DocuSign

Certificate Policy and Public Certificate Practice Statement

Protect and Sign Personal Signature : Utilisateur ETSI

CERTIFICATE POLICY AND PUBLIC CERTIFICATE PRACTICE STATEMENT PROTECT AND SIGN PERSONAL SIGNATURE : UTILISATEUR ETSI

Version du document :	2.6	**Nombre total de pages :**	88
Statut du document :	☐ Projet	☒ Version finale	
Rédacteur du document :	RSSI DocuSign France		

Liste de diffusion :	☒ Externe	☒ Interne DocuSign France
	Public	Public

Historique du document :

Date	Version	Rédacteur	Commentaires	Vérifié par
07/01/2015	1.1	EM	Création de la version (1.1) en français	JYF
23/01/2016	1.2	EM	Modification suite au rachat de TDT par DocuSign	
22/03/2016	1.3	EM	Modification pour ajout du certificat avec SSCD.	
31/03/2017	1.4	EM	Passage aux nouveau standards ETSI EN 319 411-2	
26/05/2017	1.5	EM	Intégration des commentaires LSTI.	
06/04/2018	1.6	EM	Mise à jour pour insertion d'un nouveau profil de certificat 319 411-1 LCP. Mise à jour de contenu mineure.	
16/10/2018	1.7	EM	Mise à jour et intégration du permis de conduire autrichien pour l'enregistrement d'une personne en Autriche seulement.	
26/10/2018	1.8	EM	Modification pour ne plus avoir les CGU signé par le Porteur pour le niveau LCP.	
03/06/2019	1.9	EM	Mise à jour des contacts PMA et des profils de certificats et mis à jour de la PC.	
09/08/2019	2.0	EM	Mise à jour pour intégrer les résultats d'audit de LSTI.	
08/11/2019	2.1	EM	Mise à jour pour intégrer les résultats d'audit de LSTI.	
07/10/2020	2.2	EM	Modification du profil de certificat pour avoir une date de début avec une heure de moins, CPS URI pour avoir l'URL à jour et LCP certificat a "Digital signature" au lieu "of nonrepudiation".	
17/03/2021	2.3	EM	Modification d'informations du Contact et modification de l'extension KeyUsages pour ajouter la Valeur "nonrepudiation" pour être conforme avec le nouveau standard ETSI 319 412.	
15/07/2021	2.4	EM	Intégration des commentaires LSTI et SAP délégué.	
15/04/2022	2.5	EM	Intégration du PVID.	
30/03/2023	2.6	CG	Corrections et relecture	EM

SOMMAIRE

AVERTISSEMENT

La présente Politique de Certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteurs, 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, par photocopie, par enregistrement informatique, etc*), non autorisée préalablement de manière expresse par DOCUSIGN FRANCE ou ses ayants droits, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'Article L.122-5, 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, « *toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite* » (*Article L.122-4 du Code de la Propriété Intellectuelle*).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les Articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

1 INTRODUCTION

1.1 Présentation générale

La présente Politique de Certification (*PC*) décrit les règles que DocuSign France, ses Clients et les Porteurs doivent respecter pour assurer la gestion du cycle de vie de Certificats électroniques et de bi-clés de durée de vie courte destinés à la signature électronique de Documents métier par les Porteurs dans le cadre de Transactions électroniques réalisées entre eux.

Le service de signature porte le nom « Protect and Sign (*Personal Signature*) », il est décrit dans la Politique de Signature et de Gestion de Preuve (*appelée « PSGP » dans le présent document*) publiée par DocuSign France sur son site internet (*Cf. § 2.2*).

La présente PC contient également l'information publique du « Certificate Practice Statement » (*CPS ou Déclaration des Pratiques de Certification - DPC en français*), mais le document s'appelle PC.

DocuSign France a mis en place plusieurs Autorités de Certification (*appelée « AC » dans le présent document*), pour la délivrance de Certificats Porteurs (*appelés « Certificats » dans le présent document*) qui s'appuie sur une Infrastructure de Gestion de Clés (*IGC*).

Le service « Protect and Sign (*Personal Signature*) » permet aux Porteurs de signer des Documents au format PDF à l'aide des clés privées associées aux Certificats délivrés par l'AC. Les Porteurs de Certificats peuvent valider facilement les signatures électroniques de Documents PDF en utilisant les fonctionnalités de signature natives des produits de l'éditeur Adobe.

La présente PC a pour objet de décrire la gestion du cycle de vie des :

- Certificats (*des Porteurs*) délivrés par l'AC et des bi-clés associées.
- Certificats de l'AC et des bi-clés.

L'AC met en œuvre les services décrits dans cette PC de manière non discriminatoire dans les limites de ce que les technologies actuelles autorisent.

La présente PC est élaborée conformément :

- Au RFC 3647 : « Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework » de l'Internet Engineering Task Force (*IETF*).
- Au documents ETSI :
    - [119 312] : ETSI TS 119 312 V1.4.1 (2021-08) :
        - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.
    - [319 401]: ETSI EN 319 401 V2.3.1 (2021-05) :
        - Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers.
    - [319 412] :
        - ETSI EN 319 412-1 V1.4.1 (2021-05) :
            - Electronic Signatures and Infrastructures (ESI); Certificate Profiles,

              Part 1: Overview and common data structures.
        - ETSI EN 319 412-2 V2.2.1 (2020-07) :
            - Electronic Signatures and Infrastructures (ESI), Certificate Profiles,

              Part 2: Certificate profile for certificates issued to natural persons.
        - ETSI EN 319 412-5 V2.3.1 (2020-04) :
            - Electronic Signatures and Infrastructures (ESI), Certificate Profiles,

              Part 5: QCStatements.
    - [319 411] :
        - ETSI EN 319 411-1 V1.3.1 (2021-05) :
            - Electronic Signatures and Infrastructures (ESI), Policy and security requirements for Trust Service Providers issuing certificates,

              Part 1: General requirements.
        - ETSI EN 319 411-2 V2.4.1 (2021-11) :
            - 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.
- [CRYPTO] : « Référentiel Général de Sécurité, version 2.0, Annexe B1, Mécanismes cryptographiques, Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, Version 2.03 du 21 février 2014, (*Annule et remplace la version 1.20 du 26 janvier 2010*) ».
- [PSMP]: Proof Signature and Management Policy, version 1.6 "DSF_Protect and Sign_Personal Signature_PSGP v 1 8".
- [PSM QSCD]: "Secure Information Technology Center – Austria, QSCD-CERTIFICATE PURSUANT TO ART. 30 PARA 3 LIT B. EIDAS1, Qualified Signature Creation Device (QSCD), Protect & Sign, version 5.14, QSCD-Certificate issued on: 2021-11-30, Reference number: A-SIT-VIG-21-083" notified in EU list (https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd).

1.2 Identification du document

La présente PC appelée : « Protect and Sign Personal Signature : Utilisateur ETSI » est la propriété de DocuSign France. Cette PC contient les OID suivants (*un seul OID par type de certificat*) :

- AC " Cloud Signing Personal Signature CA" :
  - SBS EU certified (*usage unique signature*) :
    - ETSI 102 042 LCP.
    - 1.3.6.1.4.1.22234.2.8.3.9 : Ce profil de certificats n'est plus émis par cette AC à partir de juillet 2017 mais l'AC émet toujours les CRL associée.
      - Il n'existe plus que des certificats expirés avec ce profil.
  - Advanced signature with qualified certificate (*usage unique de signature*) :
    - ETSI 101 456 QCP.
    - 1.3.6.1.4.1.22234.2.8.3.7 : Ce profil de certificats n'est plus émis à partir de juillet 2017 mais l'AC émet toujours les CRL associée.
      - Il n'existe plus que des certificats expirés avec ce profil.
  - SBS Qualified (*usage unique signature*) :
    - ETSI EN 319 411-2 QCP-n-qscd.
    - 1.3.6.1.4.1.22234.2.8.3.20 : Ce profil est mis en œuvre par l'AC et certifié ETSI.
      - Ce profil ne sera plus mis en œuvre par l'AC à partir du 01 octobre 2019 car l'AC ne sera plus qualifiée à partir du 01 octobre 2019.
- AC "DocuSign Premium Cloud Signing CA – SI1" :
  - SBS Qualified (*usage unique signature*).
  - ETSI EN 319 411-2 QCP-n-qscd.
    - 1.3.6.1.4.1.22234.2.14.3.31 : Ce profil est mis en œuvre par l'AC et certifié ETSI avec le nouveau profil de certificat.
- AC "DocuSign Cloud Signing CA – SI1" :
  - SBS EU certified (*usage unique signature*).
  - ETSI EN 319 411-1 LCP.
    - 1.3.6.1.4.1.22234.2.14.3.32 : Ce profil est mis en œuvre par l'AC et certifié ETSI avec le nouveau profil de certificat.

Toutes les AC ci-dessus sont signées par l'ACI (*AC Intermédiaire*) "OpenTrust CA for AATL G1".

L'ACI "OpenTrust CA for AATL G1" est signée par l'ACR (*AC Racine*) "OpenTrust Root CA G1".

La présente PC contient les exigences communes et particulières liées aux services et aux types de Certificats gérés par ces AC.

Les particularités sont identifiées dans le corps de texte directement en utilisant l'OID.

Des éléments plus explicites tels que le nom, le numéro de version, la date de mise à jour, permettent d'identifier la présente PC, néanmoins le seul identifiant de la version applicable de la PC est l'OID.

1.3 Entités intervenant dans l'IGC

Pour délivrer les Certificats, l'AC s'appuie sur les services suivants :

- Service de génération de bi-clé d'AC : ce service génère les bi-clés et les demandes de signatures de certificats (CSR) associées durant une cérémonie des clés.
- Service d'enregistrement : ce service collecte et vérifie les informations d'identification du Porteur qui demande à signer un Document métier dans le cadre d'une Transaction électronique. Ce service crée une demande de Certificat, à l'aide des informations collectées et vérifiées, et la transmet au service de génération de certificat en utilisant un Connecteur Client.
- Service de génération de certificat : ce service génère les Certificats électroniques des Porteurs à partir des informations transmises par le service d'enregistrement.
- Service de gestion des bi-clés Porteur : ce service permet de générer les bi-clés des Porteurs dans des ressources cryptographiques (*matériel certifié*).
- Service de gestion des données d'activation : ce service permet de générer et d'utiliser les données d'activation associées aux bi-clés des Porteurs.
- Service d'authentification de demande de révocation Utilisateur (*seulement pour les cas d'urgence comme décrit dans le contrat signé entre DocuSign France et le Client*) : ce service consiste à collecter les informations nécessaires à l'authentification d'un Utilisateur qui souhaite révoquer son Certificat et à transmettre la demande de révocation à l'AC.
- Service de génération de LCR : ce service génère des Liste de Certificats Révoqués (*LCR*) qui contiennent les identifiants des Certificats Utilisateurs à révoquer.
- Service de Publication : 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.
- Service OCSP : l'AC délivre une information de validité de Certificat via OCSP.
- Service de journalisation et d'audit : ce service permet de collecter l'ensemble des données utilisées et ou générées dans le cadre de la mise en œuvre des services d'IGC afin d'obtenir des traces d'audit consultables. Ce service est mis en œuvre par l'ensemble des composantes techniques de l'IGC.

La présente PC définit les exigences de sécurité pour tous les services décrits ci-dessus dans la délivrance des Certificats par l'AC aux Porteurs. La Déclaration des Pratiques de Certification (*notée DPC*) donnera les détails des pratiques de l'IGC dans cette même perspective.

Les composantes de l'IGC mettent en œuvre leurs services conformément à la présente PC et la DPC associée.

Les changements majeurs au sein du TSP ou de ses partenaires Authorités d'Enregistrement (*AE*) sont notifiés à l'ANSSI.

1.3.1 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 et des procédures mises en œuvre par les composantes de l'IGC.

La PMA :

- Valide le référentiel de sécurité composé de la PC et de la DPC.
- Autorise et valide la création et l'utilisation des composantes de l'IGC.
- Suit les audits et/ou contrôle de conformités effectuées sur les composantes de l'IGC.
- Décide des actions à mener et veille à leur mise en application.
- Valide que le Client possède des procédures spécifiques pour les services de l'AE qu'il met en œuvre.
- Valide la politique d'enregistrement du Client.

Les missions principales de la PMA sont les suivantes :

- Approuver les services IGC délivrés par l'IGC.
- 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 l'IGC.
- 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 de l'IGC.
- Approuver les rapports d'audit des AE réalisés par DocuSign France.
- Gèrer les audits externes de l'AE.
- Approuver les Protocoles de Consentements définis par DocuSign France.
- Approuver les procédures définies par le Client pour la gestion des Utilisateurs.
- 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 de l'IGC 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.

1.3.2 Autorité de Certification (AC)

L'AC génère des certificats et révoque des certificats à partir des demandes que lui envoie l'AE.

L'AC met en œuvre les services suivants :

- Génération de bi-clé d'AC.
- Génération de Certificats.
- Gestion des bi-clés Porteurs.
- Gestion des données d'activation.
- Génération de LCR et de journalisation et d'audit.

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.

L'AC agit 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 »).*
DocuSign France est AC au sens de la responsabilité de gestion du cycle de vie des certificats.

1.3.3 Autorité d'Enregistrement (AE) :

L'AE est utilisée pour la mise en œuvre des services suivants :

- Enregistrement.
- Authentification de demande de révocation Utilisateur.
- Journalisation.
- Audit.

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

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

L'AE utilise son ou ses propre(*s*) opérateur(*s*) technique(*s*) pour mettre en œuvre ses services et héberger le Connecteur Client.

L'AE est désignée et habilitée par l'AC dans le cadre d'un contrat de service « Protect and Sign (*Personal Signature*) » signé par le représentant habilité du Client.

Le rôle de l'AE est d'établir que le Porteur justifie de l'identité qui sera indiquée dans le Certificat. Ces procédures d'identification sont variables selon le niveau de confiance que le Client (*ou l'entité légale désignée par le Client*) entend apporter à cette vérification.

L'AE documente et implémente les procédures d'identification (*dans le cadre du Protocole de Consentement*) des utilisateurs professionnels (*qui appartiennent à une entité légale et signe donc des documents dans un cadre professionnel*) et particuliers (*qui signent dans un cadre personnel*), en fonction de ses besoins métiers.

Par conséquent l'AE est responsable de définir les procédures qui adressent plus particulièrement les chapitres 3, 4, 5, 6, 8 et 9 de la présente PC et qui la concernent. Si le Client désigne une entité légale différente comme AE, alors un contrat, ou un document légal (*suivant le type de lient existant entre l'AE et le Client*), doit être établit entre l'AE et le Client afin de couvrir l'ensemble des missions d'AE que l'AE doit adresser et réaliser.

Les procédures pour gérer les Utilisateurs, définies par l'AE, sont mises en œuvre par des Opérateurs d'AE.

L'AE est responsable d'établir et de maintenir à jour une liste des Opérateurs d'AE qui sont autorisés à enregistrer des Utilisateurs.

L'AE devra en tout état de cause respecter la politique (*procédures*) d'enregistrement qu'elle aura préalablement défini et mise en œuvre dans le cadre de ses pratiques commerciales (*Cf. § 1.3.7.1 Client*).

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.

1.3.4 Opérateur de Service de Certification (*OSC*)

L'OSC assure des prestations techniques, en particulier cryptographiques, nécessaires aux services d'IGC, 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 de l'IGC.

L'OSC ne peut pas commencer des opérations pour des services de l'IGC 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 et le Service de Publication (*SP*).
- Le Client est OSC pour l'AE.

1.3.5 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 § 2*).
Le SP agit conformément à la PC et à la DPC associée.

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

Le PVID est une entité contractuellement liée à DSF par un Contrat de Service.
Le PVID n'est utilisé que dans le service [QES PVID].
Le PVID prend en charge les services PKI suivants :

- Génération de traces de journal et enregistrement des informations d'enregistrements.
- Transmission de la demande de demande de certificat à l'AE.
- Authentification initiale de l'abonné à distance selon les exigences de l'ANSSI.
- Validation initiale de l'identité de l'Abonné.
- Vérifier l'identifiant de l'Abonné et collecter des données lors de l'opération d'identification (*courrier électronique, numéro de téléphone, etc*).

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

Le PVID doit être certifié par l'ANSSI avant d'être utilisé pour [QES PVID] selon les règles suivantes :

https://www.ssi.gouv.fr/actualite/publication-du-referentiel-dexigences-applicables-aux-prestataires-de-verification-didentite-a-distance-pvid/.

Une liste des PVID est établie et maintenue par l'AE.

1.3.7 Porteurs de certificats

Un Porteur est une personne physique dont l'identité apparaît dans le Certificat, qui se connecte sur l'application du Client pour signer un Document métier via l'Application « Protect and Sign - Personal Signature » sur un terminal d'affichage dans le cadre d'un Protocole de consentement avec des données d'activation selon les règles définies par le Client (*procédure d'enregistrement appliquées par l'AE et procédure de signature appliquées par le Client*).

Le Porteur est aussi appelé « Utilisateur » ou « Signataire » dans la [PSGP].

Le Porteur respecte la PC et les procédures de l'AE suivant des règles définies dans la documentation de l'AE.

1.3.8 Autres participants

1.3.8.1 Client

Le Client désigne l'entité légale, ayant signé un contrat avec DocuSign France, est responsable de :

- Désigner l'entité qui est AE.
- L'application Client qui génère le Document métier à signer et qui appelle l'Application « Protect and Sign - Personal Signature », via le Connecteur Client, pour mettre en œuvre une cinématique de signature.
- L'identification et de l'authentification des Utilisateurs conformément à sa politique d'enregistrement établie et mise en œuvre en sa qualité d'Autorité d'Enregistrement.
- La définition d'une Politique de signature, du Protocole de consentement, et des Données d'activation associées, qui s'appliquent pour chaque type de Porteur et de Document et de Transaction.
- Choisir parmi les OID de la PSGP pour sélectionner un niveau de sécurité de signature.

La définition complète du Client est donnée dans la [PSGP].

L'AE désignée doit être auditée suivant les règles définies au § 8.

1.3.8.2 Utilisateurs de certificats (*UC*)

L'utilisateur de certificat est une personne qui valide le Certificat d'un Porteur (*Cf. § 9.6.7 pour les règles de validation de l'UC*) dans le cadre de la validation de signature électronique de Document.

L'UC agît conformément à la [PSGP] en qualité de Vérificateur.

1.4 Usage des certificats

1.4.1 Domaines d'utilisations applicables

1.4.1.1 Certificat de l'AC

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

- La signature de Certificats de Porteurs.
- La signature de Certificats de répondeurs OCSP.
- La signature de LCR.

1.4.1.2 Certificat de Porteur

Les clés privées associées aux Certificats délivrés aux Porteurs sont exclusivement utilisées par les Porteurs identifiés à l'article 1.3.7 ci-dessus pour signer électroniquement des Documents dans le cadre de Transaction électronique selon un Protocole de Consentement (qui requiert une donnée d'activation technique) conformément à la Politique de signature et la CSR nécessaire à l'établissement d'un Certificat.

Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

Il est rappelé que l'utilisation de la clé privée du Porteur et du certificat associé doit rester strictement limitée au Service de signature comme défini dans la [PSGP]. Dans le cas contraire, leur responsabilité pourrait être engagée.

1.4.2 Domaines d'utilisations interdits

Les utilisations de certificats émis par l'AC à d'autres fins que celles prévues au § 1.4.1 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 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, qui elle décrit la gestion du cycle de vie des signatures.

Comme décrit dans la [PSGP], le Client élabore sa propre Politique de signature afin de définir notamment les engagements et les limites de responsabilités qu'une signature électronique confère au Document signé électroniquement, ainsi que les moyens et conditions d'établissement de la vérification de la signature électronique.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

La présente PC est sous la responsabilité de la PMA.

1.5.2 Point de contact

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

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

1.5.3 Entité déterminant la conformité d'une DPC avec cette PC

La PMA approuve la DPC. La PMA procède à des analyses/contrôles de conformité et/ou des audits qui aboutissent à l'autorisation ou non pour les composantes de l'IGC de gérer des certificats suivant les standards qui doivent être respectés. Dans tous les cas, l'évaluation de la conformité doit être effectuée par un audit indépendant de la composante d'IGC.

1.5.4 Procédure d'approbation de la conformité de la DPC

La PMA possède ses propres méthodes pour approuver le présent document. La PMA approuve les résultats de la revue de conformité effectuée par les experts qu'elle nomme à cet effet. Une DPC devient effective dès que la PMA l'a approuvée conforme à la PC.

1.6 Définitions et Acronymes

Certaines définitions sont directement reprises de la PSGP qui les complète et les précise.

1.6.1 Définitions

Accord d'utilisation de LCR: Un accord spécifiant les termes et conditions sous lesquels une Liste de Certificats Révoqués ou les informations qu'elle contient peuvent être utilisées.

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

Application « Protect and Sign - Personal Signature » : désigne l'ensemble cohérent d'informations et de programmes informatiques propriété de DocuSign France dont une partie est hébergée et exploitée sur la plateforme « Protect and Sign - Personal Signature » de DocuSign France et dont l'autre partie (*modules logiciels Connecteur Client et Proofviewer*) est incluse dans le kit de connexion livré au Client pour installation dans un environnement informatique de son choix. L'Application « Protect and Sign - Personal Signature » a pour objet de fournir au Client un service de signature de Document métier en ligne avec génération de Fichier de preuves et optionnellement d'archivage de Fichiers de preuves associés à des Transactions réalisées en ligne entre le Client et un ou plusieurs Utilisateur(*s*) au moyen d'un Terminal d'affichage.

Audit : Contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures. [ISO/IEC POSIX Security].

Critères Communs : ensemble d'exigences de sécurité qui sont décrites suivant un formalisme internationalement reconnu. Les produits et logiciels sont évalués par un laboratoire afin de s'assurer qu'ils possèdent des mécanismes qui permettent de mettent en œuvre les exigences de sécurité sélectionnées pour le produit ou le logiciel évalué.

Cérémonie de clés : Une procédure par laquelle une bi-clé d'AC ou AE est générée, sa clé privée transférée éventuellement sauvegardée, et/ou sa clé publique certifiée.

Certificat : clé publique d'une entité, ainsi que d'autres informations, rendues impossibles à contrefaire grâce au chiffrement par la clé privée de l'autorité de certification qui l'a émis [ISO/IEC 9594-8; ITU-T X.509].

Certificat d'AC : certificat pour une AC émis par une autre AC. [ISO/IEC 9594-8; ITU-T X.509]. Dans ce contexte, les certificats AC (*certificat auto signé*).

Certificat auto signé : certificat d'AC signé par la clé privée de cette même AC.

Chemin de certification : (*ou chaîne de confiance, ou chaîne de certification*) chaîne constituée de multiples certificats nécessaires pour valider un certificat.

Clé privée : clé de la bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

Clé publique : clé de la bi-clé asymétrique d'une entité qui peut être rendue publique. [ISO/IEC 9798-1].

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.

Confidentialité : La propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus [ISO/IEC 13335-1:2004].

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

Déclaration des Pratiques de Certification (*DPC*) : une déclaration des pratiques qu'une entité (*agissant en tant qu'Autorité de Certification*) utilise pour approuver ou rejeter des demandes de certificat (*émission, gestion, renouvellement et révocation de certificats*). [RFC 3647].

Disponibilité : La propriété d'être accessible sur demande, à une entité autorisée [ISO/IEC 13335-1:2004].

Document électronique métier (*Document*) : désigne un document électronique créé par le Client sous un format PDF ou XML et complété des informations relatives au Porteur.

Données d'activation : Des valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent et qui doivent être protégées (*par ex. un PIN, une phrase secrète, etc*).

Données d'activation Porteur : désigne les données (*par exemple ; OTP ou certificat d'authentification*) à un Porteur permettant de mettre en œuvre sa clé privée. Dans le cas d'un Certificat, ces données sont définies aux termes du Protocole de consentement et sont appelées données d'authentification Utilisateur.

Données d'authentification Porteur : désigne la donnée permettant de contacter le Porteur (*adresse de courrier électronique, numéro de téléphone, etc*) pour lui transmettre par exemple une donnée d'activation afin de l'authentifier lors de protocole de consentement et de mettre en œuvre sa clé privée.

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

Fonction de hachage : fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux deux propriétés suivantes :

- Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie.
- Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie [ISO/IEC 10118-1].
- Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

Identifiant de Transaction : désigne un numéro de référence unique, composé de 64 caractères au plus, généré par le Connecteur Client et permettant de lier un Original, sur lequel est apposée une Signature électronique, à un Utilisateur préalablement identifié par l'Application Client.

Infrastructure de Gestion de Clés (*IGC*) : infrastructure requise pour produire, distribuer, gérer et archiver des clés, des certificats et des Listes de Certificats Révoqués ainsi que la base dans laquelle les certificats et les LCR doivent être publiés. [2nd DIS ISO/IEC 11770-3 (08/1997)].

Intégrité : fait référence à l'exactitude de l'information, de la source de l'information, et au fonctionnement du système qui la traite.

Interopérabilité : implique que le matériel et les procédures utilisés par deux entités ou plus sont compatibles et qu'en conséquence il leur est possible d'entreprendre des activités communes ou associées.

Liste de Certificats Révoqués (LCR) : liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués.

Modules cryptographiques : Un ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (*signature, chiffrement, authentification, génération de clé, etc*). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée (*FIPS ou critères communs*), utilisé pour conserver et mettre en œuvre la clé privée d'AC.

Période de validité d'un certificat : La période de validité d'un certificat est la période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 2459].

PKCS #10 : (*Public-Key Cryptography Standard #10*) mis au point par RSA Security Inc., qui définit une structure pour une Requête de Signature de Certificat (*en anglais: Certificate Signing Request: CSR*).

Plan de secours (*après sinistre*) : plan défini par une AC pour remettre en place tout ou partie de ses services d'IGC après qu'ils aient été endommagés ou détruits à la suite d'un sinistre, ceci dans un délai défini dans l'ensemble PC/DPC.

Point de distribution de LCR *:* entrée de répertoire ou une autre source de diffusion des LCR; une LCR diffusée via un point de distribution de LCR peut inclure des entrées de révocation pour un sous-ensemble seulement de l'ensemble des certificats émis par une AC, ou peut contenir des entrées de révocations pour de multiples AC. [ISO/IEC 9594-8; ITU-T X.509].

Politique de Certification (*PC*) : ensemble de règles qui indique l'applicabilité d'un certificat à une communauté particulière et/ou une classe d'applications possédant des exigences de sécurité communes. [ISO/IEC 9594-8; ITU-T X.509].

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

Politique de sécurité : ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].

Politique de signature : désigne un ensemble de règles établies par le Client pour la création ou la validation d'une signature électronique via l'Application « Protect and Sign - Personal Signature », sous lesquelles une signature électronique peut être déterminée comme valide. Une politique de signature comprend notamment les éléments suivants :

1. L'identification d'un ou plusieurs points de confiance et des règles permettant de construire un chemin de certification entre le certificat du signataire et l'un de ces points de confiance.
2. Les moyens à mettre en œuvre pour obtenir une référence de temps destinée à positionner dans le temps la signature numérique du signataire et les données de validation.
3. Les moyens à utiliser pour vérifier le statut de révocation de chaque certificat du chemin de certification par rapport à cette référence de temps.
4. Les caractéristiques que doit comporter le Certificat du signataire.
5. L'ensemble des données de validation que le signataire doit fournir.

6. Les algorithmes cryptographiques (*signature et hachage*) à utiliser dans le cadre de la vérification de la signature numérique du document et des données de validation.

Porteur de secret : personnes qui détiennent une donnée d'activation liée à la mise en œuvre de la clé privée d'une AC à l'aide d'un module cryptographique.

Protocole de consentement : désigne l'ensemble des règles de recueil de consentement pour une application métier donnée utilisant le Service à savoir :

1. La définition des actions à réaliser par l'Utilisateur sur le Terminal d'affichage pour signer le Document métier proposé par l'Application Client.
2. Les informations utilisées pour la création de l'identité Utilisateur.
3. Les modalités de contrôle par le Service des informations saisies par l'Utilisateur par comparaison aux informations fournies par le Client pour chaque Transaction.
4. Le type de fichier soumis par le Client à signature (*XML/PDF, etc*).
5. Les modalités de visualisation du Document métier présenté et du message d'acceptation (*ou de refus*) associé. La description du protocole de consentement est définie dans le Document de mise en production.

Qualificateur de politique : Des informations concernant la politique qui accompagnent un identifiant de politique de certification (*OID*) dans un certificat X.509. [RFC 3647]

RSA : algorithme de cryptographie asymétrique utilisant une clé publique pour chiffrer et d'une clé privée pour déchiffrer des données confidentielles. inventé par par Ronald Rivest, Adi Shamir et Leonard Adleman en 1977.

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

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

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

Validation de certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de confiance et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (*révoqué ou non*), de l'identité des AC de la chaine de délivrance et la vérification de la signature électronique de l'ensemble des AC contenue dans le chemin de certification. Le concept de validation exposé dans cette PC et les CGU afférentes et les contrats liés à cette PC sont différents du concept de validation tel qu'exposé par l'ANSSI dans le document « *Référentiel Général de Sécurité, Chapitre 6. Validation des certificats par l'État* ».

1.6.2 Acronymes

- AC : Autorité de Certification.
- AE : Autorité d'Enregistrement.
- CC : Critères Communs.
- 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.

- HSM : Hardware Security Module.
- HTTP : HyperText Transport Protocol.
- IGC : Infrastructure de Gestion de Clés.
- IP : Internet Protocol.
- ISO : International Organization for Standardization.
- LCR : liste de certificats révoqués.
- LDAP : Lightweight Directory Access Protocol.
- OCSP : Online Certificate Status Protocol.
- OID : Object Identifier.
- PC : Politique de Certification.
- PIN : Personal Identification Number.
- PKCS : Public-Key Cryptography Standard.
- PMA : Policy Management Authority.
- PSGP : Politique de Signature et Gestion de Preuves.
- RFC : Request for comment.
- RSA : Rivest, Shamir, Adleman.
- SHA : Secure Hash Algorithm (*norme fédérale américaine*).
- SP : Service de Publication.
- URL : Uniform Resource Locator.

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

2.1 Entités chargées de la mise à disposition des informations

Le SP a la charge de la publication des données identifiées au § 2.2 ci-dessous.

Le SP est mis en œuvre 24 heures sur 24 et 7 jours sur 7 avec un taux de disponibilité de 99,9.

2.2 Informations devant être publiées

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

- La PC : https://www.docusign.fr/societe/politiques-de-certifications.
- Les certificats des ACR et AC : https://www.docusign.fr/societe/politiques-de-certifications.
- Le PDS est publié pour les certificats qualifiés seulement (*l'URL est dans le profil de certificat en annexe*).
- Les certificats de la chaîne de confiance auxquels les AC sont rattachées à savoir : https://www.docusign.fr/societe/politiques-de-certifications.
- Les modalités d'enregistrement et de signature : le Client est responsable de définir les modalités de communication de ces éléments aux Porteurs.
- Les conditions générales d'utilisation (*CGU*) : le Client (*AE*) est responsable de définir les modalités de communication de ces éléments aux Porteurs.
- Les certificats de l'ACR et de l'AC et du Porteur sont contenus dans le Document signé par le Porteur.
- LCR : se reporter au chapitre 10.

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. Elle sera aussi accessible en ligne en utilisant l'adresse CRL DP.

La DPC n'est pas publiée mais consultable auprès de la PMA sur demande justifiée et après autorisation de la PMA.

La PMA s'assure que les conditions générales d'utilisation, en fonction du besoin des acteurs et des utilisateurs des services de l'IGC, sont rendues disponibles de la manière suivante :

- Porteur : les CGU sont visualisées par le Porteur lors du Protocole de Consentement ou dans le Portail de l'AE.
- Le Client est responsable d'établir et rendre disponible les conditions particulières complémentaires requises par l'ETSI.
- Utilisateur de certificat : les conditions d'utilisation du service IGC comme requises par l'ETSI sont décrites dans la présente PC aux paragraphes : 1.4, 4.4, 4.5.2, 4.9.6, 5.5, 9, 9.6, 9.7, et 9.8.

2.3 Délais et fréquences de publication

Les informations identifiées au 2.2 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.

2.4 Contrôle d'accès aux informations publiées

Le SP s'assure que les informations sont disponibles et protégées en intégrité contre les modifications non autorisées. L'AC s'assure que toute information conservée dans une base documentaire de son IGC et dont la diffusion publique, ou la modification n'est pas prévue, est protégée.

L'ensemble des informations publiques et publiées (*Se reporter au § 2.2*) est libre d'accès en lecture et téléchargement sur Internet et dans un langage compréhensible.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Les identités utilisées dans un certificat sont conformes au RFC 5280, le fournisseur (*Issuer*) et le porteur (*subject*) sont identifiés par un Distinguished Name (*DN*).

Les attributs du DN sont encodés en « printableString » ou en « UTF8String » à l'exception des attributs emailAddress qui sont en « IA5String ».

3.1.1.1 Certificat d'AC

L'identité des AC dans les certificats est décrite au chapitre 10 ci-dessous.

3.1.1.2 Certificat Porteur

L'identité du porteur dans le certificat est décrite au chapitre 10 ci-dessous.

3.1.2 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.

3.1.2.1 AC

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

3.1.2.2 Porteur

Dans tous les cas, l'identité du Porteur (*Se reporter au § 3.1.1*) est construite à partir d'au moins un des noms et prénoms de son état civil tel que portés sur un document officiel d'identité.

L'AE est seule responsable de la définition de l'identité du Porteur à mettre dans le Certificat.

Seul des Certificats qui contiennent le nom de l'AE ou AED, qui a enregistré le Porteur, dans le champ « OU » du DN (*Cf. chapitre 10 pour les Certificats Porteurs*) peuvent être émis par l'AC.

3.1.3 Pseudonymisation des porteurs

3.1.3.1 AC

L'identité utilisée pour les certificats d'AC n'est ni un pseudonyme ni un nom anonyme (*Cf. § **Error! Reference source not found.**)*.

3.1.3.2 Porteur

L'identité utilisée pour les certificats de Porteurs n'est ni un pseudonyme ni un nom anonyme (*Se reporter au § 3.1.2*).

3.1.4 Règles d'interprétation des différentes formes de noms

Les UC peuvent se servir de l'identité incluse dans les certificats (*Se reporter au 3.1.1*) afin d'authentifier les Porteurs et l'AC. Pour le Porteur, le champ « CN » n'est pas garanti unique.

3.1.5 Unicité des noms

3.1.5.1 AC

Les identités des certificats (*Cf. § 3.1.1*) sont uniques au sein du domaine de certification de l'AC. La PMA assure cette unicité au moyen de son processus d'enregistrement.

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.

3.1.5.2 Porteur

Les identités portées par l'AC dans les Certificats (*Se reporter au § 3.1.1*) sont uniques au sein du domaine de certification de l'AC. Durant toute la durée de vie de l'AC, une identité attribuée à un Porteur (*Se reporter au 3.1.1.2*) de Certificat 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.

L'AE assure cette unicité au moyen de son processus d'enregistrement et de la valeur unique de l'Identifiant de Transaction attribué à un Porteur via le Connecteur Client et contenu dans le champ OU du Certificat Porteur (*se reporter au § 3.1.1.4*). Un Identifiant de transaction est associé au Porteur par l'AE pour chaque Transaction et donc pour chaque Certificat associé à la Transaction (*Cf. PSGP*).

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.

3.1.6 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.

L'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par la communauté d'utilisateur et les Clients des marques déposées, des marques notoires et des signes distinctifs, ainsi que des noms de domaine.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

3.2.1.1 AC

La preuve de la possession de la clé privée par les composantes de l'Infrastructure de Gestion de Clés et par l'AC est réalisée par les procédures de génération (*Cf. § **Error! Reference source not found.***) de la bi-clé privée correspondant à la clé publique à certifier, l'audit réalisé par la PMA sur l'AC à certifier et le mode de transmission de la clé publique (*Cf. § 6.1.3*) de l'ACI ou l'ACR qui signe les AC.

3.2.1.2 Porteur

La preuve de la possession de la clé privée par le Porteur est réalisée par les procédures de génération de la clé privée (*se reporter au § 6.1.1 ci-dessous*) correspondant à la clé publique à certifier et par le mode d'activation et

de gestion de la clé privée Porteur (*se reporter au § 6.2 ci-dessous*) via le Protocole de Consentement choisit par le Client.

3.2.2 Validation de l'identité d'un organisme

L'AC ne met aucune information liée à l'entité légale du Porteur dans le Certificat.

L'AC ne met que le nom de l'entité légale qui est AE dans un champ OU du DN du Porteur.

L'AE est authentifiée par l'AC durant la phase de contractualisation avec l'AE.

3.2.3 Validation de l'identité d'un individu

3.2.3.1 Porteur

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*).

L'enregistrement d'un Utilisateur (*identification et authentification*) est effectué par l'AE directement avant d'émettre un Certificat.

Les règles d'identification et d'authentification sont laissées à la charge de l'AE qui doit les définir, et les faire approuver par la PMA, pour les Porteurs qu'elle gère.

Le Porteur doit être authentifié en utilisant un titre officiel d'identité tel que passeport, carte nationale d'identité, titre de séjour ou permis de conduire délivré depuis le 01/03/2006 au format « Carte de crédit » avec une photo et des sécurités d'impression comme décrit ici : http://www.consilium.europa.eu/prado/en/prado-documents/AUT/F/docs-per-category.html.

Les règles particulières ci-dessous doivent être implémentées par le Client en fonction de son choix d'OID pour les Porteurs qu'il gère.

3.2.3.1.1 OID: 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

L'AE doit effectuer l'authentification de l'identité du Porteur, en vertu des règles de l'AE et répondre aux exigences définies contractuellement par l'AC et certifiées conformes par rapport à l'ETSI 319 411-2. L'authentification initiale est utilisée pour collecter l'identité, l'adresse électronique et le numéro de téléphone du Porteur. L'enregistrement initial est également utilisé pour distribuer de manière sécurisée les moyens d'authentification sécurisés au Porteur pour accéder à distance au portail de l'AE si l'AE a une telle fonction.

L'AE vérifie au moment de l'authentification initiale, par les moyens appropriés et conformément à la législation nationale, l'identité et, le cas échéant, les attributs spécifiques de la personne à laquelle un certificat qualifié est délivré. Cette vérification est effectuée au choix :

a) Par la présence en personne de la personne physique.

b) À distance, à l'aide de moyens d'identification électronique pour lesquels, avant la délivrance du certificat qualifié, la personne physique s'est présenté en personne et qui satisfont aux exigences énoncées à l'article 8 en ce qui concerne les niveaux de garantie substantiel et élevé.

c) Au moyen d'un certificat de signature électronique qualifié ou d'un cachet électronique qualifié délivré conformément au point a) ou b).

d) À l'aide d'autres méthodes d'identification reconnues au niveau national qui fournissent une garantie équivalente en termes de fiabilité à la présence en personne. La garantie équivalente est confirmée par un organisme d'évaluation de la conformité.

e) En utilisant un PVID.

Des preuves doivent être fournies :

- Nom complet (*y compris le nom de famille et les prénoms compatibles avec les pratiques nationales d'identification*).
- 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.

Si la preuve est fournie par un document d'identité reconnu à l'échelle nationale, l'AE doit vérifier que ce document est toujours valide et authentique.

3.2.3.1.2 OID: 1.3.6.1.4.1.22234.2.8.3.9 et 1.3.6.1.4.1.22234.2.14.3.32

L'AE doit collecter soit ; des preuves directement auprès du Porteur ou des attestations provenant de sources autorisées et appropriées, de l'identité du Porteur et, si besoin est, tout attribut spécifique du Porteur à qui un certificat qualifié sera émis. Les preuves soumises peuvent être au format électronique ou papier. Les vérifications de l'identité du Porteur doivent être effectuées au moment de l'enregistrement, par des moyens appropriés en fonction de la loi nationale de l'AE.

Pour le Porteur, les preuves suivantes doivent être apportées :

- Identité complet (*incluant le prénom et le nom tel qu'officiellement enregistré suivant la loi applicable et les pratiques d'identification nationale*).
- Date et lieu de naissance, un numéro national d'identité reconnu, ou tout autres attributs qui peuvent être utilisé, autant que possible, pour distinguer des personnes entre elles qui ont la même identité.

Il est recommandé que le lieu de naissance soit donné et vérifié conformément aux méthodes nationales définies pour enregistrer les naissances.

3.2.4 Informations non vérifiées du Porteur

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

3.2.5 Validation de la capacité du demandeur

La validation de la capacité d'un Porteur correspond à la validation de l'appartenance à une organisation (*se reporter au § 3.2.2 ci-dessus*).

Un Certificat issu par l'AC, contenant une affiliation implicite ou explicite du Porteur, est en ce cas émis suivant les exigences du chapitre 3.2.2.

3.2.6 Critère d'interopérabilité

Un porteur qui obtient un certificat émis par l'AC à la garantie d'être authentifiable dans le domaine de confiance CDS d'Adobe et AATL.

Les Certificats délivrés par l'AC sont gérés suivant les règles définies dans la présente PC et les procédures définies par le Client en conformité avec l'ETSI.

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

3.3.1 Identification et validation pour un renouvellement courant

3.3.1.1 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 (*Cf. § 3.2*). Dans tous les cas, la procédure d'authentification est conforme à la procédure initiale (*Cf. § 3.2*).

3.3.1.2 Porteur

Pour ce paragraphe, le Porteur est déjà enregistré par l'AE et un premier Certificat lui a été délivré avec succès. Par conséquent, l'AE peut définir un processus de délivrance des Certificats suivants pour le même Porteur. Mais dans ce cas, comme l'ensemble des informations importantes utilisées initialement pour enregistrer le Porteur peuvent toujours être encore valides, l'AE peut vouloir éviter de recommencer le processus complet d'enregistrement du Porteur comme décrit au paragraphe 3.2 ci-dessus.

Ce paragraphe traite donc d'un nouveau Certificat avec une nouvelle bi-clé pour le Porteur (*Cf. § 4.7*).

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.

Les règles de vérification d'identité du Porteur sont laissées à la charge de l'AE, qui a la charge de la gestion du Porteur pour l'opération de renouvellement.

La procédure d'identification, d'authentification et de validation d'une demande de délivrance d'un nouveau Certificat est décrite dans la [PSGP], dans le Protocole de Consentement utilisé pour chaque Client pour leur Porteurs, et est complétée par la procédure d'enregistrement et la Politique de signature définie pour l'AE en fonction du métier du Client.

La méthode d'attribution de cette identité pour un nouveau Certificat est donc définie par le Client, qui enregistre l'ensemble de ses Porteurs avec leurs données d'identification et leurs données d'authentification.

Les règles particulières ci-dessous doivent être mises en œuvre par le client selon son choix OID.

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 (*voir la section 3.1.1 ci-dessus*) ont changées alors l'enregistrement doit être réalisé avec la procédure telle que définie à l'article 3.2 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.

3.3.2 Identification et validation pour un renouvellement après révocation

3.3.2.1 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 (*se reporter au § 3.2*).

3.3.2.2 Porteur

Les mêmes procédures que celles décrites au § 3.2 s'appliquent.

L'AE documente les règles pour le renouvellement de Certificat en fonction des cas de révocation.
Un renouvellement en ce cas aussi nécessite une nouvelle bi-clé et un nouveau Certificat.

3.4 Identification et validation d’une demande de révocation

3.4.1.1 AC

Les demandes de révocation sont authentifiées par la PMA. La procédure de vérification est identique à celle utilisée pour l'enregistrement initial (Cf. § 3.2).

3.4.1.2 Porteur

L’AE authentifie les Porteur selon une procédure qui est approuvée par DocuSign France.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

L'objet du chapitre 4.1, 4.2 et 4.3 est de décrire le processus de demande d'un premier certificat. La gestion des certificats suivants sont décrits dans les chapitres 4.6, 4.7 et 4.8.

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

4.1.1.1 AC

Une demande de certificat d'AC est effectuée par la PMA.

4.1.1.2 Porteur

La demande de Certificat est assimilée à une demande de signature de Document via une Transaction.
Elle est effectuée conformément à la politique de signature et d'enregistrement mise en œuvre par l'AE.
L'AE est responsable de la demande de certificat.

4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

4.1.2.1 AC

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 (*Cf. § 6.1.1*).

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

4.1.2.2 Porteur

La demande de certificat contient les informations suivantes :

- Dans tous les cas, le Porteur fournit une adresse physique, ou une autre donnée (*adresse de courrier électronique*), qui permet à l'AE de le contacter.
- Le numéro de série de la pièce d'identité officielle contenant le nom et prénom et la date de naissance du Porteur, le type de pièce d'identité officielle, les dates de début et de fin de la validité de la pièce d'identité du Porteur et le pays d'émission de la pièce d'identité officielle.
- L'ensemble des informations nécessaires pour construire son identité (Cf. § 3.1.1) en conformité avec la loi et les pratiques d'identification du pays d'appartenance de l'AE.

4.1.2.2.1 OID 1.3.6.1.4.1.22234.2.8.3.9 et 1.3.6.1.4.1.22234.2.14.3.32

En plus des informations décrites ci-dessus, la demande de certificat contient les informations suivantes :

- Identité de l'AE et le cas échéant de l'AED.
- L'AE ou l'AC fait accepter les CGU par le Porteur avec une case à cocher dans le portail de l'AE ou la page de Protocol de consentement.

4.1.2.2.2 OID 1.3.6.1.4.1.22234.2.14.3.7, 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

En plus des informations décrites ci-dessus, la demande de certificat contient les informations suivantes :

- Identité de l'AE et le cas échéant de l'AED ou du PVID.
- Le numéro de téléphone portable du Porteur.

4.2 Traitement d'une demande de certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

4.2.1.1 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.

4.2.1.2 Porteur

La demande est authentifiée (*se reporter aux § 3.2.2 et le 3.2.5*) et validée par l'AE.

L'AE identifie et authentifie le Porteur (*Cf. § 3.2.2 et le 3.2.5*).

4.2.2 Acceptation ou rejet de la demande

4.2.2.1 AC

La PMA autorise ou rejette la création d'un certificat AC.

4.2.2.2 Porteur

L'AE est responsable de l'approbation de la demande de Certificat Porteur.

En cas d'approbation de la demande, l'AE transmet la demande à l'AC dans le cadre d'une transaction décrite dans la politique de signature du Client et la PSGP.

En cas de rejet de la demande, l'AE en informe le Porteur (*en fonction de l'origine de la demande*) en justifiant le rejet.

4.2.3 Durée d'établissement du certificat

4.2.3.1 AC

La durée du traitement d'une demande de certificat par la PMA est définie par la PMA.

4.2.3.2 Porteur

La durée du traitement est liée au processus de signature électronique et est immédiate suite à l'acceptation de la demande de signature.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

4.3.1.1 AC

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

Les ACs sont générées pendant une cérémonie des clés (se reporter au § 6.1) dans les locaux de l'OT.

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. 6.1.1 et 6.2.8*).

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. § 6.2.9*) et sont transférées dans la ressource cryptographique (*HSM*) de production (*Cf. 6.2.6*).

4.3.1.2 Porteur

L'AE transmet la demande technique de certificat à l'AC contenant les informations du Porteur (*nom, prénom, optionnellement adresse de courrier électronique et numéro de téléphone*) et les données à signer par le Porteur.

Le Porteur déclenche l'utilisation de sa bi-clé dans l'Application « Protect and Sign - Personal Signature » suivant le Protocole de consentement, choisi par le Client et décrit dans la politique de signature, en utilisant la Donnée d'activation Porteur. Le Protocol de Consentement doit permettre au Porteur de vérifier ses informations d'identité (*Cf. § 3.1.1*) avant d'accepter ou de refuser de signer.

L'AC ou l'AE authentifie le Porteur en utilisant les Données d'activation que le Porteur soumet lors du Protocole de consentement (*Cf. § 6.2.8*) et conformément à la Politique d'Enregistrement de l'AE.

La bi-clé du Porteur est utilisée par l'Application « Protect and Sign - Personal Signature » pour signer une CSR (*Pkcs#10*) afin de transmettre la clé publique à certifier à l'AC (*Cf. § 6.1.3*).

L'AC signe le certificat.

L'opération de signature est effectuée sur le Document à signer conformément à la Transaction décrite dans la politique de signature, la [PSGP] et la Politique d'Enregistrement. À la suite de l'opération de signature, l'Application « Protect and Sign - Personal Signature » détruit la bi-clé du Porteur (*Cf. § 6.2.10*).

L'Application « Protect and Sign - Personal Signature » transmet le Document signé, et donc le Certificat, à l'AE [PSGP].

Les communications, entre les différentes composantes de l'AC citées ci-dessus, sont authentifiées et protégées en intégrité et confidentialité.

4.3.1.2.1 OID 1.3.6.1.4.1.22234.2.8.3.7 ,1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

Si le Porteur accepte de signer le Document, alors il confirme ce choix à l'AE en utilisant les procédures et moyens de l'AE (*click sur l'écran*, *etc*) et durant un face à face ou une authentification PVID (*Cf. § 4.2*).

4.3.1.2.2 OID 1.3.6.1.4.1.22234.2.8.3.9 et 1.3.6.1.4.1.22234.2.14.3.32

Si le Porteur accepte de signer le Document, alors il confirme ce choix à l'AE en utilisant les procédures de l'AE (*click sur l'écran, etc*) et ses moyens.

4.3.2 Notification par l'AC de la délivrance du certificat au porteur

4.3.2.1 AC

La notification est effectuée à la fin de la cérémonie des clés de l'AC. Les certificats d'AC sont remis à la PMA.

4.3.2.2 Porteur

Non applicable.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

4.4.1.1 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.

4.4.1.2 Porteur

Le Client doit rendre disponible le Document au Porteur.

Le Client et le Porteur peuvent ensuite vérifier le contenu du certificat (*notamment les informations qui composent son identité cf. 3.1.1*). Si le Client ou le Porteur n'informe pas l'AE d'une anomalie dans le certificat, alors le certificat est considéré comme accepté. Si une anomalie est présente dans le Certificat, alors l'AE doit être alertée par la personne qui a fait le control (*l'AE ou le Porteur*).

4.4.1.2.1 OID 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

L'acceptation du Certificat est réalisée par l'AE et le Porteur en vérifiant les informations de la signature et du Document.

4.4.1.2.2 OID 1.3.6.1.4.1.22234.2.8.3.9 et 1.3.6.1.4.1.22234.2.14.3.32

L'acceptation du Certificat est réalisée par le Porteur en vérifiant les informations de la signature et du Document.

4.4.2 Publication du certificat

4.4.2.1 AC

Le certificat de l'AC est publié par le SP.

4.4.2.2 Porteur

Les Certificats ne sont pas publiés après leur émission.
Le Certificat tout comme l'ensemble des certificats d'AC du chemin de certification sont contenus dans le Document signé (*Cf. § 2.2*).
Un UC peut donc valider un certificat en validant la signature d'un Document signé (*comme indiqué dans la PSGP*).

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

4.4.3.1 AC

En cas de besoin, la PMA est responsable des communications de certificat d'AC aux entités externes.

4.4.3.2 Porteur

La notification de l'émission d'un Certificat est assimilée à l'accusé de réception (Cf. PSGP) et la communication du Document signé au Porteur par le Client.

4.5 Usage de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation des bi-clés et des certificats est définie au § 1.4 ci-dessus. L'usage d'une bi-clé et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés (*se reporter au § **Error! Reference source not found.***).

4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

L'utilisation des certificats par les UC est décrites dans les paragraphes 1.4 et 3.1.4 ci-dessus. La clé privée du porteur ne peut être utilisée que pour une opération de signature de contrat ou d'acte de gestion comme indiqué au § 1.4 en fonction du type de certificat. Un UC qui utilise le Certificat s'assure qu'il connaît la Politique de signature du Client afin de valider correctement les Certificats et les identités des Porteurs et l'ensemble des informations contenus dans le Certificats (*OIDs, key usage, etc*).

4.6 Renouvellement d'un certificat

Cette section concerne le processus de renouvellement du certificat, sans que les clés publiques ou toute autre information incluse dans les certificats soient modifiées. Seule la période de validité et le numéro de série changent.

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.

4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

Cette section concerne la génération d'un nouveau certificat avec changement de la clé publique associée.

Le changement de la clé publique d'un certificat implique la création d'un nouveau certificat.

4.7.1 AC

Dans ce cas la procédure à appliquer pour renouveler un certificat d'AC est identique à celles décrites pour la délivrance du premier certificat d'AC (*se reporter au § 3.3, § **Error! Reference source not found.**, § 4.2 et § 4.3 ci-dessus*).

4.7.2 Porteur

Dans ce cas la procédure à appliquer pour renouveler un Certificat est identique à celles décrites pour la délivrance du premier Certificat (*se reporter au § 3.3, § **Error! Reference source not found.**, § 4.2 et § 4.3 ci-dessus*).

4.8 Modification du certificat

Cette section concerne la génération d'un nouveau certificat avec conservation de la même clé. Cette opération est rendue possible uniquement si la clé publique réutilisée dans le certificat est toujours conforme aux recommandations de sécurité cryptographique applicables en matière de longueur de la clé.

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.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

Les certificats 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 la PMA.

4.9.1.1 Certificat Composante IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC :

- Suspicion de compromission, compromission avérée, perte ou vol de la clé privée de la composante.
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (*par exemple, suite à un audit de qualification ou de conformité négatif*).
- L'AC perd son droit d'émettre des Certificats.
- Cessation d'activité de l'entité opérant la composante décidée par la PMA.

4.9.1.2 Certificat Porteur

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

- L'AC est révoquée.
- Le DN (*Cf. 3.1.1*) 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.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat composante IGC

La PMA ou une autorité judiciaire via une décision de justice est à l'origine de la demande de révocation des certificats d'AC. L'AC est à l'origine de la demande de révocation des certificats de composantes d'IGC.

4.9.2.2 Certificat porteur

Le Porteur peut demander la révocation pour les raisons suivantes :

- Le DN (*Cf. 3.1.1*) est non correctement rempli.
- La clé privée du Porteur est compromise ou suspectée d'être compromise.

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

- Le DN (*Cf. 3.1.1*) 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 (*Cf. 3.1.1*) 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.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat composante IGC

La DPC précise les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC. La PMA autorise les opérations de révocation en signant une demande de révocation.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC 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, l'IGC pourra par exemple envoyer des alertes au Client et aux AE.

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 la ou des composantes de l'IGC.

Le point de contact identifié sur le site : http://www.ssi.gouv.fr doit être immédiatement informé 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.

4.9.3.2 Certificat porteur

La demande de révocation est conservée par l'AE dans ses journaux.

La demande de révocation est authentifiée conformément au § 3.4.

L'AE transmet la demande de révocation à l'AC.

L'AC authentifie l'AE et vérifie que la demande provient effectivement d'une AE autorisée par l'AC.

L'AC révoque le certificat du porteur en incluant le numéro de série du certificat dans la prochaine LCR qui sera émise par l'AC.

Le demandeur de la révocation est informé de la révocation effective du certificat porteur. De plus, si le porteur du certificat n'est pas le demandeur, le porteur est également informé de la révocation effective du certificat.

Dans le cas d'un porteur au sein d'une Entreprise ou d'une Administration, l'organisation d'appartenance (*se reporter § 3.2.2*) est informée de la révocation des certificats des porteurs qui lui sont rattachés.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

4.9.4.1 AC

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 § **Error! Reference source not found.** et la révocation est effectuée dans un délai de 10 jours ouvrés maximum.

4.9.4.2 Porteur

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.

4.9.5 Délai de traitement par l'AC d'une demande de révocation

4.9.5.1 Certificat Composantes IGC

La révocation est effectuée dans un délai de 10 jours ouvrés maximum.

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.

La révocation d'un certificat de signature de l'AC (*signature de certificats, de LCR/LAR et/ou de réponses OCSP*) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

4.9.5.2 Certificat Porteur

Le service de révocation est disponible 24 heures sur 24 et 7 jours sur 7.

Une demande de révocation, authentifié et dûment établie par l'AE, de Certificat est traitée dans un délai inférieur à 24 heures.

Les CRL émises par les AC « Cloud Signing Personal Signature CA » et « DocuSign Premium Cloud Signing CA – SI1 » contienent l'extension « ExpiredCertsOnCRL » avec la date pour « start date » correspondante à la date et l'heure du plus ancien certificat de AC.

4.9.6 Exigences de vérification de révocation pour les utilisateurs de certificats

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 (*Cf. § 4.9.9*).

L'usage de Certificat révoqué peut avoir 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 « Cloud Signing Personal Signature CA » et « DocuSign Premium Cloud Signing CA – SI1 » contient les certificats expirés et révoqués et contient l'extension « expiredCertsOnCRL ».

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 24 heures.

Cette différence d'état ne peut durer qu'au maximum 24 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.

4.9.7 Fréquences d'établissement des LCR

La LCR signée, qui a une validité de 6 jours, par l'AC est émise toutes les 24 Heures.

La CRL contient les certificats expirés révoqués pour les certificats qualifiés seulement.

La dernière LCR émise par les AC « Cloud Signing Personal Signature CA » et « DocuSign Premium Cloud Signing CA – SI1 » est publiée avec une fin de validité positionnée au 31 décembre 9999, 23h59m59s (« *99991231235959Z* »).

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.

4.9.8 Délai maximum de publication d' une LCR

Le délai maximum de publication d'une LCR est de 24H00.

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

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.

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

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: 1440 minutes (24h) Hold: 1440 minutes (24h) Revoked: 4320 minutes (72h) 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.

Field	Requirements
extensions	No extension referenced

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats d'AC la révocation à la suite d'une compromission de sa clé privée fait l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (*autres sites Internet institutionnels, journaux, etc*).

En cas de compromission de clés Porteurs, l'AC avertit le Client qui décide du plan d'action auprès des Porteurs.

4.9.13 Causes possibles d'une suspension

Sans objet.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

Le service OCSP est mis à jour à partir de la base de données de l'AC. Cependant le mécanisme principal de communication du statut des certificats est la LCR publiée par l'AC. Dans tous les cas, les utilisateurs de certificats peuvent utiliser un mécanisme de consultation libre de LCR.

4.10.2 Disponibilité de la fonction

Le service OCSP est mis à jour à partir de la base de données de l'AC. Le service OCSP et CRL est disponible 24 heures sur 24 et 7 jours sur 7 suivant un taux de disponibilité de 99,9.

Le service OCSP est coupé après la fin de vie de l'AC et seule la dernière LCR est la seule information disponible cf. 4.9.7.

4.11 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.

4.12 Séquestre de clé et recouvrement

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

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physiques

5.1.1 Situation géographique et construction des sites

Le site d'exploitation de l'OSC hébergeant l'AC, l'AE et le SP respecte les règlements et normes en vigueur et son installation tient compte des résultats de l'analyse de risques, du métier d'opérateur de certification selon la méthode EBIOS, par exemple certaines exigences spécifiques de type inondation, explosion (*proximité d'une zone d'usines ou d'entrepôts de produits chimiques, etc*) réalisées par l'OSC.

Le site d'exploitation (*protégé par des gardes ou des détecteurs d'intrusion, etc*) fournit une protection robuste contre les accès non autorisés aux équipements et données de l'AC, l'AE et le SP.

5.1.2 Accès physique

Les équipements de l'AC et de l'AE sont protégés contre les accès non autorisés et les tentatives d'endommagement. La protection physique permet d'assurer à minima les points suivants :

- La surveillance, manuelle ou électronique, des accès autorisés et non autorisés tout le temps.
- 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 personnes non autorisées sont toujours accompagnées par des personnes autorisées dans les locaux.
- Un journal des accès est maintenu et est périodiquement revu.
- Au moins deux niveaux de barrières 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 de l'AC et aux HSM, et leurs données d'activation, requière deux personnes physiques distinctes.

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 modules cryptographiques amovibles doivent être désactivés avant leur stockage.

Lorsqu'ils ne sont pas utilisés, les HSM les données d'activation associées sont placés dans des conteneurs sécurisés (*coffre, etc*).

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

5.1.3 Alimentation électrique et climatisation

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

5.1.4 Vulnérabilité aux dégâts des eaux

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.

5.1.5 Prévention et protection incendie

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 l'AC et l'AE dans la présente PC, en matière de disponibilité de ses fonctions.

5.1.6 Conservation des supports

Les différentes informations intervenant dans les activités de l'IGC sont identifiées et leurs besoins de sécurité définis (*en confidentialité, intégrité et disponibilité*).

L'AC maintient un inventaire de ces informations. L'OCS met en place des mesures pour éviter la compromission et le vol de ces informations. Les supports (*papier, disque dur, disquette, CD, etc.*) correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité.

En particulier, ils sont manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion protègent ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'OCS s'engage à conserver les informations qu'ils contiennent.

5.1.7 Mise hors service des supports

En fin de vie, les supports seront soit détruits soit réinitialisés en vue d'une réutilisation.

5.1.8 Sauvegardes hors site

L'AC réalise des sauvegardes hors site permettant une reprise rapide des services de l'AC à la suite de la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ses services. Cette sauvegarde est effectuée de manière régulière suivant la politique de DocuSign France.

L'OSC utilise des locaux qui suivent les règles de sécurité de DocuSign France et permettant la protection des données et matériels stockés hors site.

Les sauvegardes hors sites sont testées.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

Les rôles de confiance de l'AC sont conformes et similaires aux rôles définis par l'ETSI.

Pour l'OID 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31, le logiciel PSM software doit implémenter les rôles conformément à [PSM QSCD].

Le Client est responsable de définir et documenter les rôles de confiance et les opérations associées pour les services de l'AE et des AED.

5.2.2 Nombre de personnes requises par tâches

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Les clés d'AC sont sous double contrôle minimum.

Les tâches suivantes sont réalisées sous double control :

- Génération de clé d'AC.
- Activation de clé d'AC.
- Sauvegarde de clés d'AC.
- Révocation de certificat d'AC.

Le nombre de personnes requises par tâche est précisé dans la DPC.

Pour l'OID 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31, le logiciel PSM software doit implémenter les rôles conformément à [PSM QSCD].

Le Client doit documenter les règles de séparation des rôles afin que la PMA puisse juger de la sécurité de l'organisation des AE et des AED.

5.2.3 Identification et authentification pour chaque rôles

L'AC fait vérifier l'identité et les autorisations de tout membre de son personnel qui est amené à mettre en œuvre les services de l'IGC avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle.
- Que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes.
- Le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes.
- Éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu au sein de l'IGC.

Ces contrôles sont décrits dans la DPC et sont conformes à la politique de sécurité de l'AC.

Chaque attribution d'un rôle à un membre du personnel de l'IGC lui est notifiée par écrit ou équivalent.

Pour l'OID 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31, le logiciel PSM software doit implémenter les rôles conformément à [PSM QSCD].

Le Client doit documenter les règles de sécurité pour l'authentification et l'identification des rôles de confiance qui interviennent dans l'AE.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et les exigences de non-cumuls définis dans la DPC doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC. Les personnels de l'OSC en charge de la gestion des certificats doivent être différents des personnels en charges des aspects commerciaux et de la conformité (*prise de décision d'arrêt d'une composante par exemple*) et donc libre de toute pression et de conflit d'intérêts qui pourraient influencer la confiance dans les opérations qu'ils mènent.

Pour l'OID 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31, le logiciel PSM software doit implémenter les rôles conformément à [PSM QSCD].

Le Client doit documenter les règles de séparation des rôles afin que la PMA puisse juger de la sécurité de l'organisation des AE.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Chaque personne amenée à travailler au sein de l'IGC est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles. Les personnels doivent être formés pour les rôles qu'ils occupent. Les rôles et leurs missions sont documentés afin de bien gérer la séparation des rôles et l'affectation de personne en fonction de la sensibilité des rôles en fonction de leurs compétences, du contrôle des antécédents et de leurs formations. La PMA approuve les affectations de rôles. Le Client a la responsabilité de l'affectation des rôles pour l'AE.

Toute personne intervenant dans les procédures de certification de l'IGC est informée de ses responsabilités relatives aux services de l'IGC et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 Procédures de vérification des antécédents

L'IGC met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification est basée sur un contrôle des antécédents des personnes, il est vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflits d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (*au minimum tous les 3 ans*).

5.3.3 Exigences en matière de formation initiale

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondants à la composante au sein de laquelle il opère.

Cette formation couvre les aspects suivants :

- Règles de sécurité et principes de l'IGC.
- Logiciels d'IGC en fonction de leur version.
- Procédures applicables pour les services de l'IGC.
- Responsabilités du rôle.
- Procédures pour la résolution des incidents et des litiges.
- Connaissance minimale du système informatique de l'IGC.
- Procédure du plan de continuité.

Le personnel a eu connaissance et compris les implications des opérations dont il a la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

5.3.5 Fréquence et séquence de rotation entres différentes attributions

La PMA et l'OSC s'assure que les changements de rôles n'affectent pas la sécurité des services de l'IGC.

5.3.6 Sanctions en cas d'actions non autorisées

Les sanctions adéquates sont appliquées pour les personnels de l'IGC ne respectant pas les règles de sécurité de la PC de DocuSign France.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Les exigences concernant les personnels contractants sont les mêmes que celle décrites pour les employés dans ce chapitre 5.3.

5.3.8 Documentation fournie au personnel

Les documents nécessaires à la réalisation des services de l'IGC en fonction du rôle occupé sont fournis au personnel de l'IGC (*Cf. § 5.3.3*).

5.4 Procédures de constitution des données d'audit

5.4.1 Type d'événements à enregistrer

Les journaux et traces d'audit sont générés par l'OSC et la PMA pour les évènements liés à la sécurité et aux services de l'IGC.

La journalisation d'événements consiste à enregistrer les évènements manuellement ou électroniquement par saisie ou par génération automatique. Les fichiers résultants, sous forme papier et/ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

L'OSC journalise les évènements concernant les systèmes liés aux fonctions qu'elles mettent en œuvre dans le cadre de l'IGC :

- Création / modification / suppression de comptes utilisateur (*droits d'accès*) et des données d'authentification correspondantes (*mots de passe, certificats, etc.*).
- Démarrage et arrêt des systèmes informatiques et des applications.
- Évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises à la suite d'une défaillance de la fonction de journalisation.
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes.

D'autres évènements sont également recueillis.

Il s'agit d'évènements concernant la sécurité qui ne sont pas produits automatiquement par les systèmes mis en œuvre :

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

En plus de ces exigences de journalisation communes à toutes les composantes et à toutes les fonctions de l'IGC, des évènements spécifiques aux différentes fonctions de l'GC sont également journalisés par l'OSC :

- Réception d'une demande de certificat (*initiale et renouvellement*).
- Validation/rejet d'une demande de certificat.
- Évènements liés aux clés d'AC et aux certificats d'AC (*génération (cérémonie des clés), sauvegarde / récupération, destruction, etc*).

- Gestion des HSM.
- Génération des Certificats de Porteurs.
- Génération, utilisation et destruction des bi-clés de Porteurs.
- Renouvellement et révocation des Certificats Porteurs.
- Transmission des Certificats contenus dans le Document comme indiqué dans la PSGP.
- Publication et mise à jour des informations liées à l'AC.
- Génération d'information de statut d'un Certificat (*Porteur*).

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

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

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée.

Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements.

En plus de la liste ci-dessus, l'AE enregistre les informations suivantes avec le détail demandé ci-dessus :

- Les dossiers Porteurs (*Cf. § 4.1 et § 4.2*) et les informations de contacts du Porteur (*adresse de courrier électronique ou numéro de téléphone*) qui permette de vérifier l'identité du Porteur (*Cf. § 3.2, § 4.1 et § 4.2*).
- La liste des Opérateur d'AE.
- Les pages techniques du Protocole de consentement.
- Si le Client a choisi de conserver lui-même le Fichier de preuve (*qui est la trace de demande de Certificat entre l'AE et l'AC*), alors il conserve le Fichier de preuve suivant ses propres moyens de conservation (*Cf. PSGP*). Sinon c'est DocuSign France qui conserve le Fichier de preuve chez un prestataire d'archivage électronique dans un compartiment dédié au Client (*Cf. PSGP*).

5.4.2 Fréquence de traitement des journaux d'événements

Les journaux d'audits des composantes d'IGC sont revus sur une base annuelle par le responsable de l'audit de l'OSC qui conduit une recherche raisonnable de preuve d'éventuelle activité malicieuse et de suivit des opérations sensibles.

Un échantillon significatif des traces d'audits générées par les composantes d'IGC depuis la dernière revue est examiné (*où les intervalles de confiance pour chaque catégorie de données d'audit de sécurité sont déterminés par les liens de sécurité des types de données et la disponibilité d'outils pour effectuer un tel examen*) aussi pour la recherche raisonnable de preuve d'éventuelle activité malicieuse.

L'OSC procède à une revue des journaux d'audits IT et physique quotidienne.

L'OSC explique les évènements significatifs dans un rapport d'audit.

Une telle revue implique de vérifier que les logs n'ont pas été altéré, qu'il n'y a pas de discontinuité ou de perte dans les journaux.

Cette revue peut être rapide et synthétique afin de rechercher des incohérences dans les journaux d'audits.

5.4.3 Période de conservation des journaux d'événements

Les journaux d'évènements sont retenus au moins 1 an sur site avant d'être archivés.

5.4.4 Protection des journaux

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les journaux d'évènements doivent être protégés en disponibilité (*contre la perte et la destruction partielle ou totale, volontaire ou non*).

5.4.5 Procédures de sauvegarde des journaux d'événements

L'IGC mettent en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC et en fonction des résultats de l'analyse de risques de l'AC. Les sauvegardes des journaux sont protégées avec le même niveau de sécurité que les originaux.

5.4.6 Système de collecte des journaux d'événements

Les journaux d'évènement sont créés dès la mise en route d'un système et s'arrête que lorsque le système s'arrête. Le système de collecte des journaux permet de garantir l'intégrité et la disponibilité des journaux d'évènement. Si besoin est, le système de collecte des journaux protège les données en intégrité. Si un problème apparaît pendant la collecte des journaux, la PMA détermine s'il est nécessaire de suspendre les opérations de la ou des composantes impactées avant d'avoir résolu le problème.

5.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement

Quand un évènement est enregistré dans le système de collection des journaux, il est lié à un rôle de l'IGC (*personne ou machine*).

5.4.8 Évaluation des vulnérabilités

Les composantes de l'IGC doivent être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont contrôlés régulièrement afin d'identifier des anomalies liées à des tentatives en échec.

Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués.

Le résumé doit faire apparaître les anomalies et les falsifications constatées.

Pour l'analyse, les règles suivantes s'appliquent :

- Mettre en œuvre des contrôles de détection et de prévention sous le contrôle de l'OSC pour protéger les systèmes IGC contre les virus et logiciels malveillant.
- Documenter et suivre un processus de correction de la vulnérabilité qui traite de l'identification, l'examen, la réponse, et la résolution des vulnérabilités.
- Effectuer une analyse de vulnérabilité :
    - Après tout changement de système ou réseau suivant la décision de la PMA qui décide si les changements sont importants pour les AC et le Client pour l'AE.
    - Au moins une fois par semaine, sur les adresses IP publics et privées identifiées par l'OSC des systèmes de l'IGC (pour l'AC).

- Effectuer un test de pénétration sur les systèmes de l'IGC sur au moins une base annuelle et à la suite d'une modification de l'infrastructure ou des applications qui sont jugées important par la PMA pour l'AC et le Client pour l'AE.
- Enregistrer les preuves de la réalisation des analyses de vulnérabilités et des tests de pénétration.
- Enregistrer les preuves de la réalisation des analyses de vulnérabilités et des tests de pénétration ; par des personnes qualifiées, avec des outils adéquates, et suivant une démarche indépendante afin de garantir la qualité et la pertinence des analyses et des tests.
- Procéder à une veille sur les vulnérabilités et les résoudre en fonction de la politique de sécurité de l'OSC et de l'analyse de risque de l'OSC.

5.5 Archivage des données

5.5.1 Type de données à archiver

L'archivage des données permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC afin de prouver la validité d'une opération d'IGC et d'une signature électronique.

Les données archivées au niveau de chaque composante, sont les suivantes :

- Journaux IGC :
    - Accès physique à l'OSC (*3 mois maximum*).
    - Vidéo pour la protection de l'OSC (*3 mois maximum*).
    - Vidéo de cérémonie des clés (*7 ans minimum après l'expiration du certificat*).
    - Gestion des rôles de confiance (*7 ans minimum après l'expiration du certificat*).
    - Accès aux systèmes d'information (*7 ans minimum après l'expiration du certificat*)
    - Création, utilisation et destruction des bi-clés Porteurs et AC (*7 ans minimum après l'expiration du certificat*).
    - Gestion des données d'activation d'AC (*7 ans minimum après l'expiration du certificat*).
    - Journaux d'activité des systèmes d'information et des réseaux (*7 ans minimum après l'expiration du certificat*).
    - Documentation IGC (*7 ans minimum après l'expiration du certificat*).
    - Incident de sécurité et rapport d'audit (*7 ans minimum après l'expiration du certificat*).
- Documentation relative à l'audit gardé par la PMA (*7 ans minimum après l'expiration du certificat*).
- Document PC (*7 ans minimum après l'expiration du certificat*).
- Document DPC (*7 ans minimum après l'expiration du certificat*).
- Contrat entre DocuSign France et les Clients (*7 ans minimum après l'expiration du certificat*).
- Type d'équipement, logiciel et configuration pour l'AC (*7 ans minimum après l'expiration du certificat*).
- Certificats gardés par l'AC (*7 ans minimum après l'expiration du certificat*).
- Demande de certificats enregistrées par l'AC (*7 ans minimum après l'expiration du certificat*).
- Autres données et applications utilisés pour la vérification des archives (*7 ans minimum après l'expiration du certificat*).
- Tous les journaux relatifs au fonctionnement de la PMA et des audits (*7 ans minimum après l'expiration du certificat*).

L'AE doit conserver ses journaux (*Cf. 5.4.1*) et les Fichiers de preuve pendant 7 ans minimum après l'expiration du certificat.

5.5.2 Période de conservation des archives

La période de conservation des archives est donnée au § 5.5.1 ci-dessus. La PMA et les Clients, selon le propriétaire de l'archive, de garder ou d'effacer les archives à la suite de l'expiration du délai minimal de conservation.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes :

- Seront protégées en intégrité, confidentialité et authenticité.
- Seront accessibles aux seules personnes autorisées.
- Pourront être consultées et exploitées par les personnes autorisées.

5.5.4 Sauvegarde des archives

Si les supports utilisés pour le stockage des archives ne peuvent permettre de conserver les données conformément au délai de rétention définit au § 5.5.1, alors un mécanisme de transfert régulier d'archives sur de nouveau support sera mis en œuvre par l'OSC.

5.5.5 Exigences d'horodatage des données

L'utilisation de contremarque de temps n'est pas obligatoire pour l'IGC pour la protection des journaux. Seul le Fichier de Preuve est horodaté. Les journaux possèdent un temps de confiance délivré suivant les exigences du § 6.8.

5.5.6 Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données (*Se reporter au 5.4.6*).

5.5.7 Procédures de récupération et de vérification des archives

Les archives sont régulièrement testées afin de s'assurer de leur contenu et de leur lisibilité.

Seules les personnes autorisées et la PMA peuvent accéder aux archives.

5.6 Changement de clé d'AC

5.6.1 Certificat d'AC

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.

La durée de vie du certificat d'AC est donnée au § 6.3.

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, la bi-clé d'une AC est renouvelée au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats émis.

Une nouvelle clé d'AC requiert un nouveau certificat d'AC.

Dès qu'une nouvelle clé privée est générée pour l'AC, seule celle-ci est utilisée pour générer de nouveaux Certificats de Porteurs.

Le précédent certificat d'AC reste valable pour valider le chemin de certification des anciens certificats émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les Certificats Porteurs émis à l'aide de cette bi-clé. 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.

Par ailleurs, la PMA se charge de changer la bi-clé d'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.

5.6.2 Certificat de Porteur

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

La durée de validité d'un Certificat est donnée dans la DPC.

5.7 Reprise à la suite de compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

L'AC a établi un plan de continuité de service qui met en évidence les différentes étapes à exécuter dans l'éventualité de la compromission ou de la perte des ressources système, des logiciels et ou des données et qui pourraient perturber ou compromettre le bon déroulement des services d'AC.

Le plan de continuité est régulièrement testé, revu et mis à jour par la PMA.

L'AC a conduit une analyse de risque pour évaluer les risques métier et déterminer les exigences de sécurité et procédures opérationnelles afin de rédiger un plan de reprise d'activité. Les risques pris en compte sont régulièrement revus et le plan est révisé en conséquence. Le plan de continuité de l'AC fait partie du périmètre audité, selon le paragraphe 8 ci-dessous.

Les personnels de l'IGC dans un rôle de confiance sont spécialement entraînés à réagir selon les procédures définies dans le plan de reprise d'activité qui concernent les activités les plus sensibles.

Dans le cas où l'IGC détecte une tentative de piratage ou une autre forme de compromission, la PMA mène une enquête et une analyse de risque afin de déterminer la nature des conséquences et leur niveau. Si l'un des algorithmes, ou des paramètres associés, ou un ou plusieurs des services utilisés par l'IGC ou ses Porteurs devient insuffisant en termes de sécurité pour son utilisation prévue, alors la PMA :

- Informe tous les porteurs et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou à d'autres formes de relations établies. En complément, cette information est mise à disposition des autres utilisateurs de certificats.
- Révoque tous les certificats concernés par l'incident.

Si nécessaire, l'ampleur des conséquences est évalué par la PMA afin de déterminer si les services de l'AC doivent être rétablis, quels certificats porteurs doivent être révoqués, l'AC doit être déclarée compromise, certains services peuvent être maintenus (*en priorité les services de révocation et de publication d'état des certificats porteurs*) et comment, selon le plan de reprise d'activité.

Dans le cas où l'AE ou le Client détecte une tentative de piratage ou une autre forme de compromission, elle mène une enquête et une analyse afin de déterminer la nature des conséquences et leur niveau.

En cas de compromission du Connecteur Client ou d'une possible remise en cause de Documents signés, le Client doit avertir DocuSign France.

L'impact des dégâts est évalué par le Client qui détermine si des Certificats Porteurs doivent être révoqués et les services de l'AE arrêtés ou maintenus.

Le Client avertit dans tous les cas la PMA des incidents de sécurité sur l'AE.

Le plan de continuité du Client et de l'AE est documenté par le Client et l'AE.

L'AC doit également prévenir directement et sans délai le point de contact identifié sur le site : http://www.ssi.gouv.fr. Les vulnérabilités découvertes (*AC, AE, etc*) sont traitées sous 48 heures dès leurs connaissances par la PMA et l'ANSSI et Adobe est alertée par la PMA en 24H00 dès connaissance de l'incident majeure portant atteinte à la sécurité du service ou des données personnelles.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (*matériels, logiciels et / ou données*)

Si le matériel de l'AC est endommagé ou hors service alors que les clés de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des services de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC et du Client.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Si la clé de signature de l'AC est compromise, perdue, détruite, ou soupçonnée d'être compromise :

- La PMA, après enquête sur l'évènement décide de révoquer le certificat de l'AC.
- Tous les Clients dont les certificats ont été émis par l'AC compromise, sont avisés dans les plus brefs délais que le certificat d'AC a été révoqué.
- La PMA décide ou non de générer un nouveau certificat d'AC et une nouvelle bi-clé.
- Une nouvelle bi-clé AC est générée et un nouveau certificat d'AC est émis.
- Les porteurs sont informés de la capacité retrouvée de l'AC de générer des certificats.

Si le système utilisé par « Protect and sign - Personal Signature » pour générer les bi-clés des Porteurs est compromis, alors la PMA alerte les Clients et les Porteurs et donne une liste des conséquences potentielles et des risques pour les Clients et les UC.

Si un des algorithmes cryptographiques, ou des paramètres associés, utilisé par l'AC ou les Porteurs devient insuffisant en termes de sécurité, alors la PMA informe les Clients et change d'algorithme.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Le plan de reprise d'activité après sinistre traite de la continuité d'activité telle qu'elle est décrite au § 5.7.1.

5.8 Fin de vie d'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La PMA doit tenir informées l'ANSSI.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

5.8.1 Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC :

- Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (*notamment, archivage des certificats des porteurs et des informations relatives aux certificats*).
- Assure la continuité de la révocation (*prise en compte d'une demande de révocation et publication des LCR*), conformément aux exigences de disponibilité pour ses fonctions définies dans la PC.

Des précisions quant aux engagements suivants doivent ainsi être annoncées par l'AC dans sa PC :

- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des porteurs ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire.

5.8.2 Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (*par exemple : cessation d'activité pour une famille de certificats donnée seulement*).

La cessation partielle d'activité est progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, assurera la révocation des certificats et la publication des LCR conformément aux engagements pris dans la PC.

L'AC procède aux actions suivantes :

- La notification des Clients affectés.
- Le transfert de ses obligations à d'autres parties.
- La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC :

- S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats.
- Détruit la clé privée de l'AC et ses sauvegardes.
- Prend toutes les mesures nécessaires pour détruire clé privée de l'AC ou la rendre inopérante.
- Révoque son certificat d'AC.
- Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité.
- Publie les informations de révocation les plus à jour au profit des UC.

Dans le cas de l'arrêt de service de l'OSC, l'OSC est responsable de conserver l'ensemble des journaux pertinents concernant les Porteurs et les services d'IGC et de les transférer à la PMA.

5.8.3 Cessation d'activité de l'AE

En cas de fin d'activité du Client en qualité d'AE, le Client doit :

- Informer la PMA suivant les modalités prévues dans le contrat entre DocuSign France et le Client.
- Détruire les clés privées du Connecteur Client et demander leur révocation auprès de DocuSign France.
- L'AE arrête l'utilisation du Service de signature de DocuSign France.

- En cas de compromission de l'AE, alerter les Porteurs et DocuSign France et les UC concernés.
- Les archives doivent être transférées à une entité désignée par l'AE dont l'identité est communiquée à l'AC.

Dans le cas de l'arrêt de service de l'OSC, l'OSC est responsable de conserver l'ensemble des journaux pertinents concernant les Porteurs et les services d'IGC et de les transférer au Client.

6 MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Bi-clés d'AC

À la suite de l'accord de la PMA pour la génération d'un certificat d'AC, une bi-clé est générée lors d'une cérémonie de clé à l'aide d'une ressource cryptographique matérielle (*Cf. 6.2.11*).

Les cérémonies de clés se déroulent sous le contrôle d'au moins trois personnes dans des rôles de confiance (*maître de cérémonie et témoins*) et sont impartiaux. Elle se déroule dans les locaux de l'OSC. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. Les rôles impliqués dans les cérémonies de clés sont précisés dans la DPC.

Les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins deux sont externes à l'AC et sont impartiaux. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. L'ensemble de la cérémonie des clés est enregistré sous vidéo.

À la suite de leur génération, les parts de secrets (*données d'activation*) sont remises à des porteurs de données d'activation désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (*papier, support magnétique ou confiné dans une carte à puce ou une clé USB*), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur.

6.1.1.2 Porteurs

L'Application « Protect and Sign - Personal Signature » gère la génération des bi-clés.

La génération des bi-clés est effectuée dans une ressource cryptographique matérielle (*Cf. § 6.2*) hébergée par l'OSC et personnalisée par l'OSC.

La génération des bi-clés est réalisée de telle sorte à éviter toute forme de compromission des bi-clés et leur utilisation dans un contexte autre que celui d'une signature suivant un Protocole de consentement avec les données d'activation associées conformément à la PSGP et à la politique de signature du Client.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet.

6.1.3 Transmission de la clé publique à l'AC

6.1.3.1 AC

La clé publique d'AC est délivrée de manière sécurisée à l'AC intermédiaire ou racine qui émet le certificat d'AC pendant la cérémonie des clés (*Cf. § 6.1.1*) ou lors de la phase d'enregistrement (*Cf. § 4.1*).

La clé publique de l'AC est utilisée lors de la cérémonie des clés, sous un format PKCS#10, afin d'émettre le certificat d'AC.

6.1.3.2 Porteur

La clé publique est transmise à l'AC à la suite de la génération de la bi-clé, sous un format PKCS#10, par l'Application « Protect and Sign - Personal Signature ». Le mécanisme de délivrance lie l'identité du Porteur à la clé publique à certifier.

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

L'ensemble des certificats de la chaîne de confiance de l'AC est contenu dans le Document signé.

L'ensemble des certificats d'AC est publié par le SP.

Le certificat de l'AC DocuSign France dont dépend l'AC est contenu dans les logiciels d'Adobe.

6.1.5 Taille des clés

Les recommandations des organismes nationaux et internationaux compétents (*relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage, etc*) sont périodiquement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats porteurs et AC doivent ou ne doivent pas être modifiés.

L'utilisation de l'algorithme RSA avec la fonction de hachage SHA2 est utilisée pour l'AC. La taille de la bi-clé de l'AC est de 2048 bits.

La longueur des clés des Certificats Porteurs est de 2048 bits pour l'algorithme RSA avec la fonction de hachage SHA-256.

6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité

6.1.6.1 AC

Les équipements utilisés pour la génération des bi-clés d'AC sont des ressources cryptographiques matérielles évaluées certifiées EAL 4+ et qualifié renforcé.

6.1.6.2 Porteurs : OID différent de 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

Les bi-clés des Porteurs sont générées par le porteur à l'aide d'un support matériel évalué certifié FIPS 140-2 level 2 ou EAL4+.

6.1.6.3 Subscriber: OID 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

Les bi-clés des Porteurs sont générées par le porteur à l'aide d'un support matériel évalué certifié FIPS 140-2 level 2 ou EAL4+ ou équivalent et certifié conforme QSCD par rapport aux exigences de l'Annexe III de la Directive 1999/93/EC et du règlement eIDAS.

6.1.7 Objectifs d'usage de la clé

L'utilisation de l'extension "key usage" dans le certificat « Porteur » (*et aussi de l'extension « Extended Key Usage » quand elle est présente*) et dans les certificats des AC est décrite au § 10 dans les profils de certificats et indique l'objectif d'usage de la clé.

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

La ressource cryptographique matérielle de l'AC et des Porteurs utilisent des générateurs d'aléas qui devront être conformes à l'état de l'art, aux standards en vigueur ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés. Les algorithmes utilisés devront être conformes aux standards en vigueurs ou suivre les spécifications de la normalisation lorsqu'ils sont normalisés (*Cf. § 6.1.6*).

6.2.2 Contrôle de la clé privée par plusieurs personnes

6.2.2.1 AC

L'activation de la clé privée d'AC est contrôlée par au moins 2 personnes détenant des données d'activations et qui sont dans des rôles de confiance. Les personnes de confiance participant à l'activation de la clé privée d'AC font l'objet d'une authentification forte. L'AC est activée dans un boîtier cryptographique afin qu'elle puisse être utilisée par les seul rôles de confiances et processus autorisés qui peuvent émettre des certificats et des CRL.

6.2.2.2 Porteur

Les clés des Porteurs sont activées après l'authentification réussit du Porteur utilisant les données d'activation (*Cf. § 6.4*) prévu dans le Protocole de Consentement et la Politique d'Enregistrement et les règles de sécurité du [PSM QSCD] (*uniquement pour les OIDs 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31*).

6.2.3 Séquestre de clé privée

Les clés privées d'AC et des Porteurs ne font jamais l'objet de séquestre.

6.2.4 Copie de secours de de clé privée

6.2.4.1 AC

La bi-clé d'AC est sauvegardée sous le contrôle de plusieurs personnes à des fins de reprise d'activité.

Les sauvegardes des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles.

Les sauvegardes sont rapidement transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'AC.

Les sauvegardes de clés privées d'AC sont stockées dans des ressources cryptographiques matérielles ou sous forme de fichier chiffrée créés par la ressource cryptographique.

L'AC possède au moins une sauvegarde des clés hors site.

6.2.4.2 Porteur

Sans objet.

6.2.5 Archivage de la clé privée

Les clés privées d'AC et de Porteur ne font jamais l'objet d'archives.

6.2.6 Transfert de la clé privée vers / depuis le module cryptographique

6.2.6.1 AC

Les clés d'AC sont générées, activées et stockées dans des ressources cryptographiques matérielles ou sous forme chiffrées.

Quand elles ne sont pas stockées dans des ressources cryptographiques ou lors de leur transfert, les clés privées d'AC sont chiffrées au moyen de l'algorithme AES ou 3DES.

Une clé privée d'AC chiffrée ne peut être déchiffrée sans l'utilisation d'une ressource cryptographique matérielle et la présence de multiples personnes dans des rôles de confiance.

6.2.6.2 Porteur

Sans objet.

6.2.7 Stockage de la clé privée dans un module cryptographique

6.2.7.1 AC

Les clés privées d'AC sont stockées dans des ressources cryptographique matérielles sont protégées avec le même niveau de sécurité que celui dans lequel elles ont été générées (*Cf. 6.1.6*).

6.2.7.2 Porteur : OID différent de 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

Les clés privées Porteurs sont stockées dans des ressources cryptographiques matérielles dédiées à cet usage et sont protégées avec le même niveau de sécurité que celui dans lequel elles ont été générées (*Cf. 6.1.6*).

Les clés sont ainsi stockées en vue de leur utilisation via le mécanisme du Protocole de consentement en utilisant les données d'activation Porteur.

6.2.7.3 Porteur : OID 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

Les clés privées Porteurs sont stockées dans des ressources cryptographiques matérielles dédiées (*partition dédiée*) à cet usage et sont protégées avec le même niveau de sécurité que celui dans lequel elles ont été générées (*Cf. 6.1.6*).

Les clés sont ainsi stockées en vue de leur utilisation via le mécanisme du Protocole de consentement en utilisant les données d'activation Porteur comme définit dans [PSM QSCD].

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 AC

Les clés privées d'AC ne peuvent être activées qu'avec un minimum de 2 personnes dans des rôles de confiance et qui détiennent des données d'activation de l'AC en question.

Une fois que les clés d'AC sont dans des HSM personnalisés, seul le système d'AC de l'IGC en ligne peut utiliser les clés d'AC via des rôles authentifiés sur les interfaces de l'IGC.

6.2.8.2 Porteur : OID différent de 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

À la suite de l'authentification réussie du Porteur lors du Protocole de consentement, et à l'aide de ses données technique d'activation (*par exemple : code OTP, certification d'authentification pour s'authentifier ou support OTP*), la bi-clé Porteur est utilisée dans un HSM.

L'authentification est mise en œuvre conformément à la politique de signature du Client et la PSGP.

6.2.8.3 Porteur: OID 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

L'activation de la bi-clé de signature par le Porteur est réalisation suivant les règles de [PSM QSCD] et la Politique d'Enregistrement.

Le Protocole de Consentement est mis en œuvre par l'AE ou l'AC.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 AC

Les ressources cryptographiques matérielles dans lesquelles des clés d'AC ont été activées ne sont pas laissées sans surveillance ou accessible à des personnes non autorisées. Après utilisation, les ressources cryptographiques matérielles sont désactivées. Les ressources cryptographiques sont ensuite stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

Les ressources cryptographiques de signature de l'AC sont en ligne uniquement afin de signer des certificats porteurs et des LCR après avoir authentifié la demande de certificat et la demande de révocation.

Les ressources cryptographiques se désactivent automatiquement en cas d'incident.

6.2.9.2 Porteur

La désactivation de la clé privée du porteur est effectuée par la destruction de la bi-clé réalisée à la fin de la Transaction avec le Porteur comme décrit dans la PSGP.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 AC

Les clés privées d'AC sont détruites quand elles ne sont plus utilisées ou quand les certificats auxquels elles correspondent sont expirés ou révoqués. La destruction d'une clé privée implique la destruction des copies de sauvegarde, des données d'activation et l'effacement de la ressource cryptographique qui la contient, de manière qu'aucune information ne puisse être utilisée pour la retrouver. L'opération de destruction des clés dans le HSM s'effectue à l'aide des fonctions d'effacement du HSM. Si le HSM n'est plus opérationnel, alors la destruction des clés d'AC s'effectue en détruisant physiquement le HSM.

L'opération de destruction s'effectue dans un environnement sécurisé (*Cf. § 5.1*) et avec des rôles de confiance (*Cf. § 5.2*).

6.2.10.2 Porteur

La destruction de la clé privée du Porteur est effectuée à l'aide du support matériel de la bi-clé en utilisant les fonctions logiques d'effacement pour le support matériel de la bi-clé et cette opération est pilotée par l'Application « Protect and Sign - Personal Signature ».

Si le HSM n'est plus opérationnel, alors la destruction des clés Porteur s'effectue en détruisant physiquement le HSM.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs d'authentification et de signature

Se reporter au § 6.1.6.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques sont archivées par archivage des certificats (*se reporter au § 5.5.2 ci-dessus*).

6.3.2 Durée de vie des bi-clés et des certificats

6.3.2.1 AC

La durée opérationnelle maximale pour la clé privée de l'AC est de 5 ans moins la durée de vie du Certificat Porteur.

La durée opérationnelle maximale pour la clé publique de l'AC est de 5 ans.

6.3.2.2 Porteur

La durée de vie opérationnelle d'un certificat est limitée par son expiration qui est donné dans la DPC. La durée de vie opérationnelle d'une bi-clé est équivalente à celle du certificat auquel elle correspond et le nombre de Document à signer par un Porteur lors d'une Transaction.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

6.4.1.1 AC

Les données d'activation des clés privées d'AC sont générées durant les cérémonies de clés (*Se reporter au § 6.1.1.1*). Les données d'activation sont générées automatiquement selon un schéma de type M of N. Dans tous les cas les données d'activation sont remises à leurs porteurs après génération pendant la cérémonie des clés. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance. Les données d'activation ne peuvent pas être transmises par d'autres procédures. Les données d'activation les plus sensibles sont redondées (*la DPC donne plus de détail*).

6.4.1.2 Porteur : OID différent de 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

Le type de Données d'activation qu'utilise le Porteur est décrit dans la politique de signature du Client.

Les données d'activation sont soit enregistrées par l'AE soit générées par l'AE et distribuées de manière sécurisée au Porteur, de façon à avoir l'assurance que seul le Porteur pourra signer un Document à l'aide de la donnée d'activation, et à l'Application « Protect and Sign - Personal signature » qui les utilisent dans la mise en œuvre du Protocole de consentement. L'Application « Protect and Sign - Personal signature » peut aussi générer les données d'activation et les remettre au Porteur via les informations de contacts (*Cf. § 4.1*) de façon à avoir l'assurance que seul le Porteur pourra signer un Document à l'aide de la donnée d'activation.

La politique de signature indique si une donnée d'activation est utilisée ou pas.

Une donnée d'authentification technique (*OTP par exemple*) est obligatoire pour les Porteurs qui signent des Documents à distance.

6.4.1.3 Porteur : OID 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

Le Protocole de Consentement doit être conforme aux règles de [PSM QSCD] et la Politique d'Enregistrement.

6.4.2 Protection des données d'activation

6.4.2.1 AC

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique.
Les porteurs de données d'activation sont responsables de leur gestion et de leur protection.
Un porteur de données d'activation ne peut détenir plus d'une donnée d'activation d'une même AC à un même instant.
Les données d'activation sont gérées par la PMA qui requiert qu'elles soient stockées dans des coffres.
Si les données d'activation sont sur support papier alors elles sont stockées de manière protégées dans un coffre.

6.4.2.2 Porteur : OID différent de 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

L'AE et l'Application « Protect and Sign - Personal signature » sont responsables de la protection des données d'activation.
Le Porteur est responsable de la protection de sa donnée d'activation.

6.4.2.3 Porteur : OID 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31

Le Porteur est responsable de la protection de sa donnée d'activation.

Quand la donnée d'activation est gérée par PSM, alors l'AC est responsable de la protection du code OTP afin d'empêcher toute compromission de ce code et tout autre usage illicite par des entités différentes du Porteur.

6.4.3 Autres aspects liés aux données d'activation

Les données d'activation de l'AC sont changées dans le cas où les ressources cryptographiques sont changées ou retournées au constructeur pour maintenance.

Les autres aspects de la gestion des données d'activation sont précisés dans la DPC.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité techniques spécifiques aux systèmes informatiques

Les fonctions suivantes sont fournies par le système d'exploitation, ou par une combinaison du système d'exploitation, de logiciels et de protection physiques. Un composant d'une IGC comprend les fonctions suivantes :

- Identification et authentification forte des utilisateurs pour l'accès au système (*authentification à deux facteurs*).
- Gestion des droits des utilisateurs (*permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles*).
- Gestion de sessions d'utilisation (*déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur*).
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels.
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès.
- Protection du réseau contre toute intrusion d'une personne non autorisée.
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent.
- Fonctions d'audits (*non-répudiation et nature des actions effectuées*).
- Éventuellement, gestion des reprises sur erreur.

Quand un composant d'IGC est hébergé sur une plateforme évaluée au regard d'exigences d'assurance de sécurité, il doit être utilisé dans sa version certifiée.

Au minimum le composant utilise la même version de système d'exploitation que celle sur lequel le composant a été certifié.

Les composants d'IGC sont configurés de manière à limiter les comptes et services aux seuls éléments nécessaires pour supporter les services d'AC.

La plate-forme de cérémonie des clés est dédiée aux cérémonies des clés et n'est jamais connecté à un réseau.

Les ordinateurs utilisés pour administrer les systèmes d'IGC sont dédiées à l'administration des systèmes d'IGC.

Les règles suivantes s'appliquent pour les composantes de l'IGC (*AC et AE*) :

- Suivre une procédure documentée pour l'attribution et la gestion des rôles de confiances de l'IGC.
- Documenter les missions et les responsabilités des rôles de confiances de l'IGC et la séparation des rôles pour l'ensemble des rôles de l'IGC en tenant compte des risques de sécurité pour les composantes et services d'IGC.
- S'assurer que seules les personnes avec des rôles de confiances peuvent accéder aux services des composantes d'IGC attribués à leur rôle.
- S'assurer qu'une personne avec un rôle de confiance agît seulement dans le cadre du rôle qui lui est assigné quand il se connecte sur une composante de l'IGC.
- Exiger des employés et des contractants de n'accéder qu'aux seules fonctions strictement nécessaires à la mission qu'ils doivent conduire dans le cadre de leurs rôles.
- Exiger des personnes qui se connectent avec un rôle de confiance aux interfaces des composantes de l'IGC d'utiliser un moyen qui leur est propre et dédié afin d'être authentifiées par les composantes d'IGC.
- Si une personne avec un rôle de confiance utilise un moyen de type login/mot de passe alors cette authentification et la gestion des login/mot de passe doit être effectué en accord avec la politique de sécurité de l'OSC.
- Exiger et gérer la fermeture des sessions sur les composantes d'IGC pour les rôles de confiance qui s'y connectent ainsi que le verrouillage des stations de travail lorsqu'ils ne les utilisent plus.
- Configurer les composantes d'IGC et les stations de travails des rôles de confiances afin de gérer la fermeture automatique des sessions de connexion et des postes de travail à la suite d'une inactivité détectée du rôle de confiance.
- Contrôles des comptes et des accès des rôles de confiance et supprimer les accès et les comptes des personnes ayant eu des rôles de confiance mais ne les exerçant plus.
- Si cela est applicable pour une composante d'IGC (*c'est-à-dire pour des composantes qui n'utilisent pas de certificat pour leurs rôles de confiance*), alors implémenter un blocage automatique d'accès qui se déclenche à la suite d'un nombre maximum de tentatives infructueuses de connexion.
- Implémenter une procédure de désactivation des accès et des droits aux composantes de l'IGC, effective en 24 heures, pour une personne quittant son rôle de confiance suite à une fin de contrat.
- Obliger une authentification forte pour les rôles de type « administration » des composantes de l'IGC.

6.5.2 Niveau de qualification des systèmes informatiques

Pas d'exigence.

Pour l'OID 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31, le logiciel PSM est certifié selon [PSM QSCD].

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développements des systèmes

Le contrôle des développements des systèmes de l'IGC s'effectue comme suit :

- Des matériels et des logiciels achetés de manière à réduire les possibilités qu'un composant particulier soit altéré.
- Les matériels et logiciels mis au point l'ont été dans un environnement contrôlé, et le processus de mise au point défini et documenté. Cette exigence ne s'applique pas aux matériels et aux logiciels achetés dans le commerce.
- Tous les matériels et logiciels doivent être expédiés ou livrés de manière contrôlée permettant un suivi continu depuis le lieu de l'achat jusqu'au lieu d'utilisation.
- Les matériels et logiciels sont dédiés aux activités d'IGC. Il n'y a pas d'autre application, matériel, connexion réseau, ou composant logiciels installés qui ne soit pas dédiés aux activités d'IGC.
- Il est nécessaire de prendre soin de ne pas télécharger de logiciels malveillants sur les équipements de l'IGC. Seules les applications nécessaires à l'exécution des activités IGC sont acquises auprès de sources autorisées par politique applicable de l'AC. Les matériels et logiciels de l'AC font l'objet d'une recherche de codes malveillants dès leur première utilisation et périodiquement par la suite.
- Les mises à jour des matériels et logiciels sont achetées ou mises au point de la même manière que les originaux, et seront installés par des personnels de confiance et formés selon les procédures en vigueur.

6.6.2 Mesures liées à la gestion de la sécurité

La configuration du système de l'IGC, ainsi que toute modification ou évolution, est documentée et contrôlée par les responsables des composantes de l'IGC.

Il existe un mécanisme permettant de détecter toute modification non autorisée du logiciel ou de la configuration de l'IGC.

Une méthode formelle de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'IGC.

Lors de son premier chargement, on vérifie que le logiciel de l'IGC est bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

Les règles suivantes s'appliquent :

- L'OSC implémente un système de contrôle des configurations qui notifie les rôles de confiance en charge de l'administration des systèmes des composantes de l'IGC d'un changement de configuration.
- Former et exiger des rôles de confiance qu'ils remontent les évènements anormaux et les problèmes de sécurité.
- Conduire des analyses de journaux (*cf. 5.4.8*).

6.6.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

En ce qui concerne les logiciels et matériels évalués, l'AC poursuit sa surveillance des exigences du processus de maintenance pour maintenir le niveau de confiance.

Une gestion de la montée en charge des services est effectuée afin d'être assurée d'avoir les ressources nécessaires pour opérer les services d'IGC.

6.7 Mesures de sécurité réseau

L'AC est en ligne accessible par des postes informatiques sous contrôle. Les composantes accessibles de l'IGC sont connectées à l'Internet dans une architecture adaptée présentant des passerelles de sécurité et assurent un service continu (*sauf lors des interventions de maintenance ou de sauvegarde*).

Les autres composantes de l'IGC utilisent des mesures de sécurité appropriées pour s'assurer qu'elles sont protégées contre des attaques de déni de service et d'intrusion. Ces mesures comprennent l'utilisation de gardes, de pare-feu et de routeurs filtrants. Les ports et services réseaux non utilisés sont coupés.

Les règles suivantes s'appliquent :

- Tout appareil de contrôle de flux utilisé pour protéger le réseau sur lequel le système IGC est hébergé refuse tout service, hormis ceux qui sont nécessaires au système IGC, même si ces services ont la capacité d'être utilisés par d'autres appareils du réseau.
- Les composantes d'IGC sont séparées dans des zones réseaux distinctes en fonction de leurs relations fonctionnelles (*type de service rendu*), logiques et physiques entre elles et avec leur environnement. Il faut autoriser uniquement les flux réseaux d'administration et de services IGC entre les composantes d'IGC et leur environnement.
- Maintenir et protéger les composantes d'IGC dans au moins des zones dédiées en faisant la différence entre les interfaces de composantes d'IGC qui sont connectées sur internet et les autres qui ne le sont pas (*les composantes d'IGC doivent être séparées en zone front-end et back-end comme dans une architecture N-Tiers*).
- Implémenter et configurer un réseau d'administration (*un système utilisé pour fournir des fonctions de sécurités telles que ; l'authentification, le contrôle du réseau, la création et la collecte des journaux, l'analyse des journaux, les scans de vulnérabilité, les analyses anti-virus quand cela s'applique et l'administration du système d'information*) qui protège les systèmes et la communication entre les composantes d'IGC et son environnement (*en dehors des zones réseaux des composantes IGC*).
- Configurer chaque point de contrôle du réseau (*mur pare feu, commutateur, router, passerelle ou tout autre composant réseau*) avec des règles qui n'autorisent que les services, ports, protocoles et communications nécessaires aux services et composantes d'IGC.
- Configurer les composantes et systèmes d'IGC en désactivant les comptes utilisateursles , les services, ports et les protocoles qui ne sont pas nécessaires aux services et composantes d'IGC et n'activer que ce qui est nécessaire aux services et composantes d'IGC.
- Vérifier la configuration des systèmes des composantes d'IGC au moins une fois par semaine (*pour l'AC*), et suivant une fréquence déterminée par le Client pour l'AE, afin de détecter toute modification non voulue.
- Ne donner que des droits d'administration sur les composantes d'IGC aux seuls rôles de confiance qui le nécessitent.
- Implémenter un système d'authentification forte pour l'accès par les rôles de confiances aux interfaces des composantes d'IGC.
- Changer les clés d'authentification et les mots de passe pour les comptes des personnes ou des machines dont les droits sont changés ou révoqués.
- Appliquer les mises à jour, recommandées par les CERT et les fournisseurs des logiciels des composantes d'IGC afin d'éviter des attaques concrètes et risquées sur les services d'IGC, dans un délai de 6 mois suite à la sortie officielle de la mise à jour, à moins que la PMA ou le Client démontre que la mise à jour introduise de nouvelle(*s*) vulnérabilité(*s*) ou que l'instabilité engendré l'emporterait sur les bénéfices attendus.

Pour l'OID 1.3.6.1.4.1.22234.2.8.3.20 et 1.3.6.1.4.1.22234.2.14.3.31, le logiciel PSM est installé et configuré conformément à [PSM QSCD].

6.8 Horodatage / Système de datation

Il n'y a pas d'horodatage utilisé par l'IGC mais une datation sûre.

Seul le Fichier de preuve est horodaté comme décrit [PSGP].

Tous les composants de l'IGC sont régulièrement synchronisés avec un serveur de temps tel qu'une horloge atomique ou un serveur Network Time Protocol (*NTP*).

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

- Du début de validité d'un certificat Porteur.
- De la révocation d'un certificat Porteur 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.

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 Profil de Certificats

7.1.1 Numéro de version

Les certificats émis par l'AC sont des certificats au format X.509 v3 (*populate version field with integer "2"*).

Les champs des certificats Porteurs et AC sont définis par le RFC 5280 et précisés dans le chapitre 10 ci-dessous.

7.1.2 Extensions de Certificats

Cf. § 10.

7.1.3 Identifiant d'algorithmes

Les certificats émis sous cette PC utilisent les algorithmes :

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

Sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(5)}

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

7.1.4 Formes de noms

Cf. § 3.1.1.

7.1.5 Contraintes de noms

Cf. § 3.1.1.

7.1.6 Identifiant d'objet (OID) de la Politique de Certification

Les certificats émis par l'AC contiennent l'OID de la PC qui est donné au § 1.2.

7.1.7 Extensions propres à l'usage de la Politique

Sans objet.

7.1.8 Syntaxe et Sémantique des qualificateurs de politique

Sans objet.

7.1.9 Interprétation sémantique de l'extension critique "Certificate Policies"

Pas d'exigence formulée.

7.2 Profil de LCR

7.2.1 LCR et champs d'extensions des LCR

L'annexe 10 donne le détail.

7.3 Profil OCSP

Le chapitre 4.9.10 donne le détail.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquence et/ou circonstances des audits

Les composantes de l'IGC 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 IGC hébergées par l'OSC à fonctionner en conformité avec la présente PC selon le "*guide d'audit IGC*" fourni par la PMA.

Le PMA a le droit d'exiger une vérification complémentaire non périodique de la conformité des composantes de l'IGC (*surtout l'AE*) 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.

Avant d'autoriser un Client à utiliser « Protect and Sign - Personal Signature » en utilisant un OID certifié, la PMA audite et vérifie les procédures d'AE et de gestion de l'AE telles que définies par le client afin d'être sûre de la cohérence et la conformité avec les exigences énoncées dans la PC. Si les procédures et les modes de fonctionnement de l'AE sont conformes aux exigences de la PC, alors la PMA autorise le Client à utiliser « Protect and Sign - Personal Signature » avec l'AE.

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 pour tous les OIDs.

Pour qu'un Client puisse utiliser « Protect and Sign - Personal Signature » avec un OID certifié, l'AE doit être auditée par un auditeur externe, choisi par la PMA, afin d'auditer sa conformité vis-à-vis de la PC et les exigences de l'ETSI selon l'OID sélectionné.

Sinon le Client ne peut pas prétendre que le Certificat Porteur est compatible avec un des OID certifié contenus dans la présente PC. Le programme de vérification de l'AE est organisé comme suit avec une vérification chaque année au moins :

- Premier audit est réalisé par l'auditeur externe avant la mise en service.
- La première année suivant l'audit initial, l'audit est réalisé selon le programme d'audit DocuSign France.
- La deuxième année après l'audit initial, l'audit est réalisé de nouveau par un auditeur externe.

8.2 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 d'IGC.

8.3 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.

8.4 Sujets couverts par les évaluations

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

Pour l'AC, le périmètre de l'audit est l'OSC, l'AC, le contrat entre le Client et DocuSign France et les rapports d'audit de l'AE.

L'AE assure plus précisément les fonctions suivantes :

- La gestion et la mise en œuvre des bi-clés et certificats utilisés pour le Connecteur Client.
- La gestion et la mise en œuvre du Connecteur Client et son interconnexion avec l'Application Client et l'Application « Protect and Sign - Personal signature ».
- La gestion des identités (*données personnelles*) et des données d'activation des Porteurs.
- L'authentification des Porteurs par l'AE dans le cadre de la Cinématique de signature et de la politique d'enregistrement et du Protocole de consentement.
- La gestion des Opérateurs d'AE.
- L'archivage des Fichier de preuves et des journaux de l'AE.
- La gestion par l'Application Client des Documents présentés au Porteur dans le cadre de la politique de signature.

8.5 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 de l'IGC, 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 de l'IGC ou de prendre toute autre mesure qu'il juge opportune.

Quand les actions correctives sont réalisées, la composante de l'IGC 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*).

8.6 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 au § 8.1 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 au § 8.5 ci-dessus. Le Rapport de Contrôle de Conformité n'est pas rendu disponible à des tiers utilisateurs sur Internet.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

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

9.1.2 Tarifs pour accéder aux certificats

Les certificats de la chaîne de confiance sont accessibles par les Utilisateurs de certificats gratuitement via le SP et sont dans le Document signé.

Les certificats Porteurs ne sont pas publiés.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation des certificats

Le service de publication de l'AC (*qui contient la LCR pour les certificats Porteurs et d'AC*) est accessible gratuitement sur Internet.

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

La politique de remboursement applicable est définie dans les conditions générales d’utilisation à destination du Porteur et dans le contrat établi entre le Client et DocuSign France.

9.1.6 Politique de pénalité

La politique de pénalité applicable est définie dans les conditions générales d’utilisation à destination du Porteur et dans le contrat établi entre le Client et DocuSign France.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

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

9.2.2 Autres ressources

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

9.2.3 Couverture et garantie concernant les entités utilisatrices

En cas de dommage subi par une entité utilisatrice du fait d’un manquement par l’AC à ses obligations, l’AC pourra être amené à dédommager l’entité utilisatrice dans la limite de la responsabilité de l'AC définie dans le contrat établi entre le Client et DocuSign France.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- Les clés privées de l'AC, des composantes et des Porteurs.
- Les données d'activation associées aux clés privées d'AC et des Porteurs.
- Tous les secrets de l'IGC.
- Les journaux d'évènements des composantes de l'IGC.
- Le dossier d'enregistrement (*comprenant la demande de certificat*) et les données personnelles du Porteur.
- Les bi-clés du Connecteur Client.
- Le plan de continuité.
- La politique de sécurité interne de l'AC.
- 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.

9.3.2 Informations hors du périmètre des informations confidentielles

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

9.3.3 Responsabilité en termes de protection des informations confidentielles

Les composantes de l'IGC ont mis en place et respectent des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme confidentielles au sens de l'article 9.3.1 ci-dessus.

A cet égard, les composantes de l'IGC 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.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

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

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

9.4.2 Informations à caractère personnel

L'AC considère que les données d'identification et de contacts Porteur, contenues dans les dossiers d'enregistrement et le Fichier de preuve, sont des informations à caractère personnel qui doivent être protégées suivant la loi nationale de l'AE et de l'AC.

9.4.3 Informations à caractère non personnel

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

9.4.4 Responsabilité en termes de protection des données personnelles

L'AC a mis en place et respecte des procédures de protection des données personnelles pour garantir la sécurité des informations caractérisées comme personnelles au sens de l'article 9.4.1 ci-dessus dans le cadre de la délivrance et la gestion d'un certificat de porteur.

A cet égard, l'AC respecte notamment la législation et la réglementation en vigueur sur le territoire français, en particulier, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés révisée 2006.

En application de l'article 34 de la loi Informatique et Libertés du 6 janvier 1978, 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 signataires peuvent s'adresser au Correspondant Informatique et Libertés de DocuSign France en utilisant les informations fournies dans les CGU.

L'AE doit documenter sa politique et ses responsabilités en termes de gestion des données personnelles.

9.4.5 Notification et consentement d'utilisation de données personnelles

Aucune des données à caractère personnel communiquées lors de l'enregistrement ne peut être utilisée par l'IGC, 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 l'AE dans les conditions définies par l'AE et par l'AC lors de l'acceptation de signer un document lors de la mise en œuvre du Protocol de consentement (*Cf. § 4.3*) et du fait de l'acceptation par le Porteur (*Cf. § 4.4*) du Certificat émis par l'AC.

Le Porteur accepte que les données personnelles le concernant recueillies par l'IGC 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 (*via le Fichier de preuve*).

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

L'IGC 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*).

9.4.7 Autres circonstances de divulgation d'informations personnelles

La PMA obtient l'accord des composantes d'IGC de transférer ses données à caractère personnel dans le cas d'un transfert d'activité tel qu'il est décrit au § 5.8.

9.5 Droits sur la propriété intellectuelle et industrielle

Tous les droits de propriété intellectuelle détenus par l'AC 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.

L'AC 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.

9.6 Interprétations contractuelles et garanties

Les composantes de l'IGC, les Clients et la communauté d'utilisateurs de certificats 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 des contrats.

Les obligations communes des différentes composantes de l'IGC 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 de l'IGC.
- Respecter et appliquer les termes de la présente PC qu'elles reconnaissent.
- 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 de l'IGC.

9.6.1 Obligations et garanties de la PMA

Les obligations de la PMA sont les suivantes :

- L'élaboration de la PC et de la DPC.
- L'audit de l'IGC et en particulier des AE et y compris lorsque la composante d'IGC est opérée par un sous-traitant.
- L'approbation des politiques de signature et d'enregistrement du Client et de l'AE au regard des choix d'OID.
- Le contrôle de la relation contractuelle avec le Client agissant en tant qu'AE.
- Documente les schémas de certification qu'elle entretient avec des AC tierces.

9.6.2 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.

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 sa DPC.

Les obligations communes aux composantes de l'AC sont :

- N'utiliser ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles ils ont été générés et avec les moyens appropriés, comme spécifié dans la DPC.
- Respecter et appliquer les dispositions de la partie de la DPC qui les concerne (*cette partie de la DPC doit être transmise à la composante concernée*).
- Documenter ses procédures internes de fonctionnement afin de compléter la DPC générale.
- Mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC conformément à la politique de sécurité de DocuSign France.
- Notifier les Clients en cas de compromission de bi-clé d'AC ou de Porteur.
- Met à la disposition de l'AE l'ensemble des moyens techniques nécessaires à la réalisation de ses obligations.
- Protéger les données d'activation et les remettre de manière sûre aux Porteurs.
- Générer et protéger et détruire les bi-clés des Porteurs avec l'Application « Protect and Sign - Personal signature ».
- Conduire une analyse de risque afin de déterminer les risques métiers et les mesures de sécurité adéquates.
- Respecter les règles de sécurité de [PSM QSCD].
- Prendre toutes les mesures raisonnables pour s'assurer que les Porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.

9.6.3 Obligations de l'AE

Les obligations de l'AE sont les suivantes :

- Pour l'OID 1.3.6.1.4.1.22234.2.8.3.7, 1.3.6.1.4.1.22234.2.8.3.20, 1.3.6.1.4.1.22234.2.14.3.31 et 1.3.6.1.4.1.22234.2.14.3.32 :
    - Assurer que les Porteurs soient dûment authentifiés et identifiés.
    - Assurer que les demandes de certificats soient valides, complètes et dûment autorisées.
    - Respecter les règles de sécurité de [PSM QSCD] ;
- Pour l'OID 1.3.6.1.4.1.22234.2.8.3.9 :
    - Assurer que les preuves d'identité des Porteurs sont soit dûment examinées dans le cadre du service défini de l'AE ou, le cas échéant, conclu grâce à l'examen d'attestation provenant de sources appropriées et autorisées.
    - Assurer que les demandes de certificats soient valides, complètes et dûment autorisées selon les preuves d'identités ou les attestations recueillies.
- Soumettre des demandes de certificats avec les informations complètes et valides à l'AC conformément à [PSGP].

- Permettre au Porteur de visualiser les informations personnelles qui seront portées dans le Certificat durant le Protocol de consentement.
- Avant de permettre la signature d'un Document par un Porteur, l'AE doit rendre disponible les CGU au Porteur dans un langage compréhensible et à partir de moyens qui garantissent la pérennité de l'information communiquée.
- Alerter la PMA en cas d'incident(*s*) de sécurité constaté(*s*) dans les services rendus par l'AC.
- Protéger les clés du Connecteur Client et s'assurer de la connexion avec l'Application « Protect and Sign - Personal signature ».
- Protéger les données d'activation et les remettre de manière sûre au Porteur.
- Collecter et vérifier les pièces justificatives qui permettent l'authentification du Porteur et la création de l'identité du Porteur.
- Protéger les données personnelles du Porteur.
- Exercer une attention suffisante et raisonnable afin d'éviter l'utilisation non autorisée des clés privées du Porteur.
- Gérer l'AE et les Opérateur d'AE (*maintenir une liste d'AE*) conformément aux exigences du Client.
- Appliquer la politique d'enregistrement du Client.
- Alerter le Client en cas d'incident de sécurité ayant des conséquences sur le Service de signature et/ou d'AE.
- La conservation des journaux et des fichiers de preuve pendant 5 ans.
- Respecter la PC et la DPC de l'AC.
- En cas de délégation complète de l'AE, respecter les modalités du contrat établit avec DocuSign France.

9.6.4 Obligation du Client

Les obligations du Client 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.
- Accepter le résultat et les conséquences d'un contrôle de conformité et, en particulier, remédier aux non-conformités qui pourraient être révélées.
- Alerter les Porteurs concernés en cas d'incident de sécurité sur le processus de signature et/ou leurs clés privées et/ou de l'AC et/ou les données d'activation des Porteurs.
- Exercer une attention suffisante et raisonnable afin d'éviter l'utilisation non autorisée des clés privées des Porteurs.
- Signer le contrat qui le lie à DocuSign France et l'engage en qualité d'AE.
- Établir un contrat entre l'entité qui est OSC et l'AE, quand ce sont deux entités légales différentes, qui identifie clairement les services qui sont mis en œuvre et les obligations et responsabilités selon les services gérés.
- Définir la politique d'enregistrement et de signature.
- Choisir le niveau de sécurité et donc l'OID de PC.
- Alerter la PMA en cas d'incident sur l'AE ou l'Application Client.
- Choisir et définir le Protocole de consentement et le type de donnée d'activation associées.

- Respecter la PC et la DPC de l'AC.
- Garantir la sécurité de l'Application Client.

9.6.5 Obligations de l'OSC

Les obligations de l'OSC sont :

- Respecter sa politique de sécurité.
- Alerter la PMA ou le Client (*en fonction des services hébergés*) en cas d'incident(*s*) de sécurité(*s*).
- Protéger les données personnelles et les données d'activation.
- Documenter ses procédures internes afin de compléter la DPC et sa politique de sécurité.
- Respecter la totalité du contrat qui l'engage vis-à-vis du Client et de DocuSign France.

9.6.6 Obligation du PVID

Les obligations du PVID sont :

- Enregistre et archive toutes les informations demandées.
- Protéger les informations de l'Abonné.
- Faire preuve d'une diligence raisonnable pour éviter tout accès non autorisé à l'Application de signature DocuSign.
- Respecter leur politique d'identification.
- Être certifié par l'ANSSI.
- Alerter l'AC en cas d'incident lié à la politique d'identification et au processus de certification.
- Respecter la réglementation RGPD.

9.6.7 Obligations et garanties du Porteur

Les obligations du porteur sont :

- Protéger en confidentialité et intégrité les informations confidentielles qu'il détient, données d'activations, afin d'en éviter un usage non autorisé.
- N'utiliser les données d'activation que dans le cadre de l'Application Client et pour le Protocole de consentement selon la [PSGP] et la Politique de signature Client.
- Se conformer à toutes les exigences de la PC et de la DPC associée.
- Garantir que les informations qu'il fournit à l'AE sont complètes et correctes.
- Se conformer aux exigences des CGU.
- Arrêter d'utiliser le Certificat si ce dernier n'est plus valide et le retirer des applications qui l'utilisent.
- Aviser immédiatement l'AE en cas de non-conformité détectée sur son identité inscrite dans le certificat émis.

9.6.8 Obligations et garanties des autres participants

9.6.8.1 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.
- 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 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].

9.7 Limite de garantie

La PMA garantit au travers de ses services d'IGC :

- L'identification et l'authentification des AC, avec le certificat d'AC émis par la chaîne de confiance choisit par la PMA.
- Gérer les certificats d'AC et leur information de validité.
- Approuver le contenu des Certificats en approuvant la politique d'enregistrement.
- La sécurité de l'utilisation de la clé privée d'un Porteur en approuvant le Protocol de consentement choisit par le Client.

L'AC garantit au travers de ses services d'IGC :

- L'identification et l'authentification de l'AC.
- L'identification et l'authentification des Porteurs avec les Certificats générés par l'AC à partir des informations vérifiées et transmises par l'AE.
- La gestion des certificats correspondants et des informations de validité des certificats selon la présente PC.

Ces garanties sont exclusives de toute autre garantie de l'AC.

Chaque partie s'interdit de prendre un engagement au nom et pour le compte de l'autre partie à laquelle elle ne saurait en aucun cas se substituer.

9.8 Limite de responsabilité

DocuSign France n'est pas responsable quant à la forme, la suffisance, l'exactitude, l'authenticité la falsification ou l'effet juridique des documents et informations remis lors de la demande d'émission, de renouvellement ou de révocation d'un Certificat.

DocuSign France ne garantit pas l'exactitude des informations fournies par le Porteur et le Client en qualité d'AE à l'utilisateur de certificat ni à l'AC, ni les conséquences d'une négligence ou d'un manque de précaution ou de sécurité imputable au Porteur ou au Client.

En outre, le Porteur et le Client demeurent responsables à l'égard de DocuSign France, via l'Application Client et l'Application « Protect and Sign - Personal signature », de :

- La véracité des informations portées dans le Certificat.

- L’utilisation non autorisée de la clé privée d’un Porteur.
- Dommages qui pourraient en résulter.

DocuSign France n’assume aucun engagement ni responsabilité quant aux conséquences dues à tout retard, perte, altération, destruction, utilisation frauduleuse des données, transmission accidentelle de virus ou tout autre élément nuisible via toute télécommunication telle que Internet.

En outre, DocuSign France n’est pas responsable de la qualité de la liaison internet du Client et du Porteur.

Dans le cas où la responsabilité de DocuSign France serait retenue au titre des présentes, il est expressément convenu que DocuSign France serait tenue à réparation des dommages directs certains et immédiats, dont le Client apportera la preuve, dans les limites maximums fixées par DocuSign France dans le contrat établi avec le Client.

DocuSign France exclut toute responsabilité en cas de non-respect par le Client de ses obligations définies dans le contrat établi avec DocuSign France et dans la PC.

DocuSign France ne sera pas responsable des préjudices indirects ou imprévisibles subis par le Client, tels que notamment les pertes de bénéfices, de vente, de contrats, de chiffre d'affaires, de revenus ou d’économies anticipées, perte de clientèle, préjudice d’exploitation, atteinte à l’image de marque, perte de données ou usage de celles-ci, inexactitude ou corruption de fichiers, en relation à ou provenant de l’inexécution ou exécution fautive du contrat établi entre le Client et DocuSign France ou inhérents à l'utilisation des Certificats émis par DocuSign France.

Sont également exclus de toute demande de réparation les dommages causés par un événement de force majeure au sens de l’article 9.15.5 ci-après.

9.9 Indemnités

Les parties conviennent qu’en cas de prononcé d’une quelconque responsabilité de l’AC vis-à-vis d’un tiers utilisateur, les dommages, intérêts et indemnités à sa charge seront déterminés lors de la procédure prévue à l’article 9.2 des présentes.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 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.

9.10.2 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 AC concernées, soit de donner instruction à l'AC de prendre les mesures nécessaires pour se rendre conforme dans un délai fixé.

9.10.3 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 de l'AC pour les certificats émis conformément à la PC. L’AC ne peut plus émettre de Certificat.

9.11 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.

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

La PMA révise sa PC et sa DPC au moins une fois par an.

D'autres révisions peuvent être décidées à tout moment à la discrétion de la PMA.

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.

La PMA communique les modifications de la PC aux parties impactées par les modifications.

9.12.2 Mécanisme et période d'information sur les amendements

La PMA donne un préavis d'1 mois au moins aux composantes de l'IGC de son intention de modifier sa PC/DPC 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 profil de certificat, etc*) et non sur la forme de la PC et de la DPC.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

Si la PMA estime qu'une modification de la PC modifie le niveau de confiance assuré par les exigences de la PC ou par le contenu de la DPC, elle peut instituer une nouvelle politique avec un nouvel identifiant d'objet (*OID*).

9.13 Dispositions concernant la résolution de conflits

La PMA s'assure que tous les accords qu'elle conclut prévoient des procédures adéquates pour le règlement des différends.

Entre autres, l'AC définit sa politique de nommage et propose, et s'autorise dans certains cas, de régler les différends concernant l'identité à inscrire dans un certificat et dans le cas où les parties ne parviendraient pas à un accord amiable, le différend sera réglé par un tribunal français.

Lorsque le différend porte sur une identité, alors il est du ressort de l'AE de gérer et de résoudre le litige.

9.14 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.

9.15 Conformité aux législations et réglementations

La PC est sujette aux lois, règles, règlements, ordonnances, décrets et ordres nationaux d'état, locaux et étrangers concernant les, mais non limités aux, restrictions à l'importation et à l'exportation de logiciels ou de matériels cryptographiques ou encore d'informations techniques.

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

9.16 Disposition diverses

9.16.1 Accord global

Le cas échéant, la DPC précisera les exigences spécifiques.

9.16.2 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.

9.16.3 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.

9.16.4 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.

9.16.5 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.

9.17 Autres dispositions

Le cas échéant, la DPC en fournira les détails.

10 PROFIL DE CERTIFICAT, CRL AND OCSP

10.1 "DocuSign Premium Cloud Signing CA – SI1" CA

10.1.1 Natural person qualified signature with QSCD : 1.3.6.1.4.1.22234.2.14.3.31

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Premium Cloud Signing CA - SI1		
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 String1**
	C	Country code on 2 character ISO 3166-1 Country where the legal entity acting as RA or DRA is officially registered	PrintableString
	OU	RA or DRA <name>	UTF8String
	OU	<*Transaction identification number*>	UTF8String
	serialNumber	random value of 16 bytes of entropy generated by PSM	PrintableString
	pseudonym	Equal to serialNumber. This field can be here only if givenName and surname are not present.	UTF8String
	givenName	First name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	surName	Last name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	CN	First name and last name of the Signatory.	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

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)

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

Extensions	Criticality (True/False)	Value
Key Usage	**TRUE**	
Non Repudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.31
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusignpremiumcloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusignpremiumcloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusignpremiumcloudsigningcasi1.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://pds.dsf.docusign.net/docusignpremiumcloudsigningcasi1.pdf

10.1.2 Natural person qualified signature with QSCD with DTM : 1.3.6.1.4.1.22234.2.14.3.31

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Premium Cloud Signing CA - SI1		
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 String2**

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

	C	Country code on 2 character ISO 3166-1 Country where the legal entity acting as RA or DRA is officially registered	PrintableString
	OU	RA or DRA <name>	UTF8String
	OU	<*Transaction identification number*>	UTF8String
	OU	<Envelope number>	UTF8String
	serialNumber	random value of 16 bytes of entropy generated by PSM	PrintableString
	pseudonym	Equal to serialNumber. This field can be here only if givenName and surname are not present.	UTF8String
	givenName	First name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	surName	Last name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	CN	First name and last name of the Signatory.	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

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		1.3.6.1.4.1.22234.2.14.3.31
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusignpremiumcloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusignpremiumcloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusignpremiumcloudsigningcasi1.p7c

Extensions	Criticality (True/False)	Value
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://pds.dsf.docusign.net/docusignpremiumcloudsigningcasi1.pdf

10.1.3 OCSP Responder certificate

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Premium Cloud Signing CA - SI1		
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 String3**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	OU	0002 812611150	UTF8String
	CN	OCSP Responder <*date*>	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

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)

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

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

10.1.4 Certificate Revocation List

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Premium Cloud Signing CA - SI1
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)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

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		2017/03/08 11:35:50 Z

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

10.2 “DocuSign Cloud Signing CA – SI1” CA

10.2.1 Natural person remote certificate LCP : 1.3.6.1.4.1.22234.2.14.3.32

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Cloud Signing CA - SI1		
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 String4**
	C	Country code on 2 character ISO 3166-1 Country where the legal entity acting as RA is officially registered	PrintableString
	OU	RA <name>	UTF8String
	OU	<*Transaction identification number*>	UTF8String
	serialNumber	random value of 16 bytes of entropy generated by PSM	PrintableString
	pseudonym	Equal to serialNumber. This field can be here only if givenName and surname are not present.	UTF8String
	givenName	First name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	surName	Last name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	CN	First name and last name of the Signatory.	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

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**	

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

Extensions	Criticality (True/False)	Value
Digital Signature		Set
Non Repudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.32
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusigncloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusigncloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusigncloudsigningcasi1.p7c

10.2.2 Natural person remote certificate LCP with DTM : 1.3.6.1.4.1.22234.2.14.3.32

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Cloud Signing CA - SI1		
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[5]**
	C	Country code on 2 character ISO 3166-1 Country where the legal entity acting as RA is officially registered	PrintableString
	OU	RA <name>	UTF8String
	OU	<*Transaction identification number*>	UTF8String

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

	OU	*<Envelope number>*	UTF8String
	serialNumber	random value of 16 bytes of entropy generated by PSM	PrintableString
	pseudonym	Equal to serialNumber. This field can be here only if givenName and surname are not present.	UTF8String
	givenName	First name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	surName	Last name of the signatory if transmitted by RA if not the field is empty.	UTF8String
	CN	First name and last name of the Signatory.	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

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
Non Repudiation		Set
Extended Key Usage	**FALSE**	
Adobe-AuthenticDocumentTrust		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.14.3.32
policyQualifier-cps		https://www.docusign.fr/societe/politiques-de-certifications
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		None
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.dsf.docusign.net/docusigncloudsigningcasi1.crl
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.dsf.docusign.net/docusigncloudsigningcasi1
caIssuers		http://crt.dsf.docusign.net/docusigncloudsigningcasi1.p7c

10.2.3 OCSP Responder certificate

Basic Certificate Fields	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Cloud Signing CA - SI1		
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 String6**
	C	FR	PrintableString
	O	DocuSign France	UTF8String
	OU	0002 812611150	UTF8String
	CN	OCSP Responder <*date*>	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

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
Basic Constraint	**TRUE**	
cA		False
Extended Key Usage	**FALSE**	
id-kp-OCSPSigning		Set
OCSPNoCheck	**FALSE**	
NULL		NULL

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

10.2.4 Certificate Revocation List

CRL Fields	Value
Version	1 (=version 2)
Issuer	C = FR O = DocuSign France OU = 0002 81261115 CN = DocuSign Cloud Signing CA - SI1
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)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

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