisation comme décrit dans [SSAS] et les bi-clés des Certificats Cachet sont détruit dès que le Certificat est expiré, révoqués ou que la clé privée ne peut plus être utilisée.

Le PSCo sécurise la gestion, le stockage, l'usage et la configuration, et les données d'activation et parts de secret associés, des [QSCD] dans lesquels les bi-clés des Porteurs sont générées et utilisées.

Les bi-clés du Porteur, de l'AC et de l'OCSP générées et utilisées par le PSCo sont importées et exportées dans le [QSCD] en appliquant des mesures de sécurités en conformité avec les hypothèses environnementales et les objectifs de sécurité du [QSCD] qui permettent de s'assurer que seul l'AC, l'OCSP et Porteur utilisent leur bi-clés respectifs et qu'une autre composante ou personne non autorisée ne puisse pas utiliser la bi-clé. Ces mesures sont déterminées en fonction des vulnérabilités et menaces identifiées dans l'analyse de risque et leur robustesse testée par un auditeur technique externe lors de test d'intrusion.

Le PSCo décrit dans sa DPC les mesures qui sont prises en cas de modification du statut d'un [QSCD] qui arriverait avant la fin de validité d'un Certificat.

6.5.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

Le PSCo génère et gère et utilise les bi-clés des AC, des OCSP et des Porteurs dans des [QSCD] qui sont notifié comme QSCD sur le site de l'EU.

Les [QSCD] sont exploités conformément à la configuration décrite dans la documentation de certification appropriée ou selon une configuration équivalente permettant d'atteindre le même objectif de sécurité.

Les [QSCD] utilisés pour l'AC, l'OCSP et les Porteurs sont EAL 4+ certifié conforme au PP 419 214-2 et 419 221-5.

En production, les clés privées de l'AC, des OCSP et Porteurs sont temporairement conservées et utilisée au sein du [QSCD].

Lorsque les clés privées de l'AC, OCSP et Porteur se trouvent hors du [QSCD], la clé privée est protégée de manière à garantir un niveau de protection équivalent à celui offert par le [QSCD] conformément aux possibilités proposées par le [QSCD].

La clé privée de l'AC et des OCSP sont sauvegardées, stockées et récupérées uniquement par le personnel de confiance du PSCo, utilisant au minimum un double contrôle dans un environnement physiquement sécurisé (voir la clause 6.4.2).

Le nombre de personnes autorisées à effectuer la sauvegarde, le stockage et la récupération de la clé privée de l'AC et de l'OCSP est réduit au minimum et conforme aux pratiques du PSCo.

Les copies de la clé privée de l'AC sont soumises à un niveau de contrôle de sécurité au moins égal à celui des clés actuellement utilisées.

Lorsque la clé privée de l'AC et ses copies sont stockées dans un [QSCD] dédié, des contrôles d'accès doivent être mis en place afin de garantir que les clés ne soient pas accessibles en dehors de ce [QSCD].

Le [QSCD] ne doit pas être altéré pendant le transport.

Le [QSCD] ne doit pas être altéré pendant son stockage.

Le [QSCD] doit fonctionner correctement.

La clé privée de l'AC stockée [QSCD] doivent être détruites dans le [QSCD] lors de la mise hors service du [QSCD].

6.5.3 Autres aspects de la gestion des bi-clés

Le PSCo utilise la clé privée de l'AC de manière appropriée et en particulier :

- Le PSCo n'utilise pas la clé privée de l'AC au-delà de l'expiration du Certificat d'AC.
- La clé privée de l'AC utilisée pour générer les Certificats, tels que définis à la clause 6.3.3, et/ou pour émettre des informations sur l'état de révocation, ne sont pas utilisées à aucune autre fin.
- Les clés de signature des certificats sont utilisées uniquement dans des locaux physiquement sécurisés.
- L'utilisation de la clé privée de l'AC est compatible avec l'algorithme de hachage, l'algorithme de signature et la longueur de la clé de signature utilisés pour générer les Certificats, conformément aux pratiques actuelles et à l'exigence [CRYPTO].
- Toutes les copies des clés privées de l'AC sont détruites à la fin de leur cycle de vie.

6.5.4 Données d'activation

L'installation et la récupération des bi-clés de l'AC dans un [QSCD] nécessite le contrôle simultané d'au moins deux employés de confiance.

Les données d'activation du Porteur pour les Certificats Signature sont gérées conformément à [SSAS].

Il est de la responsabilité du CT de définir et configurer les données d'activation associé à sa clé privée pour les Certificats Cachet.

6.5.5 Mesures de sécurité des systèmes informatiques

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.

Les composants du réseau local (par exemple, les routeurs) doivent être conservés dans un environnement physiquement et logiquement sécurisé.

La configuration des composants du réseau local (par exemple, les routeurs) est vérifiée périodiquement afin de garantir sa conformité aux exigences spécifiées par le PSCo.

Le PSCo impose l'authentification multi facteur pour tous les comptes susceptibles de déclencher directement l'émission de certificats.

Le SP en production impose un contrôle d'accès aux tentatives d'ajout ou de suppression de certificats et de modification d'autres informations associées.

L'application de gestion du statut de révocation doit appliquer un contrôle d'accès aux tentatives de modification des informations relatives au statut de révocation.

Des dispositifs de surveillance continue et d'alarme doivent être mis en place pour permettre au fournisseur de services de télécommunications de détecter, d'enregistrer et de réagir en temps opportun à toute tentative d'accès non autorisée et/ou irrégulière à ses ressources.

6.5.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.5.6.1 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.

6.5.6.2 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.

6.5.6.3 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.

6.5.6.4 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.

Les besoins en capacité doivent être surveillés et des projections des besoins futurs en capacité sont établies afin de garantir la disponibilité d'une puissance de traitement et d'un stockage adéquat.

6.5.7 Mesures de sécurité 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 PSCo 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.

Le PSCo maintenir et protéger tous les systèmes de l'AC dans une zone sécurisée et mettre en œuvre une procédure de sécurité protégeant les systèmes et les communications entre les systèmes situés dans les zones sécurisées et les zones de haute sécurité.

Le PSCo configure tous les systèmes du PSCo en supprimant ou en désactivant tous les comptes, applications, services, protocoles et ports non utilisés pour le fonctionnement de l'AC.

Le PSCo limite l'accès aux zones sécurisées et aux zones de haute sécurité aux seuls rôles de confiance.

L'ACR et l'ACI ne sont mis en œuvre que dans des systèmes dit hors ligne (aucune connexion à internet ou un quelconque réseau) et dans un local totalement séparé de la production dite en ligne et dans une zone sécurisée.

6.5.8 Horodatage / Système de datation

Tous les composants du PSCo sont régulièrement synchronisés avec une source NTP.

Le temps fourni par ce serveur de temps doit être utilisé pour établir l'heure :

- Du début de validité d'un Certificat.
- De la révocation d'un Certificat et des réponses OCSP.

Des procédures automatiques ou manuelles peuvent être utilisées pour maintenir l'heure du système.

Les réglages de l'horloge sont des événements susceptibles d'être audités.

6.6 Profils des Certificats, OCSP ET DES LCR

6.6.1 Profil de Certificats

Les certificats émis par l'AC sont des Certificats au format ISO/IEC 9594-8/Recommendation ITU-T X.509 ou IETF RFC 5280.

Les numéros de série de tous les certificats font 20 octets et sont aléatoires.

6.6.1.1 AC « Docusign Qualified CA G1 »

Base Certificate Fields	**Value**		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = OpenTrust OU = 0002 478217318 CN = OpenTrust CA for AATL G1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	2038/01/01 00:00:00 Z		
Subject	**Attribute type**	**Attribute value**	**Directory String**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	organizationIdentifier	NTRFR-812611150	UTF8String
	CN	Docusign Qualified CA G1	UTF8String
Subject Public Key Info	Key size	4096 bits	

Base Certificate Fields	Value	
	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)
Signature (algorithm & OID)	Sha384WithRSAEncryption (1.2.840.113549.1.1.12)	

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Issuer key hash
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Method 1
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
Certificate Policies	**FALSE**	
policyIdentifier		anyPolicy (2.5.29.32.0)
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.1
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
CRL Distribution Points	**False**	
distributionPoint		URL=http://get-crl.certificat.com/public/opentrustcaforaatlg1.crl
Authority Information Access	**FALSE**	
Ocsp		http://get-ocsp.certificat.com/opentrustcaforaatlg1

6.6.1.2 AC « Docusign Advanced Seal CA G1 »

Base Certificate Fields	Value
Version	2 (=version 3)
Serial number	Defined by the software
Issuer	C = FR O = OpenTrust OU = 0002 478217318 CN = OpenTrust CA for AATL G1
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)
NotAfter	2038/01/01 00:00:00 Z

Base Certificate Fields	Value		
Subject	**Attribute type**	**Attribute value**	**Directory String**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	organizationIdentifier	NTRFR-812611150	UTF8String
	CN	Docusign Advanced Seal CA G1	UTF8String
Subject Public Key Info	Key size	4096 bits	
	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
Signature (algorithm & OID)	Sha384WithRSAEncryption (1.2.840.113549.1.1.12)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Issuer key hash
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Method 1
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
Certificate Policies	**FALSE**	
policyIdentifier		anyPolicy (2.5.29.32.0)
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.1
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
CRL Distribution Points	**False**	
distributionPoint		URL=http://get-crl.certificat.com/public/opentr ustcaforaatlg1.crl
Authority Information Access	**FALSE**	
Ocsp		http://get-ocsp.certificat.com/opentrustcaforaatlg1

6.6.1.3 AC « Docusign Qualified Seal CA G1 »

Base Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = OpenTrust OU = 0002 478217318 CN = OpenTrust CA for AATL G1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	2038/01/01 00:00:00 Z		
Subject	**Attribute type**	**Attribute value**	**Directory String**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	organizationIdentifier	NTRFR-812611150	UTF8String
	CN	Docusign Qualified Seal CA G1	UTF8String
Subject Public Key Info	Key size	4096 bits	
	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
Signature (algorithm & OID)	Sha384WithRSAEncryption (1.2.840.113549.1.1.12)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Issuer key hash
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Method 1
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
Certificate Policies	**FALSE**	
policyIdentifier		anyPolicy (2.5.29.32.0)
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.1
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
CRL Distribution Points	**False**	

Extensions	Criticality (True/False)	Value
distributionPoint		URL=http://get-crl.certificat.com/public/opentrustcaforaatlg1.crl
Authority Information Access	**FALSE**	
Ocsp		http://get-ocsp.certificat.com/opentrustcaforaatlg1

6.6.1.4 AC « Docusign Qualified TimeStamp CA G1 »

Base Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = OpenTrust OU = 0002 478217318 CN = OpenTrust CA for AATL G1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	2038/01/01 00:00:00 Z		
Subject	**Attribute type**	**Attribute value**	**Directory String**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	organizationIdentifier	NTRFR-812611150	UTF8String
	CN	Docusign Qualified TimeStamp CA G1	UTF8String
Subject Public Key Info	Key size	4096 bits	
	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
Signature (algorithm & OID)	Sha384WithRSAEncryption (1.2.840.113549.1.1.12)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Issuer key hash
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Method 1
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Basic Constraint	**TRUE**	
cA		True

Extensions	Criticality (True/False)	Value
pathLenConstraint		0
Certificate Policies	**FALSE**	
policyIdentifier		anyPolicy (2.5.29.32.0)
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.1
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
CRL Distribution Points	**FALSE**	
distributionPoint		URL=http://get-crl.certificat.com/public/opentrustcaforaatlg1.crl
Authority Information Access	**FALSE**	
Ocsp		http://get-ocsp.certificat.com/opentrustcaforaatlg1

6.6.1.5 Certificat Signature : QCP-N QSCD : 1.3.6.1.4.1.22234.2.14.3.60

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Qualified CA G1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date minus 1 hour)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 10 days		
Subject	**Attribute type**	**Attribute value**	**Directory String[1]**
	C	Country code of the country who issued the verified ID document	PrintableString
	OU	RA DocuSign France	UTF8String
	OU	<Envelope ID number>	UTF8String
	OU	TR <context identifier as viewed by SSAS>	UTF8String
	serialNumber	random value of 20 bytes of entropy generated by CSE	PrintableString
	givenName	First name(s) of the signatory as contained in JSON from PVID	UTF8String
	surName	Last name(s) of the signatory as contained in JSON from PVID	UTF8String
	CN	First name(s) and last name(s) of the Signatory	UTF8String

[1] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Basic Certificate Fields	Value	
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)
	Key size	3072 bits minimum
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)	

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Non Repudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.60
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
CRL Distribution Points	**FALSE**	
distributionPoint		http://certs.tsp2.dsf.docusign.net/crl/docusignqualifiedcag1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.tsp2.dsf.docusign.net/ocsp
caIssuers		http://certs.tsp2.dsf.docusign.net/cer/docusignqualifiedcag1.p7c
Qualified Certificate Statements	**FALSE**	
esi4-qcStatement-1		*No value (QcCompliance)*
esi4-qcStatement-4		*No value (SSCD)*
esi4-qcStatement-6		QcType=id-etsi-qct-esign
esi4-qcStatement-5		en: https://certs.tsp2.dsf.docusign.net/pds/docusignqualifiedcag1.pdf

6.6.1.6 Certificat Cachet : NCP + : 1.3.6.1.4.1.22234.2.14.3.61

Basic Certificate Fields	**Value**		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Qualified TimeStamp CA G1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z (certificate issuance date + 6 years)		
Subject	**Attribute type**	**Attribute value**	**Directory String[2]**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	organizationIdentifier	NTRFR-812611150	UTF8String
	CN	Qualified TimeStamping <date of certificate request>	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	3072 bits minimum	
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	

[2] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality (True/False)	Value
Digital Signature		Set
nonRepudiation		Set
Extended Key Usage	**TRUE**	
timeStamping		Set
Private Key Usage Period	**FALSE**	
notBefore		Certificate issuance date
notAfter		Certificate issuance date + 1 year
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.61
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
CRL Distribution Points	**FALSE**	
distributionPoint		http://certs.tsp2.dsf.docusign.net/crl/docusignqualifiedtimestampcag1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.tsp2.dsf.docusign.net/ocsp
calssuers		http://certs.tsp2.dsf.docusign.net/cer/docusignqualifiedtimestampcag1.p7c
QCStatements	**FALSE**	
qcStatement-2		semanticsIdentifier=id-etsi-qcs-SemanticsId-Legal
esi4-qcStatement-4		*No value (SSCD)*

6.6.1.7 Certificat Cachet : LCP : 1.3.6.1.4.1.22234.2.14.3.63

Basic Certificate Fields	Value
Version	2 (=version 3)
Serial number	Defined by the software
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Advanced Seal CA G1
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum

Basic Certificate Fields	**Value**		
Subject	**Attribute type**	**Attribute value**	**Directory String[3]**
	C	Code pays ISO 3166-1 sur 2 caractères. Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale) est officiellement enregistré (tribunal de commerce, ministère, …). Il est en majuscule.	PrintableString
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	organizationIdentifier	Au choix : • TVA intracommunautaire : « VATEU-XXNNNNNNN » avec XX = code pays EU et NNNN numéro local. • TVA d'un autre pays : « VATxx-NNNNNNN » avec xx = code pays et NNNNNNN = numéro de TVA. • Numéro d'enregistrement national (type SIREN) : NTRxx-NNNNNNN avec xx = code pays et NNNNNNN = numéro d'enregistrement de l'entreprise • Entités Légales qui ne peuvent pas utiliser les deux solutions ci-dessus alors LEI est utilisé « LEIXG-NNNNNNN » avec NNNNNNN = code LEI de l'entité.	UTF8String
	CN	Nom du service applicatif	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	3072 bits minimum	
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
nonRepudiation		Set
Extended Key Usage	**FALSE**	

[3] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality (True/False)	Value
1.2.840.113583.1.1.5 (Adobe Certified Document Signing)		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.63
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
CRL Distribution Points	**FALSE**	
distributionPoint		http://certs.tsp2.dsf.docusign.net/crl/docusignadvancedsealcag1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.tsp2.dsf.docusign.net/ocsp
caIssuers		http://certs.tsp2.dsf.docusign.net/cer/docusignadvancedsealcag1.p7c
QCStatements	**FALSE**	
qcStatement-2		semanticsIdentifier=id-etsi-qcs-SemanticsId-Legal

6.6.1.8 Certificat Cachet : QCP-L : 1.3.6.1.4.1.22234.2.14.3.64

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Qualified Seal CA G1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 3 years maximum		
Subject	**Attribute type**	**Attribute value**	**Directory String[4]**
	C	Code pays ISO 3166-1 sur 2 caractères. Pays de l'autorité compétente auprès de laquelle le Client (Entité Légale) est officiellement enregistré (tribunal de commerce, ministère, …). Il est en majuscule.	PrintableString

[4] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Basic Certificate Fields	Value		
	O	Nom officiel complet du Client tel qu'enregistré auprès des autorités compétentes (tribunal de commerce, ministère, …)	UTF8String
	organizationIdentifier	Au choix : • TVA intracommunautaire : « VATEU-XXNNNNNNN » avec XX = code pays EU et NNNN numéro local. • TVA d'un autre pays : « VATxx-NNNNNNN » avec xx = code pays et NNNNNNN = numéro de TVA. • Numéro d'enregistrement national (type SIREN) : NTRxx-NNNNNNN avec xx = code pays et NNNNNNN = numéro d'enregistrement de l'entreprise • Entités Légales qui ne peuvent pas utiliser les deux solutions ci-dessus alors LEI est utilisé « LEIXG-NNNNNNN » avec NNNNNNN = code LEI de l'entité.	UTF8String
	CN	Nom du service applicatif	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	3072 bits minimum	
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
nonRepudiation		Set
Extended Key Usage	**FALSE**	
1.2.840.113583.1.1.5 (Adobe Certified Document Signing)		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.64
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	

Extensions	Criticality (True/False)	Value
cA		False
CRL Distribution Points	**FALSE**	
distributionPoint		http://certs.tsp2.dsf.docusign.net/crl/docusignqualifiedsealcag1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.tsp2.dsf.docusign.net/ocsp
caIssuers		http://certs.tsp2.dsf.docusign.net/cer/docusignqualifiedsealcag1.p7c
Qualified Certificate Statements	**FALSE**	
esi4-qcStatement-1		*No value (QcCompliance)*
qcStatement-2		semanticsIdentifier=id-etsi-qcs-SemanticsId-Legal
esi4-qcStatement-6		QcType=id-etsi-qct-eseal
esi4-qcStatement-5		en: https://certs.tsp2.dsf.docusign.net/pds/docusignqualifiedsealcag1.pdf

6.6.2 Profil de LCR

6.6.2.1 AC « Docusign Qualified CA G1 »

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Qualified CA G1
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z = thisUpdate + 6 days
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)

CRL Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
CRL Number	**FALSE**	
crlNumber		Monotonically increasing sequence number
Expired Certs On CRL	**FALSE**	
expiredCertsOnCRL		YYYY/MM/DD hh:mm:ss Z (CA certificate validity start)

CRL Entry Extensions	Criticality (True/False)	Value
No CRL entry extension allowed	**N/A**	N/A

6.6.2.2 AC « Docusign Advanced Seal CA G1 »

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Advanced Seal CA G1
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z = thisUpdate + 6 days
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)

CRL Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
CRL Number	**FALSE**	
crlNumber		Monotonically increasing sequence number

CRL Entry Extensions	Criticality (True/False)	Value
No CRL entry extension allowed	**N/A**	N/A

6.6.2.3 AC « Docusign Qualified Seal CA G1 »

CRL Fields	Value
Version	1 (=version 2)

CRL Fields	Value
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Qualified Seal CA G1
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z = thisUpdate + 6 days
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)

CRL Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
CRL Number	**FALSE**	
crlNumber		Monotonically increasing sequence number
Expired Certs On CRL	**FALSE**	
expiredCertsOnCRL		2026/02/10 11:25:51 Z (CA certificate validity start)

CRL Entry Extensions	Criticality (True/False)	Value
No CRL entry extension allowed	**N/A**	N/A

6.6.2.4 AC « Docusign Qualified TimeStamp CA G1 »

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Qualified TimeStamp CA G1
ThisUpdate	YYYY/MM/DD HH:MM:SS Z (CRL issuance date)
NextUpdate	YYYY/MM/DD HH:MM:SS Z = thisUpdate + 6 days
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)

CRL Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
CRL Number	**FALSE**	
crlNumber		Monotonically increasing sequence number

CRL Entry Extensions	Criticality (True/False)	Value
No CRL entry extension allowed	**N/A**	N/A

6.6.3 Profil OCSP

L'OCSP est définit conformément au RFC 6960.

Tous les certificats d'OCSP inclue l'extension OCSPnoCheck.

6.6.3.1 AC « Docusign Qualified CA G1 »

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Qualified CA G1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 1 year		
Subject	**Attribute type**	**Attribute value**	**Directory String[5]**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	organizationIdentifier	NTRFR-812611150	UTF8String
	CN	OCSP Responder <identifiant d'AC optionnel><*date*>	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	3072 bits minimum	
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)		

[5] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Extended Key Usage	**FALSE**	
id-kp-OCSPSigning		Set
Basic Constraint	**TRUE**	
cA		False
OCSPNoCheck	**FALSE**	
NULL		NULL

6.6.3.2 AC « Docusign Advanced Seal CA G1 »

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Advanced Seal CA G1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 1 year		
Subject	**Attribute type**	**Attribute value**	**Directory String[6]**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	organizationIdentifier	NTRFR-812611150	UTF8String
	CN	OCSP Responder <identifiant d'AC optionnel><*date*>	UTF8String

[6] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Basic Certificate Fields	Value	
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)
	Key size	3072 bits minimum
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)	

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Extended Key Usage	**FALSE**	
id-kp-OCSPSigning		Set
Basic Constraint	**TRUE**	
cA		False
OCSPNoCheck	**FALSE**	
NULL		NULL

6.6.3.3 AC « Docusign Qualified Seal CA G1 »

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Qualified Seal CA G1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 1 year		
Subject	**Attribute type**	**Attribute value**	**Directory String[7]**

[7] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Basic Certificate Fields	**Value**		
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	organizationIdentifier	NTRFR-812611150	UTF8String
	CN	OCSP Responder <identifiant d'AC optionnel><*date*>	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	3072 bits minimum	
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Extended Key Usage	**FALSE**	
id-kp-OCSPSigning		Set
Basic Constraint	**TRUE**	
cA		False
OCSPNoCheck	**FALSE**	
NULL		NULL

6.6.3.4 AC « Docusign Qualified TimeStamp CA G1 »

Basic Certificate Fields	**Value**		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France organizationIdentifier = NTRFR-812611150 CN = Docusign Qualified TimeStamp CA G1		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z 1 year		
Subject	**Attribute type**	**Attribute value**	**Directory String[8]**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	organizationIdentifier	NTRFR-812611150	UTF8String
	CN	OCSP Responder <identifiant d'AC optionnel><*date*>	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	3072 bits minimum	
Signature (algorithm & OID)	sha384WithRSAEncryption (1.2.840.113549.1.1.12)		

Extensions	**Criticality (True/False)**	**Value**
Authority Key Identifier	**FALSE**	
keyIdentifier		Defined by issuer CA (in its Subject Key Identifier)
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	

[8] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality (True/False)	Value
Digital Signature		Set
Extended Key Usage	**FALSE**	
id-kp-OCSPSigning		Set
Basic Constraint	**TRUE**	
cA		False
OCSPNoCheck	**FALSE**	
NULL		NULL

6.7 Audit de conformité et autres évaluations

6.7.1 Fréquence et/ou circonstances des audits

Les composantes du PSCo sont soumises à des vérifications de conformité périodique au moins une fois par an, pour permettre à la PMA d'autoriser ou non (basé sur le résultat de l'audit) les composantes du PSCo hébergées par l'OSC à fonctionner en conformité avec la présente PC.

Le PMA a le droit d'exiger une vérification complémentaire non périodique de la conformité des composantes du PSCo qui fonctionnent selon de la présente PC. La PMA indique la raison de toute vérification de conformité non périodique.

Au cours de la période dans laquelle l'AC émet des certificats, la PMA doit veiller au respect de la PC, de la DPC et des exigences de l'AE et contrôler strictement la qualité de service en effectuant des auto-vérifications sur au moins une base annuelle à partir d'un échantillon choisi au hasard sur au moins trois pour cent des certificats délivrés par elle au cours de la période commençant immédiatement après le précédent échantillon d'auto-vérification.

En complément, la PMA mandate un auditeur externe régulièrement, conformément aux exigences de l'ANSSI et d'eIDAS, afin de contrôler la conformité de l'AC aux exigences de l'ETSI et eIDAS pour tous les OIDs.

6.7.2 Identités/qualifications des évaluateurs

Les auditeurs doivent démontrer leurs compétences dans le domaine des audits de conformité, ainsi qu'être familiers avec les exigences de la PC.

Les auditeurs en charge de l'audit de conformité doivent effectuer l'audit de conformité comme tâche principale.

La PMA apporte une attention particulière quant à l'audit de conformité, notamment vis-à-vis de ses exigences en matière d'audit.

La PMA effectue elle-même le choix des auditeurs.

La PMA contrôle les méthodes d'audits des composantes du PSCo.

6.7.3 Relation entre évaluateurs et entités évaluées

Les auditeurs en charge de l'audit de conformité sont soit une entreprise privée indépendante de la PMA, soit une entité de la PMA suffisamment séparée des composantes auditées afin d'effectuer une évaluation juste et indépendante.

La PMA détermine si un auditeur remplit cette condition.

6.7.4 Sujets couverts par les évaluations

L'objectif de l'audit de conformité est de vérifier qu'une composante du PSCo opère ses services en conformité avec la présente PC et la DPC.

6.7.5 Actions prises à la suite des conclusions des évaluations

La PMA peut décider que l'AC, l'AE ou l'une de ses composantes n'agit pas en conformité avec les obligations définies dans la présente PC. Quand une telle décision est prise, la PMA peut suspendre les opérations de la composante non conforme du PSCo, ou peut donner l'ordre de cesser toute relation avec la composante en question, ou peut décider que des actions correctives sont à prendre.

Quand l'auditeur en charge de l'audit de conformité trouve une divergence avec les exigences de la présente PC, les mesures suivantes doivent être prises :

- L'auditeur note la divergence.
- L'auditeur avise l'entité en question de la divergence. L'entité en avise rapidement la PMA.
- La partie responsable de la correction de la divergence détermine quelles sont les mesures à prendre en fonction des exigences de la présente PC, et les effectue sans délai avec l'approbation de la PMA.

Suivant la nature et la gravité de la divergence, et la rapidité avec laquelle elle peut être corrigée, la PMA peut décider de suspendre temporairement le fonctionnement de la composante du PSCo ou de prendre toute autre mesure qu'il juge opportune.

Quand les actions correctives sont réalisées, la composante du PSCo en informe la PMA et lui fournit un rapport de mise à hauteur, pour évaluation.

Pour une AE, la PMA remet le rapport d'audit de l'AE au Client. En cas de non-conformité majeure découverte lors de l'audit effectué par DocuSign France ou l'auditeur externe, l'AE doit résoudre le problème rapidement et un audit, par un auditeur externe, sera conduit pendant la même année afin de vérifier les résultats vis-à-vis de la ou des non-conformité(*s*) majeure(*s*).

6.7.6 Communication des résultats

Un Rapport de Contrôle de Conformité, incluant la mention des mesures correctives déjà prises ou en cours par la composante, est remis à la PMA comme prévu ci-dessus. Ce rapport cite les versions des PC et DPC utilisées pour cette évaluation. Quand nécessaire, le rapport de contrôle peut être diffusé comme prévu ci-dessus. Le Rapport de Contrôle de Conformité n'est pas rendu disponible à des tiers utilisateurs sur Internet.

6.8 Autres PROBLEMATIQUES METIERS ET LEGALES

6.8.1 Tarifs

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

6.8.2 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 PSCo 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.

6.8.3 Confidentialité des données professionnelles

6.8.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- Les clés privées de l'AC, des composantes du PSCo et des Porteurs.
- Les données d'activation et parts de secret associées aux clés privées d'AC, des composantes du PSCo et des Porteurs.
- Les journaux d'évènements des composantes du PSCo.
- Le dossier d'enregistrement et les données personnelles du Porteur.
- La politique de sécurité interne du PSCo.
- Les contrats entre DocuSign France et les Clients.
- Les procédures de sécurité de l'OSC.
- Les parties de la DPC considérées comme confidentielles.

Par ailleurs, l'AC garantit que seuls ses personnels dans des rôles de confiance autorisés, les personnels contrôleurs dans la réalisation des audits de conformité, ou d'autres personnes détenant le besoin d'en connaître, ont accès et peuvent utiliser ces informations confidentielles.

L'AE et le Client doivent maintenir la confidentialité des informations commerciales et techniques qui sont désignées comme confidentielles dans la présente PC, le contrat établi avec DocuSign France ou par sa nature devrait raisonnablement être compris comme confidentielles, et devront traiter ces informations suivant des règles définies par le Client et l'AE.

6.8.3.2 Informations hors du périmètre des informations confidentielles

Les données figurant dans le certificat ne sont pas considérées comme confidentielles.

6.8.3.3 Responsabilité en termes de protection des informations confidentielles

Les composantes du PSCo ont mis en place et respectent des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme confidentielles.

A cet égard, les composantes du PSCo respectent notamment la législation et la réglementation en vigueur applicables.

En particulier, il est précisé qu'elle peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales.

6.8.4 Protection des données personnelles

6.8.4.1 Politique de protection des données 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. Le PSCo met en œuvre des mesures de sécurité afin de protéger les données personnelles quand elles sont stockées et transmises avec des composants qui sont en dehors du PSCo ou avec le Porteur.

La collecte et l'usage de données personnelles par les composantes du PSCo dans le cadre du traitement des Certificats et des bi-clés sont réalisés dans le strict respect de la législation et de la réglementation en vigueur en Europe.

Le Client veille à ce que l'IDP applique une politique de gestion des données personnelles, conformément à la loi européenne et comme stipulé dans le contrat entre l'IDP et DocuSign France, afin de protéger les informations personnelles qu'elles recueillent.

6.8.4.2 Informations à caractère personnel

Le PSCo considère que les données d'identification et de contacts contenues dans les dossiers d'enregistrement et les traces d'audit d'utilisation des bi-clés associées au Certificat, sont des informations à caractère personnel qui doivent être protégées suivant la loi nationale du PSCo (GDPR).

6.8.4.3 Informations à caractère non personnel

Les informations contenues dans un Certificat sont par nature publiques et ne doivent pas être considérées comme confidentielles.

6.8.4.4 Responsabilité en termes de protection des données personnelles

Le PSCo a mis en place et respecte des procédures de protection des données personnelles pour garantir la sécurité des informations caractérisées comme personnelles ci-dessus dans le cadre de la délivrance et la gestion d'un Certificat de Porteur.

A cet égard, le PSCo respecte notamment la législation et la réglementation en vigueur sur le territoire français à savoir le GDPR.

En application du GDPR, les Porteurs disposent d'un droit d'accès, de modification, de rectification et de suppression des données qui les concernent comme convenu et décrit dans les CGU du Client.

Pour l'exercer, les Porteurs doivent s'adresser à DocuSign France en utilisant les informations fournies dans les CGU.

Pour toute autre information relative à l'exercice de leurs droits en matière de données à caractère personnel, les Porteurs peuvent s'adresser à Docusign en utilisant les informations fournies dans les CGU.

6.8.4.5 Notification et consentement d'utilisation de données personnelles

Aucune des données à caractère personnel communiquées lors de l'enregistrement (Cf. § 6.2.2, § 6.2.3 et § 6.2.4, § 6.31 et § 6.3.2) ne peut être utilisée par le PSCo, pour une autre utilisation autre que celle définie dans le cadre de la PC, sans consentement explicite et préalable de la part du Porteur.

Le consentement du Porteur pour l'utilisation desdites données comme défini dans le cadre de la PC est considéré comme obtenu par le PSCo dans les conditions définies par le PSCo lors de l'acceptation des CGUs comme définit au § 6.3.2.

Le Porteur accepte que les données personnelles le concernant recueillies par le PSCo fassent l'objet d'un traitement informatique aux seules fins : d'être authentifié par l'AE, pour communiquer des données d'activation, de permettre la construction de l'Identité portée dans les Certificats et d'apporter les preuves nécessaires à la gestion des Certificats et l'usage des clés privées associées au Certificat.

6.8.4.6 Condition de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Le PSCo agit conformément aux réglementations européenne et française, et dispose de procédures sécurisées pour permettre l'accès aux données à caractère personnel aux autorités judiciaires sur décision(*s*) judiciaire(*s*) ou autre autorisation(*s*) légale(*s*).

6.8.4.7 Autres circonstances de divulgation d'informations personnelles

La PMA obtient l'accord des composantes du PSCo de transférer ses données à caractère personnel dans le cas d'un transfert d'activité tel qu'il est décrit dans le présent document.

6.8.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par le PSCo sont protégés par la loi, règlement et autres conventions internationales applicables.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages Web, bases de données, textes originaux, etc) est sanctionnée par le Code de la propriété intellectuelle.

Le PSCo détient tous les droits de propriété intellectuelle et elle est propriétaire de la PC et de la DPC associée, des certificats émis par l'AC.

Le Porteur détient tous les droits de propriété intellectuelle sur les informations personnelles contenues dans les Certificats porteurs émis par l'AC et dont il est propriétaire.

L'Entité Légale du Porteur détient tous les droits de propriété intellectuelle sur les informations de l'Entité Légale contenues dans les Certificats Porteurs et dont elle est propriétaires.

6.8.6 Interprétations contractuelles et garanties

Les composantes du PSCo, les Clients et la communauté de Porteurs sont responsables pour tous dommages occasionnés en suite d'un manquement de leurs obligations respectives telles que définies aux termes de la PC, des CGU et les contrats Clients.

Les obligations communes des différentes composantes du PSCo sont :

- Accepter que l'équipe de contrôle effectue les audits et lui communiquer toutes les informations utiles, conformément aux intentions de la PMA de contrôler et vérifier la conformité avec la PC.
- Assurer l'intégrité et la confidentialité des clés privées dont elles sont dépositaires, ainsi que des données d'activation desdites clés privées, le cas échéant.
- N'utiliser les clés publiques et privées dont elles sont dépositaires qu'aux seules fins pour lesquelles elles ont été émises et avec les moyens appropriés.
- Mettre en œuvre les moyens techniques adéquats et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elles s'engagent.
- Documenter leurs procédures internes de fonctionnement à l'attention de leurs personnels respectifs en charge de leurs applications dans le cadre des fonctions qui leurs sont dévolues en qualité de composante du PSCo.
- Protéger les données personnelles.
- Fournir les services qui leur incombe en accord avec la DPC et la PC et le référentiel du PSCo.
- Accepter le résultat et les conséquences d'un contrôle de conformité et, en particulier, remédier aux non-conformités qui pourraient être révélées.
- Respecter les conventions qui les lient aux autres entités composantes du PSCo.

6.8.6.1 Obligations et garanties de la PMA

Les obligations de la PMA sont les suivantes :

- L'élaboration de la PC et de la DPC et de l'analyse de risque.

- L’audit du PSCo et en particulier des AE et y compris lorsque la composante du PSCo est opérée par un sous-traitant.
- La désignation des rôles de confiance du PSCo.
- L’homologation des services du PSCo.
- Le maintien de la conformité des services du PSCo y compris en cas de sous-traitance.

6.8.6.2 Obligations et garanties de l'AC

L'AC s'assure que toutes les exigences détaillées dans la présente PC et la DPC associée, sont satisfaites en ce qui concerne ; l'émission et la gestion de Certificats Porteurs et de leur bi-clés associées et des CRL et OCSP et des bi-clés des composantes du PSCo.

L'AC est responsable du maintien de la conformité aux procédures prescrites dans la présente PC.

L'AC fournit tous les services de certification en accord avec la DPC et la PC et le référentiel du PSCo.

6.8.6.3 Obligations de l’AE

L'AE s'assure que toutes les exigences détaillées dans la présente PC et la DPC associée, sont satisfaites en ce qui concerne l'émission et la gestion de l’identification et l’authentification des Porteurs et du traitement des demande de Certificat et de révocation.

L'AE est responsable du maintien de la conformité aux procédures prescrites dans la présente PC.

L'AE fournit tous les services de certification en accord avec la DPC et la PC et le référentiel du PSCo.

6.8.6.4 Obligation du Client

Les obligations du Client sont définies dans le contrat entre Docusign et le Client.

6.8.6.5 Obligations de l’OSC

Les obligations de l’OSC sont :

- Respecter la politique de sécurité du PSCo.
- Protéger les secrets du PSCo.
- Documenter ses procédures internes afin de compléter la DPC et la politique de sécurité du PSCo.
- Respecter la totalité du contrat qui l’engage vis-à-vis de DocuSign France.

6.8.6.6 Obligation de l’IDP

Les obligations de l’IDP sont décrites dans le contrat entre l’IDP et DocuSign France. L’IDP est responsable de maintenir sa certification PVID ou [119 461] pour l’identification des Porteurs.

6.8.6.7 Obligations et garanties du Porteur

Les obligations du porteur sont définies dans les CGUs qu’ils acceptent.

6.8.6.8 Obligations et garanties de l’UC

Les obligations de l’UC sont :

- Accepter seulement les usages autorisés des Certificats comme mentionnés dans l’extension « KeyUsage » des Certificats.
- Vérifier la validité des Certificats en utilisant les méthodes recommandées dans [RFC 5280] avant de faire confiance à un Certificat et celles décrites dans le présent document au § 5.5 et § 6.3.5.

- Vérifier que les OIDs contenus dans les Certificats afin d'être assuré de n'utiliser que les types de Certificats souhaités en provenance de l'AC.
- Vérifie que les Certificats Porteurs sont signés par l'AC.
- Contrôle l'état de validité des certificats d'AC à l'aide des CRLs et/ou OCSP publiée par les AC de la chaîne de certification.
- Arrêter d'utiliser le Certificat s'il n'est plus valide et le retirer des applications qui l'utilisent.
- Conserver le Document signé, les applications nécessaires à sa lecture et sa vérification technique de signature aussi longtemps que l'UC aura besoin de vérifier la signature et le Certificat.
- Vérifie que les certificats d'AC sont signés par une AC valide et en vérifier le chemin de certification comme indiqué dans [RFC 5280].

6.8.7 Limite de garantie

Les limites de garanties sont décrites dans les contrats Client avec Docusign et les CGUs.

6.8.8 Limite de responsabilité

Les limites de responsabilité sont décrites dans les contrats Client avec Docusign et les CGUs.

6.8.9 Indemnités

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

6.8.10 Durée et fin anticipée de validité de la PC

6.8.10.1 Durée de validité

La PC devient effective une fois approuvée par la PMA. La PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

6.8.10.2 Fin anticipée de validité

Selon l'importance des modifications apportées à la PC, la PMA décidera soit de faire procéder à un audit de la PC/DPC des composantes du PCSo concernées, soit de donner instruction aux composantes du PSCo de prendre les mesures nécessaires pour se rendre conforme dans un délai fixé.

6.8.10.3 Effets de la fin de validité et clauses restant applicables

La fin de validité de la PC entraîne la cessation de toutes les obligations et responsabilités du PCSo pour les certificats émis conformément à la PC. L'AC concernée ne peut plus émettre de Certificat.

6.8.11 Notifications individuelles et communications entre les participants

La PMA fournit la nouvelle version de la PC via le SP dès que la PC est validée par la PMA.

6.8.12 Amendements à la PC

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 PC 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.

6.8.13 Dispositions concernant la résolution de conflits

La PMA s'assure que tous les accords contractuels avec les Clients et les Porteurs qu'elle établir prévoient des procédures adéquates pour le règlement des différends.

Les CGUs et les contrats Client avec Docusign décrive la résolution des litiges.

6.8.14 Juridictions compétentes

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

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique, et faute d'être parvenues à un accord amiable ou à une transaction, les parties règlent le litige conformément aux règles établies dans le contrat entre le Client et DocuSign France.

6.8.15 Conformité aux législations et réglementations

Le PSCo est opéré conformément à la réglementation GDPR, eIDAS et aux lois françaises qui s'appliquent.

Le PSCO applique un programme d'audit interne et externe comme définit au § 6.7 et mène une veille active dans le domaine de la standardisation à l'ETSI et dans les instances idoines de standardisation en lien avec eIDAS.

Le Client et DocuSign France s'accordent sur le droit applicable dans le contrat établit entre DocuSign France et le Client.

6.8.16 Dispositions diverses

6.8.16.1 Transfert d'activités

Sauf si spécifié dans d'autres contrats, seule la PMA a le droit d'affecter et de déléguer la PC à une partie de son choix.

6.8.16.2 Conséquence d'une clause non valide

Le caractère inapplicable dans un contexte donné d'une disposition de la Politique de Certification n'affecte en rien la validité des autres dispositions, ni de cette disposition hors du dit contexte.

La Politique de Certification continue à s'appliquer en l'absence de la disposition inapplicable et ce tout en respectant l'intention de ladite Politique de Certification.

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

6.8.16.3 Application et renonciation

Les exigences définies dans la PC/DPC doivent être appliquées selon les dispositions de la PC et de la DPC associée sans qu'aucune exonération des droits, dans l'intention de modifier tout droit ou obligation prescrit, ne soit possible.

6.8.16.4 Force majeure

L'AC ne saurait être tenue pour responsable de tout dommage indirect et interruption de ses services relevant de la force majeure, laquelle aurait causé des dommages directs aux porteurs ou aux UC.

6.9 Autres dispositions

6.9.1 Organisationnelle

L'organisation du PSCo est organisée de telle sorte à être fiable.

En particulier :

- Les politiques et pratiques du PSCo sont non discriminatoires.
- Le PSCo rend ses services accessibles à tous les demandeurs dont les activités relèvent de son domaine d'activité déclaré et qui acceptent de respecter leurs obligations telles que spécifiées dans les CGUs.
- Le PSCo maintient des ressources financières suffisantes et/ou souscrire une assurance responsabilité civile appropriée, conformément à la législation applicable, pour couvrir les responsabilités découlant de ses opérations et/ou activités.
- Le PSCo dispos de la stabilité financière et des ressources nécessaires pour exercer ses activités conformément à la présente politique.
- Le PSCo a des politiques et des procédures pour le règlement des plaintes et des litiges reçus des clients ou d'autres parties s'appuyant sur eux concernant la fourniture des services ou toute autre question connexe.

Les opérations et les domaines de responsabilité sont séparés afin de réduire les risques de modification, de conflit d'intérêt ou d'utilisation abusive non autorisée ou involontaire des actifs du PSCo.

Les composants et personnels du PSCo chargés de la génération et de la révocation des Certificats sont indépendants des autres organisations de Docusign pour leurs décisions relatives à la mise en place, à la fourniture, au maintien et à la suspension des services, conformément à la présente PC.

En particulier :

- La direction, les cadres supérieurs et le personnel occupant des rôles de confiance du PSCo chargé de la génération et de la révocation des Certificats Porteurs, d'AC et d'OCSP sont exempts de toute pression commerciale, financière ou autre susceptible de nuire à la confiance dans les services fournis.
- Les composants et personnels du PSCo chargés de la génération et de la révocation des Certificats Porteurs, d'AC et d'OCSP disposent d'une structure documentée garantissant l'impartialité des opérations.

6.9.2 Certificat de test

Un Client a la possibilité de tester tous les profils de Certificats des ACs de la présente PC avec l'une des deux manières en fonction du service de signature :

- En environnement de production : en ce cas le Certificat est émis exactement suivant les exigences et pratiques de la présente PC et quand cela est nécessaire pour les Certificat Cachet la mention « TEST » est insérée dans le DN et dans tous les cas une vraie identité pour le Certificat Signataire est utilisée. Le PSCo demande au Client de signer un document de test et peux si besoin révoquer le Certificat émis.
- En environnement dit de démo (avec des AC dite de démo et donc différente de celles de PROD) : en ce cas, les profils ont les mêmes caractéristiques que ceux décrits dans la présente PC et cependant

ont un champ OU en plus dans le DN du sujet qui comporte au moins le terme « TEST » et l'OID d'Adobe qui permet d'afficher une croix rouge « 1.2.840.113583.1.2.2 ».

Les Certificats de test sont utilisés de la même manière que les Certificats de production.

6.9.3 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.

6.9.4 Termes et conditions (CGU)

Le PSCo met les CGUs à la disposition de tous les Porteurs et des Vérificateurs via le SP.

Les CGUs précise au moins les aspects suivants :

- La gestion des données personnelles et l'accord du Porteur par rapport à la collecte et à la gestion des données personnelles par le PSCo ;
- L'obligation de fournir au PSCo des informations exactes et complètes conformément aux exigences du présent document, notamment en ce qui concerne l'enregistrement ;
- L'obligation d'utiliser la bi-clé uniquement conformément aux limitations notifiées au Porteur ou au CT et RL en fonction du type de Certificat ;
- L'interdiction d'utilisation non autorisée de la clé privée associé au Certificat ;
- L'obligation d'informer le PSCo sans délai si l'un des événements suivants se produit jusqu'à la fin de la période de validité indiquée dans le Certificat :
    - i) La clé privée associée au Certificat a été potentiellement compromise ;
    - ii) Le contrôle de la clé privée associée au Certificat a été perdu en raison de la compromission des Facteurs d'Activation ou de connexion à la plateforme Docusign pour tous les Certificats ou au service de persistance d'identité pour les Certificat Signataire ou pour d'autres raisons ;
    - iii) une inexactitude ou des modifications du contenu du Certificat, telles que notifiées au Porteur ;
- L'obligation, à la suite de la compromission de la clé privée associée au Certificat, de cesser immédiatement et définitivement l'utilisation de cette clé ;
- Les modalités d'acception des CGUs ;
- La durée de rétention des données personnelles ;
- Les obligations des Porteurs pour le Certificat Signataire ;
- Les obligations du RL et CT pour le Certificat Cachet ;
- 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.