Politique de Certification

Protect and Sign Personal Signature : Utilisateur

Emmanuel Montacutelli

08/01/2015

DBD_Protect and Sign_Personal Signature_PC Utilisateur V 2.2

PROTECT AND SIGN PERSONAL SIGNATURE : UTILISATEUR

Version du document :	2.2	**Nombre total de pages :**	70
Statut du document :	☐ Projet	☒ Version finale	
Rédacteur du document :	Emmanuel Montacutelli	DocuSign France	

Liste de diffusion :	☒ Externe	☒ Interne DocuSign France
	Public	

Historique du document :				
Date	Version	Rédacteur	Commentaires	Vérifié par
24/11/2014	2.0	EM	Création de la version 2.0 qui intègre le service « Protect and Sign (Personal Sign) »	JYF
08/01/2015	2.1	EM	Correction de fautes et erreurs typographiques	JYF
23/01/2016	2.2	EM	Modification suite au rachat de TDT par DocuSign	

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'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de DocuSign France.

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

DocuSign France a mis en place l'Autorité de Certification dénommée « KEYNECTIS K.Websign CDS » (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).

L'AC « KEYNECTIS K.Websign CDS » est certifiée par l'AC « KEYNECTIS CDS CA » elle-même signée par l'AC racine d'adobe « Adobe Root CA ». De ce fait l'AC « KEYNECTIS K.Websign CDS » est inclue dans le domaine de confiance de l'éditeur logiciel Adobe.

Le service « Protect and Sign (Personal Sign) » 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 « KEYNECTIS K.Websign CDS » et des bi-clés.

La présente PC est élaborée conformément :

- Au RFC 3647 : « X.509 Public Key Infrastructure Certificate Policy Certification Practise Statement Framework » de l'Internet Engineering Task Force (IETF) ;
- [Adobe CP for CDS]: "Adobe Systems Incorporated, CDS Certificate Policy, October 2005, Revision #14".

1.2 Identification du document

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

- AC « KEYNECTIS K.Websign CDS » :
  - avant la V4 du service « Protect and Sign (Personal Sign) » comme décrit dans la PSGP :
    - 1.3.6.1.4.1.22234.2.8.3.1 ;
  - à partir de la V4 du service « Protect and Sign (Personal Sign) » comme décrit dans la PSGP :
    - A distance (signature à distance) : 1.3.6.1.4.1.22234.2.8.3.10 ;
    - Face to face (signature en face à face) : 1.3.6.1.4.1.22234.2.8.3.8.

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

Les particularités sont identifiées dans le corps de texte directement en utilisant l'OID ou le vocabulaire « à distance » ou « face à face ».

Des éléments plus explicites comme 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 signature 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 de génération de LCR : ce service génère des Liste de Certificats Révoqués (LCR) ;
- 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 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.

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, de 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. Elle autorise et valide la création et l'utilisation des composantes de l'IGC. Elle 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. Elle valide que le Client possède des procédures spécifiques pour les services de l'AE qu'il met en œuvre. Elle valide la politique d'enregistrement du Client.

1.3.2 Autorité de Certification (AC)

L'AC génère des certificats et révoque des Certificats à partir des demandes que lui envoie l'Autorité d'Enregistrement. L'AC met en œuvre les services ; de génération de bi-clé d'AC, de génération de Certificat, de gestion des bi-clés Porteur, de gestion des données d'activation, de 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 « 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 ; d'enregistrement, gestion des données d'activation et journalisation et d'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 Sign) » 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 devra en tout état de cause respecter la politique d'enregistrement qu'elle aura préalablement défini et mises en œuvre dans le cadre de ses pratiques commerciales (Cf. § 1.3.8.2 Client).

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

1.3.4 Autorité d'Enregistrement Déléguée (AED)

Dans le cadre de la présente PC, pour le niveau « face à face », l'AE peut déléguer l'authentification et l'identification des Utilisateurs à une AED (Autorité d'Enregistrement Déléguée). Une AE ou une AED utilise des Opérateurs d'AE qui authentifient, identifient les Utilisateurs et gère la signature électronique par l'Utilisateur à l'aide d'un Terminal d'affichage. Dans la suite du document le terme « Opérateur d'AE » est utilisé pour un opérateur qui réalise des fonctions d'enregistrement des utilisateurs, indépendamment qu'il dépende d'une AE et l'AED, afin de facilité la lisibilité des exigences. De même, les exigences sont seulement rédigées pour l'AE ou un Opérateur d'AE. L'AED agît conformément aux politiques d'enregistrement, de certification et de signature du Client.

Dans tous les cas, l'AED agit conformément à la PC et à la DPC associée qui sont établies par la PMA et au contrat qui la lie à l'AE. En fonction des services qu'elle met en œuvre, l'AED respecte les exigences qui incombent à l'AE pour les services supportées. La PC ne précise donc pas les procédures avec ou sans AED. Le Client apporte ces précisions.

1.3.5 Service de Publication (SP)

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 Opérateur de Service de Certification (OSC)

L'OSC assure des prestations techniques, en particulier cryptographiques, nécessaires au processus de certification de l'AC, 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 que l'AC définit afin de répondre aux exigences de la présente PC.

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.

1.3.7 Porteurs de certificats

Désigne la personne physique qui se connecte sur l'Application du Client et qui signe le Document métier via l'Application « Protect and Sign (Personal Sign) » sur Terminal d'affichage dans le cadre d'un Protocole de consentement avec des données d'activation.

Le Porteur est aussi appelé « utilisateur » ou « signataire » dans la PSGP.

1.3.8 Autres participants

1.3.8.1 Utilisateurs de certificats (UC)

L'utilisateur de certificat est une personne qui valide le Certificat d'un Porteur dans le cadre de la validation de signature électronique de Document. L'UC agît conformément à la PSGP en qualité de Vérificateur.

1.3.8.2 Client

Le Client désigne l'entité légale, ayant signé un contrat avec DOCUSIGN FRANCE, et responsable de :

- L'application Client qui génère le Document métier à signer et qui appelle l'Application « Protect and Sign (Personal Sign) », 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 et 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.

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Certificat de l'AC

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

- La signature de Certificats de Porteur ;
- 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 utilisés par les Porteurs identifiés à l'article 1.3.7 ci-dessus pour signer électroniquement des Documents dans le cadre de Transaction électronique.

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'utilisation 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 l'AC ne peut être en aucun cas tenue pour responsable d'une utilisation des certificats qu'elle émet 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 clé 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

Coordonnées de la personne ou de la direction responsable de l'élaboration de la PC :

- DocuSign France ;
- Mr. Thibault de Valroger ;
- Contact : Director, Business Development ;
- DocuSign France – 175, rue Jean-Jacques Rousseau - 92131 Issy-les-Moulineaux Cedex – France ;
- Email: PMA-DocuSignFrance@docusign.fr ;
- Phone: (+33) (0)1 53 94 22 00 ;
- Fax: (+33) (0)1 53 94 22 01.

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

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.

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.

1.6 Définitions et Acronymes

Certaines définitions sont directement reprises de la PSGP qui les complètes et les précises.

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 Sign) » : désigne l'ensemble cohérent d'informations et de programmes informatiques propriété de DocuSign France dont une partie est hébergée et exploitée sur la plateforme « Protect and Sign (Personal Sign) » de DocuSign France et dont l'autre partie (modules logiciels Connecteur Client 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 Sign) » 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 Sign) ») 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, …).

Données d'activation Porteur : désigne les données ou actions associées à un Porteur permettant de mettre en œuvre sa clé privée. Dans le cas d'un Certificat, ces données ou actions sont définies aux termes du Protocole de consentement et sont appelées données d'authentification Utilisateur.

Données d'authentification Porteur : désigne la donnée d'activation particulière (par exemple ; mot de passe temporaire envoyé par SMS, mot de passe généré par l'Application Client et transmis par le Client à l'utilisateur, …) qui permet au Porteur de s'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 associées 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) : également appelée IGC (Infrastructure de Gestion de Clés), c'est l'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 …). 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 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 Sign) », sous lesquelles une signature électronique peut être déterminée comme valide. Une politique de signature comprend notamment les éléments suivants : (i) 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 ; (ii) 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 ; (iii) les moyens à utiliser pour vérifier le statut de révocation de chaque certificat du chemin de certification par rapport à cette référence de temps ; (iv) les caractéristiques que doit comporter le Certificat du signataire ; (v) l'ensemble des données de validation que le signataire doit fournir ; (vi) 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 détient 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 (i) la définition des actions à réaliser par l'Utilisateur sur le Terminal d'affichage pour signer le Document métier proposé par l'Application Client, (ii) les informations utilisées pour la création de l'identité Utilisateur, (iii) les modalités de contrôle par le Service des informations saisies par l'Utilisateur par comparaison aux informations fournies par le Client pour chaque Transaction, (iv) le type de fichier soumis par le Client à signature (XML/PDF…), (v) 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 cryptographique à clé publique inventé par Rivest, Shamir, et Adelman.

Service (« Protect and Sign (Personal Sign) ») : 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, …) 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 (V4) 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 identifié 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 y afférente et les contrats liés à cette PC sont différent 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 ;
- 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 est en charge de la publication des données identifiées au § 2.2ci-dessous.

2.2 Informations devant être publiées

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

- La PC : https://www.opentrustdtm.com/PC/ ;
- Les certificats des AC : https://www.opentrustdtm.com/PC/ ;
- La PSGP : https://www.opentrustdtm.com/PC/ ;
- Les certificats de la chaîne de confiance auxquels les AC sont rattachées à savoir : https://www.opentrustdtm.com/PC/ ;
- 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 est responsable de définir les modalités de communication de ces éléments aux Porteurs ;
- Les certificats de l'ACR « Adobe Root CA », de l'AC « KEYNECTIS CDS CA », de l'AC « KEYNECTIS K.Websign CDS » et du Porteur sont contenus dans le Document signé par le Porteur ;
- LCR :
    - Pour vérifier le certificat de l'AC « KEYNECTIS CDS CA » :
        - http://crl.adobe.com/cds.crl ;
    - Pour vérifier le certificat de l'AC « KEYNECTIS K.Websign CDS » :
        - http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_CDS_CA.crl ;
    - Pour vérifier le Certificat Porteur :
        - avant la V4 du service « Protect and Sign (Personal Sign) » come décrit dans la PSGP : http://crl.certificat.com/KEYNECTIS/AC_KEYNECTIS_KWA_KWEBSIGN.CDS.crl
        - à partir de la V4 du service « Protect and Sign (Personal Sign) » come décrit dans la PSGP : http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_KWebsign_CDS.crl.

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 : la communication des CGU est gérée par le Client ;
- Client et AE : sont contenues dans le contrat établit avec DocuSign France ;
- Utilisateur de certificat : les conditions d'utilisation du service IGC sont décrites dans la présente PC aux paragraphes : 1.4, 4.5.2, 5.5, 9, 9.6, 9.7, et 9.8.

2.3 Délais et fréquences de publication

La PC de l'AC et le certificat de l'AC sont disponibles en permanence et mises à jour selon les besoins suivant un taux de disponibilité définie dans la DPC.

Une nouvelle LCR est publiée toutes les 24 heures suivant un taux de disponibilité définie dans la DPC.

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.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Les identités utilisées dans un certificat sont décrites suivant la norme X.500. Dans chaque certificat X.509, 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 ACR : « Adobe Root CA »

L'identité de l'ACR dans le certificat de l'ACR est la suivante :

Champ de base	Valeur
Issuer	cn=Adobe Root CA ou=Adobe Trust Services o=Adobe Systems Incorporated c=US
Subject	cn=Adobe Root CA ou=Adobe Trust Services o=Adobe Systems Incorporated c=US

3.1.1.2 Certificat AC : « KEYNECTIS CDS CA »

L'identité de l'AC dans le certificat de l'AC est la suivante :

Champ de base	Valeur
Issuer	cn=Adobe Root CA ou=Adobe Trust Services o=Adobe Systems Incorporated c=US
Subject	cn=KEYNECTIS CDS CA ou=KEYNECTIS for Adobe o=KEYNECTIS c=FR

3.1.1.3 Certificat AC : « KEYNECTIS K.Websign CDS »

L'identité de l'AC dans le certificat de l'AC est la suivante :

Champ de base	Valeur
Issuer	cn=KEYNECTIS CDS CA ou=KEYNECTIS for Adobe o=KEYNECTIS

	c=FR
Subject	cn=KEYNECTIS K.Websign CDS ou=KEYNECTIS for Adobe o=KEYNECTIS c=FR

3.1.1.4 Certificat Porteur

L'identité du porteur dans le certificat est la suivante :

Champ de base	Valeur
Issuer	cn=KEYNECTIS K.Websign CDS ou=KEYNECTIS for Adobe o=KEYNECTIS c=FR
Subject	C = FR O = KWEBSIGN (uniquement avant la V4 du service « Protect and Sign (Personal Sign) » come décrit dans la PSGP) OU = Identifiant de Transaction OU = <Nom du Client> (avant la V4 du service « Protect and Sign (Personal Sign) » come décrit dans la PSGP) ou RA <Nom du Client> (à partir de la V4 du service « Protect and Sign (Personal Sign) » come décrit dans la PSGP) <OU= D'autres instances de l'attribut organizationalUnitName peuvent être présentes au choix du Client et dans un maximum définit par l'AC> CN = Prénom et Nom du Porteur E = adresse de courrier électronique du Porteur (uniquement avant la V4 du service « Protect and Sign (Personal Sign) » come décrit dans la PSGP)

3.1.2 Nécessité d'utilisation de noms explicites

3.1.2.1 AC

L'identité utilisée pour le certificat d'AC permet d'identifier KEYNECTIS.

3.1.2.2 Porteur

Dans tous les cas, l'identité du Porteur (Se reporter au § 3.1.1.2) est construite à partir des nom et prénom de son état civil tel que porté sur un document officiel d'identité.

Lorsque le Certificat est pour un Porteur au sein d'une Entreprise ou d'une Administration, alors l'identité de l'Entreprise ou de l'Administration peut aussi être contenue dans le Certificat dans un champ OU si le Client en a fait le Choix.

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. § **Erreur ! Source du renvoi introuvable.**).

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.

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 « KEYNECTIS CDS CA ». 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. § **Erreur ! Source du renvoi introuvable.**) 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'AC « KEYNECTIS CDS CA » 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).

3.2.2 Validation de l'identité d'un organisme

3.2.2.1 AE

L'authentification d'un Client, qui souhaite être AE, repose sur la vérification des informations fournies par le Client dans le cadre de l'établissement de la relation contractuelle avec DocuSign France.

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

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

3.2.2.2 AED

L'authentification des AED est réalisée par l'AE suivant les procédures approuvées par le Client.

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

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

Le Client doit décrire les règles d'identification, d'authentification et de gestion des AED dans la Politique d'enregistrement.

3.2.2.3 Porteur

Si le Porteur appartient à une entité légale alors l'AE doit vérifier que le Porteur appartient effectivement à l'entité légale et l'existence de l'entité légale.

L'AE qui procède à la vérification s'assure que l'entité légale du Porteur existe bien et est légalement autorisée à utiliser exclusivement son nom, en comparant les informations fournies par le Porteur aux informations recueillies dans les bases de données officielles de référence ou ses bases de données internes clients ayant déjà fait l'objet de telles vérifications.

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

Le Client doit décrire les règles d'identification, d'authentification et de gestion des Porteurs dans la Politique d'enregistrement.

3.2.3 Validation de l'identité d'un individu

3.2.3.1 Opérateur d'AE

Les Opérateurs d'AE sont identifiés et authentifié suivant la politique d'enregistrement établie par le Client et validée par DocuSign France.

3.2.3.2 Porteur : face à face : 1.3.6.1.4.1.22234.2.8.3.8 et 1.3.6.1.4.1.22234.2.8.3.1

Dans le cadre du niveau « face à face », le Client s'engage à informer chaque AE et AED des obligations prévues au présent article et de celles qui lui incombent.

A cet égard, le Client devra s'assurer du respect par chaque AE et AED des obligations suivantes :

- Identifier et authentifier les Utilisateurs lors du face-à-face par l'Opérateur d'AE en demandant à chaque Utilisateur de présenter une pièce d'identité officielle (un original en cours de validité) ;
- Documenter ses règles de vérification de la ressemblance entre les informations de l'Utilisateur portées sur le Terminal d'affichage, les informations portées sur sa pièce d'identité officielle présentée à l'Opérateur d'AE et, pour les professionnels seulement, les informations portées dans les justificatifs d'appartenance à une entité légale le cas échéant sa fonction au sein de l'entité légale ;
- Mettre en forme les informations d'Identité Utilisateur, notamment en reportant, dans le Document Métier, les nom et prénoms figurant sur les justificatifs d'identité ou obtenus le protocole utilisé pour vérifier l'identité de l'Utilisateur ;
- Assurer la sécurisation des « Terminaux d'Affichage » utilisés par les Opérateurs d'AE pour se connecter, transmettre les données à l'Application Client et à l'Application « Protect and Sign (Personal Sign) » et réaliser le Protocole de consentement ;
- Collecter et conserver une copie des pièces justificatives de l'identité de l'Utilisateur ainsi que les données d'identité et d'authentification ;
- Respecter la Politique de signature et la politique d'enregistrement de l'AE ainsi que la Politique de Certification Utilisateur applicable ;
- Informer l'Utilisateur de la gestion de ses données personnelles et des conditions générales d'utilisation de la signature électronique.

En outre, le Client veillera à ce que chaque AE et AED n'utilise le Service que pour des Transactions conclues avec un Porteur sur le lieu de vente, au moyen des seuls outils prévus à cette fin (Terminal d'affichage), et uniquement à des fins de signature de Documents métiers du Client en conformité avec la Politique de signature définie par le Client.

Enfin, il devra informer chaque AE et AED de leur obligation de l'alerter immédiatement pour tout incident de sécurité survenant sur son Terminal d'affichage et/ou sur le lieu de vente. Le Client s'engage par suite à en informer sans délai DOCUSIGN FRANCE.

En tout état de cause, le Client se porte-fort du respect par chaque AE et AED des obligations définies dans la présente PC.

3.2.3.3 Porteur : à distance : 1.3.6.1.4.1.22234.2.8.3.10 et 1.3.6.1.4.1.22234.2.8.3.1

Dans le cadre du niveau « à distance », le Client s'engage à informer chaque AE et AED des obligations prévues au présent article et celles qui leur incombent.

A cet égard, le Client devra s'assurer du respect par chaque AE des obligations suivantes :

- Identifier et authentifier les Utilisateurs
    - Si l'Utilisateur n'a pas fait l'objet d'une vérification d'identité préalable, l'AE doit s'assurer de l'identification et l'authentification des Utilisateurs par l'Opérateur d'AE ou le processus automatique équivalent en demandant à chaque Utilisateur de transmettre des justificatifs d'identité (par exemple une pièce d'identité officielle dans le cadre de l'ouverture d'un compte en ligne) ou d'utiliser un autre moyen équivalent (utilisation d'un processus automatisé qui permette d'authentifier l'Utilisateur à partir d'une base de connaissance ou qui s'appuie sur un tiers ayant déjà authentifié l'Utilisateur) ;
    - Si l'Utilisateur a déjà fait l'objet d'une vérification d'identité préalable par l'AE ou par un tiers reconnu par l'AE, l'AE doit utiliser un moyen d'authentification permettant de s'assurer que l'Utilisateur est bien la personne ayant fait l'objet de la vérification initiale (exemple : utilisation d'un compte protégé par un mot de passe, envoi d'un code unique aléatoire par SMS sur un numéro de téléphone mobile vérifié comme étant celui de l'Utilisateur, certificat, etc…) ;

- Documenter ses règles de vérification des pièces justificatives ;
- Mettre en forme les informations d'Identité Utilisateur, notamment en reportant, dans le Document Métier, les noms et prénoms figurant sur les justificatifs d'identité ou le protocole utilisé pour vérifier l'identité de l'Utilisateur ;
- Collecter et conserver une copie des pièces justificatives de l'identité de l'Utilisateur ainsi que les données d'identité et d'authentification collectées lors de la vérification d'identité initiale
- Respecter la Politique de signature et la politique d'enregistrement de l'AE ainsi que la Politique de Certification Utilisateur applicable ;
- Informer l'Utilisateur de la gestion de ses données personnelles et des conditions générales d'utilisation de la signature électronique.

En outre, le Client veillera à ce que chaque AE n'utilise le Service que pour des Transactions conclues avec un Utilisateur dans le cadre de l'Application Client et uniquement à des fins de signature de Documents métiers du Client en conformité avec la Politique de signature définie par le Client.

Enfin, il devra informer chaque AE de leur obligation de l'alerter immédiatement pour tout incident de sécurité survenant. Le Client s'engage par suite à en informer sans délai DOCUSIGN FRANCE.

En tout état de cause, le Client se porte-fort du respect par chaque AE des obligations définies dans la présente PC.

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) et son autorisation par un représentant légal de l'organisation.

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.

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

Un nouveau Certificat ne peut pas être fourni au Porteur sans renouvellement de la bi-clé correspondante.

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

Sans objet car les Certificats ne sont pas révocable.

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

Sans objet car les Certificats ne sont pas révocable.

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.

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

4.1.2.1 AC

Les ACs sont enregistrées auprès de la PMA.

Une demande de création d'AC contient l'identifiant de l'AC « KEYNECTIS CDS CA » qui signe son certificat.

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

4.1.2.2 Porteur

Le Client décrit dans sa politique d'enregistrement les informations et les processus qui sont utilisées pour enregistrer un Porteur. Si le Protocole de consentement nécessite de contacter le Porteur (via SMS ou adresse de courrier électronique), alors l'AE doit collecter l'adresse de courrier électronique ou le numéro de téléphone utilisé par le Porteur.

Lorsqu'une AED est utilisée alors la garantie de l'origine de la demande doit être garantie.

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.

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 ou l'AED identifie et authentifie le Porteur (Cf. § 3.2.2 et le 3.2.5).

L'AE ou l'AED s'assure que le porteur a pris connaissance des conditions générales d'utilisation.

L'AE conserve dans ses journaux l'ensemble des informations qui composent le dossier d'enregistrement.

Lorsque l'AE passe par une AED, alors l'AED peut conserver l'ensemble des informations qui composent le dossier d'enregistrement.

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. En cas d'acceptation, la PMA, DocuSign France procède à la cérémonie des clés et à la création du certificat d'AC en fonction de la demande.

4.2.2.2 Porteur

Si une AED est utilisé, alors l'AED transmet la demande à l'AE.

En cas d'approbation de la demande, l'AE transmet la demande à l'AC dans le cadre de 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 définit par la PMA.

4.2.3.2 Porteur

La durée du traitement est liée au processus de signature électronique et est immédiate suite à 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

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

Le Porteur déclenche l'utilisation de sa bi-clé dans l'Application « Protect and Sign (Personal Sign) » suivant le Protocole de consentement choisi par le Client et décrit dans la politique de signature.

L'AC authentifie le Porteur en utilisant les Données d'activation que le Porteur soumet lors du Protocole de consentement (Cf. § 6.2.8).

La bi-clé du Porteur est utilisée par l'Application « Protect and Sign (Personal Sign) » 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 et la PSGP. Suite à l'opération de signature l'Application « Protect and Sign (Personal Sign) » détruit la bi-clé du Porteur (Cf. § 6.2.10).

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

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

Il n'y a pas de notifications particulières de la délivrance du certificat. Le certificat est temporaire et utilisé immédiatement dans les opérations de signature électronique.

Le certificat est intégré au Document signé du Porteur.

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.

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.

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 § **Erreur ! Source du renvoi introuvable.**). 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.

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.

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.

Il est interdit de prolonger ainsi les bi-clés d'AC. Par défaut, il n'existe pas de prolongation des clés d'AC. Ce cas peut être autorisé si les conditions opérationnelles des applications utilisatrices le requièrent et qu'il n'existe pas d'autre solution. En ce cas, la PMA pourra accepter ce type de renouvellement uniquement si les recommandations en matière cryptographique (portant sur les algorithmes de signature et les algorithmes de calcul d'empreinte) le permettent et que ce renouvellement n'engendre pas un risque pour les applications utilisatrices.

Au plus, un seul renouvellement de certificat sans changement de bi-clé d'AC est autorisé.

Dans tous les cas, pour le changement de certificat d'AC, la procédure à suivre est identique à la procédure initiale de certification décrite aux § 3.2 et § 4.1, § 4.2 et § 4.3 ci-dessus.

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, § **Erreur ! Source du renvoi introuvable.**, § 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, § **Erreur ! Source du renvoi introuvable.**, § 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.

Il est interdit de prolonger ainsi les bi-clés d'AC. Par défaut, il n'existe pas de prolongation des clés d'AC. Ce cas peut être autorisé si les conditions opérationnelles des applications utilisatrices le requièrent et qu'il n'existe pas d'autre solution. En ce cas, la PMA pourra accepter ce type de renouvellement uniquement si les recommandations en matière cryptographique (portant sur les algorithmes de signature et les algorithmes de calcul d'empreinte) le permettent et que ce renouvellement n'engendre pas un risque pour les applications utilisatrices.

Au plus, un seul renouvellement de certificat sans changement de bi-clé d'AC est autorisé.

Dans tous les cas, pour le changement de certificat d'AC, la procédure à suivre est identique à la procédure initiale de certification décrite aux § 3.2 et § 4.1, § 4.2 et § 4.3 ci-dessus.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

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, 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) ;

- Cessation d'activité de l'entité opérant la composante.

4.9.1.2 Certificat Porteur

Sans objet.

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

Sans objet.

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.

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.

4.9.3.2 Certificat porteur

Sans objet.

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 § **Erreur ! Source du renvoi introuvable.**.

4.9.4.2 Porteur

Sans objet.

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

4.9.5.1 Certificat Composantes IGC

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

Sans objet.

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).

4.9.7 Fréquences d'établissement des LCR

La LCR signée, qui a une validité de 7 jours, par l'AC est émise toutes les 24 Heures mais ne contient pas de Certificat révoqué.

4.9.8 Délai maximum de publication d'une LCR

Le délai maximum de publication d'une LCR suite à sa génération est de 30 minutes.

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

L'AC met en œuvre un serveur OCSP dont l'URL est : http://ocsp.certificat.com/keynectis-kwebsign-cds.

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

Cf. chapitre 4.9.6 ci-dessus.

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 suite à 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 des LCR émises par 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. Ces LCR sont des LCR au format V2.

4.10.2 Disponibilité de la fonction

Le service OCSP est mis à jour à partir des LCR émises par l'AC. Le service est disponible 24 heures sur 24 et 7 jours sur 7 suivant un taux de disponibilité préciser dans la DPC. Lorsque la fonction de vérification en ligne du statut d'un certificat (OCSP) est mise en œuvre, le temps de réponse du serveur à la requête reçue est fixé à un maximum donné dans la DPC.

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'AC 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,...) réalisées par l'OSC.

5.1.2 Accès physique

Afin de limiter l'accès aux applications et aux informations de l'IGC et afin d'assurer la disponibilité du système d'exploitation de l'AC, l'OSC, l'AED et l'AE mettent en place un périmètre de sécurité opéré pour ses besoins. La mise en œuvre de ce périmètre permet de respecter les principes de séparation des rôles de confiance telle que prévus dans cette PC.

Les accès au site de l'OSC, de l'AED et de l'AE, qui mettent en œuvre les services d'IGC, sont limités aux seules personnes nécessaires à la réalisation des services. Tout évènement de sécurité fait l'objet d'un enregistrement et d'un traitement.

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 et l'AE permettent de respecter les exigences et les engagements pris par l'AC, l'AED et l'AE dans la présente PC, en matière de disponibilité de ses fonctions.

5.1.6 Mise hors service des supports

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

5.1.7 Sauvegardes hors site

L'OSC réalise des sauvegardes hors site permettant une reprise rapide des services d'IGC suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ses services.

Les précisions quant aux modalités des sauvegardes des informations sont fournies dans la DPC.

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 classés en 5 groupes :

- Les personnels d'exploitation, dont la responsabilité est le maintien de des systèmes qui supportent l'IGC en conditions opérationnelles de fonctionnement ;
- Les personnels d'administration, dont la responsabilité est l'administration technique des composantes de l'IGC ;

- Les personnels opérationnels dont la responsabilité est de mettre en œuvre les fonctions d'IGC ;
- Les personnels de « sécurité », dont la responsabilité est de réaliser les opérations de vérification de la bonne application des mesures et de la cohérence de fonctionnement de la composante d'IGC ;
- Les personnels porteurs de données d'activation de clé.

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.

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 ;
- Eventuellement, 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.

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

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, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC.

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.

5.3 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.

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

de la personne, 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 conflit 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.

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

Des précisions sont fournies dans la DPC.

5.3.6 Sanctions en cas d'actions non autorisées

Des précisions sont fournies dans la DPC.

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

Des précisions sont fournies dans la DPC.

5.3.8 Documentation fournie au personnel

Des précisions sont fournies dans la DPC.

5.4 Procédures de constitution des données d'audit

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.

5.4.1 Type d'événements à enregistrer

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 ;
- Evènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à 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,...).

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 ;
- Evènements liés aux clés d'AC et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, destruction,...) ;
- Génération des Certificats de Porteurs ;
- Génération, utilisation et destruction des bi-clés de 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 ;
- 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.

Selon le type de l'évènement concerné, les champs suivants peuvent être enregistrés:

- Destinataire de l'opération ;
- Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande ;
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- Cause de l'évènement ;
- Toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

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

- Les dossiers Porteurs (Cf. § 4.1 et § 4.2) ;
- Les informations de contacts du Porteur (adresse de courrier électronique ou numéro de téléphone) qui doivent être dans le Fichier de preuve (Cf. § 4.1 et § 4.2) ;
- La liste des Opérateur d'AE ;
- Les demandes issues de l'AED ;
- Les pages techniques du Protocole de consentement ;
- Les traces liées à la gestion du Connecteur Client.

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 opérations de journalisation sont effectuées au cours du processus considéré. En cas de saisie manuelle, l'écriture se fera, sauf exception, le même jour ouvré que l'évènement. Des précisions sont fournies dans la DPC.

5.4.3 Période de conservation des journaux d'événements

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).

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.4 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.

5.4.5 Système de collecte des journaux d'événements

Des précisions sont fournies dans la DPC.

5.4.6 Evaluation des vulnérabilités

L'AC et l'AE 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.

Les journaux sont analysés au moins à une fréquence mensuelle. 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.

5.5 Archivage des données

L'archivage des données permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

5.5.1 Type de données à archiver

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

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- La politique de certification ;
- La déclaration des pratiques de certification ;
- Les certificats tels qu'émis ou publiés ;
- Les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement (pour les entreprises et les administrations) ;
- Les dossiers complets de demandes de certificats ;
- Les journaux d'évènements des différentes entités de l'IGC.

L'AE doit conserver ses journaux (Cf. 5.4.1) et les Fichiers de preuve.

5.5.2 Période de conservation des archives

Certificats et LCR émis par l'AC

Les certificats de porteur et d'AC sont archivés 5 ans après leur expiration.

Journaux d'événements

Les journaux techniques d'évènements traités au chapitre 5.4 sont archivés pendant 5 ans après leur génération.

Dossier de demande de Certificat

L'AE doivent conserver ses journaux (Cf. § 5.4.1) et les Fichiers de preuve pendant 5 ans minimum.

L'AED doit conserver ses journaux (Cf. § 5.4.1) pendant 3 ans maximum.

5.5.3 Protection des archives

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

- Seront protégées en intégrité ;
- seront accessibles aux seules personnes autorisées ;
- pourront être consultées et exploitées.

5.5.4 Exigences d'horodatage des données

Si un service d'horodatage est utilisé pour dater les enregistrements, il doit répondre aux exigences formulées à l'article 6.8.

5.5.5 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 5.5.3).

5.5.6 Procédures de récupération et de vérification des archives

Les archives papier sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées. Les sauvegardes électroniques archivées sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées.

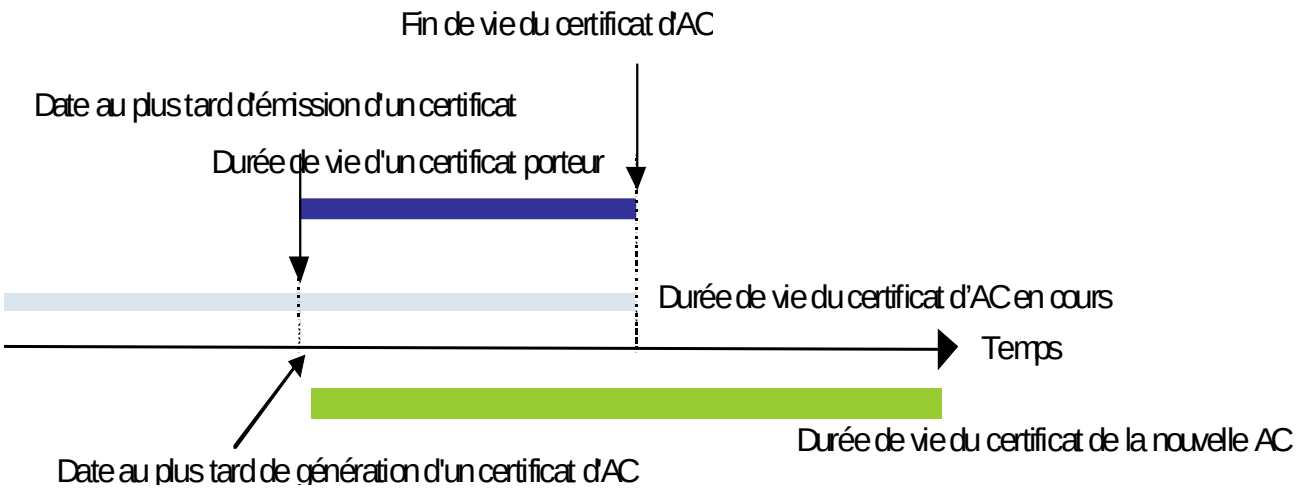
5.6 Changement de clé d'AC

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 DPC précise les standards utilisés.

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.

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.



Par ailleurs, l'AC change sa bi-clé 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 validité d'un certificat est de 5 minutes.

5.7 Reprise suite à 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 corruption 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.

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'AC 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'AC détecte une tentative de piratage ou une autre forme de compromission, elle mène une analyse afin de déterminer la nature des conséquences et leur niveau. Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors l'AC :

- 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.

Si nécessaire, l'ampleur des conséquences est évalué par l'AC 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 détecte une tentative de piratage ou une autre forme de compromission, elle mène 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 Document signés, le Client doit avertir DocuSign France.

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 service de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC.

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 ;
- 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.

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. Le SP est installé afin d'être disponible 24 heures sur 24 et 7 jours sur 7.

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 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.

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 entités affectées ;
- 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 ;
- Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- Révoque son certificat ;
- Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- Informe (par exemple par récépissé) tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

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.

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

Suite à 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 deux 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 d'au moins un témoin. Le témoin atteste, 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.

Suite à 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 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 suite à 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…) 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 SHA1 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-1 (avant la V4 du service « Protect and Sign (Personal Sign) » come décrit dans la PSGP) ou SHA-256 (à partir de la V4 du service « Protect and Sign (Personal Sign) » come décrit dans la PSGP).

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

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+.

6.1.7 Objectifs d'usage de la clé

L'utilisation du champ "key usage" dans le certificat porteur et certificat AC est la suivante :

- AC :
    - Key CertSign ;
    - Key CRL Sign ;
- Porteur :
    - : Digital signature.

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 utilise 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.

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

Suite à l'authentification réussie du Porteur lors du Protocole de consentement, et à l'aide de ses données d'activation, la bi-clé Porteur est utilisée dans un HSM. L'authentification est mise en œuvre conformément à la politique de signature et la PSGP.

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.

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

Les clés privées Porteurs 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).

6.2.8 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.

6.2.8.2 Porteur

Suite à l'authentification réussie du Porteur lors du Protocole de consentement, et à l'aide de ses données d'activation, la bi-clé Porteur est utilisée dans un HSM. L'authentification est mise en œuvre conformément à la politique de signature et la PSGP.

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.

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 à ce qu'aucune information ne puisse être utilisée pour la retrouver.

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 matérielle de la bi-clé et cette opération est pilotée par l'Application « Protect and Sign (Personal Sign) ».

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

Se reporter au § 6.1.6.1.

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

Comme une AC ne peut émettre de certificats porteurs d'une durée de vie supérieure à celle de son propre certificat, la bi-clé et le certificat auquel elle correspond sont renouvelés au plus tard à la date d'expiration du certificat d'AC moins la durée de vie des certificats porteurs émis.

6.3.2.2 Porteur

La durée de vie opérationnelle d'un certificat est limitée par son expiration. 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.

6.4.1.2 Porteur

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 (1.3.6.1.4.1.22234.2.8.3.10).

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.

6.4.2.2 Porteur

L'AE et l'Application Protect and Sign (Personal signature) sont responsable de la protection des données d'activation.

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

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) ;
- Eventuellement, 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.

6.5.2 Niveau de qualification des systèmes informatiques

Les composants d'IGC utilisés pour supporter les services d'AC et qui sont hébergés par l'OSC ont été conçus en suivant les recommandations du document du CEN CWA 14167-1 "Security requirement for trustworthy system managing digital certificates for electronic signatures".

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.

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.

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 réseau non utilisés sont coupés. 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.

6.8 Horodatage / Système de datation

Il n'y a pas d'horodatage utilisé par l'IGC mais une datation sûre. 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 de l'AC;
- De la révocation d'un certificat de l'AC;
- De l'affichage de mises à jour de LCR.

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

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.

7.1.1 Extensions de Certificats

Cf. § 10.

7.1.2 Identifiant d'algorithmes

Cf. § 10.

7.1.3 Formes de noms

Cf. § 10.

7.1.4 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.

7.1.5 Extensions propres à l'usage de la Politique

Sans objet.

7.1.6 Syntaxe et Sémantique des qualificateurs de politique

Sans objet.

7.1.7 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

La DPC donne le détail.

7.3 Profil OCSP

La DPC donne le détail.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquence et/ou circonstances des audits

L'ensemble des composantes de l'IGC (y compris les AE et les AED) fait l'objet d'audits de conformité, réalisés par DocuSign France, de manière régulière, pour permettre à la PMA d'autoriser l'AC et l'AE d'émettre ou non (selon le résultat des audits) des Certificats Porteurs au titre de la présente PC.

Le Client est donc averti qu'en sa qualité d'AE il peut être soumis à des audits de la part de DocuSign France. De même, les AED peuvent aussi être auditée par DocuSign France.

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.

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 de l'AC 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.

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 et des données d'activation des Porteurs ;
- L'authentification des Porteurs par l'AE et/ou l'AED dans le cadre de la Cinématique de signature et de la politique d'enregistrement et du Protocole de consentement ;
- La gestion des AE et des AED ;
- L'archivage des Fichier de preuve et des journaux de l'AE et de l'AED ;
- La gestion des Documents par l'Application Client présentés au Porteur dans le cadre de la politique de signature.

8.5 Actions prises suite aux 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 non-conformité avec les exigences de la présente PC, les mesures suivantes doivent être prises :

- L'auditeur note la non-conformité ;
- L'auditeur avise l'entité en question de la non-conformité. L'entité en avise rapidement la PMA ;

- La partie responsable de la correction de la non-conformité 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, la gravité et la rapidité avec laquelle la non-conformité 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'elle 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 ou une AED, la PMA remet le rapport d'audit de l'AE et/ou de l'AED au Client.

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.

9.2 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 :

- La partie non-publique de la DPC de l'AC ;
- 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 du Porteur ;
- Les bi-clés du Connecteur Client ;
- La politique de sécurité interne de l'AC ;

- 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 sur le territoire français. 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 sur le territoire français, en particulier de la loi CNIL.

Le Client veille à ce que l'AE et les AED appliquent une politique de gestion des données personnelles, conformément à la loi européenne et comme stipuler dans le contrat entre le Client et DOCUSIGN FRANCE, afin de protéger les informations personnelles qu'elles recueillent.

9.4.2 Informations à caractère personnelles

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.

9.4.3 Informations à caractère non personnel

Sans objet.

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 contenues 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 contenues dans les CGU.

Les infractions aux dispositions de la loi Informatique et Libertés du 6 janvier 1978 sont prévues et réprimées par les articles 226-16 à 226-24 du code pénal.

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 exprès et préalable de la part du Porteur. Le consentement du Porteur pour l'utilisation desdites données comme définie 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 les concernant recueillies par l'IGC fassent l'objet d'un traitement informatique aux seules fins : d'être authentifié par l'AE, et le cas échéant l'AED, de 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 des autorités judiciaires sur décision judiciaire ou autre autorisation légale aux données à caractère personnel.

9.4.7 Autres circonstances de divulgation d'informations personnelles

L'AC et l'AE obtiennent l'accord du Porteur (se reporter au § 9.4.5) 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, …) 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 légales 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.

9.6.1 Obligations communes

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 leur personnel respectif ayant à en connaître dans le cadre des fonctions qui lui 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.

9.6.2 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 ;
- Le contrôle de la relation contractuelle avec le Client agissant en tant qu'AE ;
- La documentation des schémas de certification qu’elle entretient avec des AC tierces.

9.6.3 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 ;
- 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) ;
- Prendre toutes les mesures raisonnables pour s’assurer que ses 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.

9.6.4 Obligations de l’AE

Les obligations de l'AE sont les suivantes :

- Avant de permettre la signature d'un Document par un Porteur, l'AE doit rendre disponible les CGU au Porteur ;
- 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 aux Porteurs ;
- L'authentification du Porteur et la collecte des pièces justificatives permettant de créer l'identité du Porteur ;
- Protéger les données personnelles du Porteur ;
- Gérer les AED 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 ;
- 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.

9.6.4.1 Obligations et garanties de l'AED

Les obligations de l'AED sont :

- L'authentification du porteur ;
- 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 ;
- Respecter la PC et la DPC de l'AC ;
- Respecter les obligations qui la lient à l'AE.

9.6.5 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 leur clé privées et/ou de l'AC ;
- Signer le contrat qui le lie à DocuSign France en l'engage en qualité d'AE ;
- 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 Protocol 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.

9.6.6 Obligations et garanties du porteur

Les obligations du porteur sont :

- Protéger en confidentialité et intégrité les informations confidentielles qu'il détient, donnée d'activation, 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 il 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.

9.6.7 Obligations et garanties du SP

Les obligations du SP sont :

- De publier les LCR ;
- De publier les certificats d'AC ;
- De garantir les taux de disponibilités des informations publiées ;
- De protéger les accès au SP.

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 si 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

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 retards, 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 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.

9.11 Amendements à la PC

9.11.1 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.

9.11.2 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, …) et non sur la forme de la PC et de la DPC.

9.11.3 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).

9.12 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 autre, 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.

9.13 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 règle le litige conformément aux règles établies dans le contrat entre le Client et DocuSign France.

9.14 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'accorde sur le droit applicable dans le contrat établit entre DocuSign France le Client.

9.15 Disposition diverses

9.15.1 Accord global

Le cas échéant, la DPC précisera les exigences spécifiques.

9.15.2 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.

9.15.3 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.

9.15.4 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.

9.15.5 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.

9.16 Autres dispositions

Le cas échéant, la DPC en fournira les détails.

10 PROFIL DE CERTIFICAT

10.1 AC

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = KEYNECTIS OU = KEYNECTIS for Adobe CN = KEYNECTIS CDS CA		
NotBefore	jeudi 31 janvier 2008 01:00:00		
NotAfter	mercredi 31 janvier 2018 01:00:00		
Subject	**Attribute type**	**Attribute value**	**Directory String1**
	C	FR	PrintableString
	O	KEYNECTIS	PrintableString
	OU	KEYNECTIS for Adobe	PrintableString
	CN	KEYNECTIS K.Websign CDS	PrintableString
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	Sha1WithRSAEncryption (1.2.840.113549.1.1.5)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		9f 22 78 d7 71 1b de 33 b0 7f c9 20 7a a9 a8 e0 4e 62 e3 fb
Subject Key Identifier	**FALSE**	
Methods of generating key ID		ae 17 c5 29 d1 d9 51 e5 f9 04 d2 68 5a 28 92 e7 8f df 67 d7
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Extended Key Usage	**FALSE**	
Documents Acrobat authentiques 1.2.840.113583.1.1.5		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.keynectis.com/PC/
policyQualifier-unotice		This certificate has been issued in accordance with the Acrobat Credentials CPS
Basic Constraint	**TRUE**	
cA		True
pathLenConstraint		0
CRL Distribution Points	**FALSE**	
distributionPoint		http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_CDS_CA.crl

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

Extensions	Criticality (True/False)	Value
Reasons		n/a
cRLIssuer		n/a

10.2 Porteur : 1.3.6.1.4.1.22234.2.8.3.1

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	CN = KEYNECTIS K.Websign CDS OU = KEYNECTIS for Adobe O = KEYNECTIS C = FR		
NotBefore	YYYY/MM/DD HH:MM:SS Z (date d'émission du Certificat)		
NotAfter	YYYY/MM/DD HH:MM:SS Z plus 5 minutes		
Subject	**Attribute type**	**Attribute value**	**Directory String2**
	DN	Cf. 3.1.1.4	PrintableString
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	Sha1WithRSAEncryption (1.2.840.113549.1.1.5)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		ae 17 c5 29 d1 d9 51 e5 f9 04 d2 68 5a 28 92 e7 8f df 67 d7
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
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.8.3.1
policyQualifier-cps		http://www.keynectis.com/PC/
policyQualifier-unotice		This certificate has been issued in accordance with the Adobe CDS CPS and KEYNECTIS CDS CPS OID 1.3.6.1.4.1.22234.2.8.3.1
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		N/A
CRL Distribution Points	**FALSE**	
distributionPoint		http://crl.certificat.com/KEYNECTIS/AC_KEYNECTIS_KWA_KWEBSIGN.CDS.crl
Reasons		n/a
cRLIssuer		n/a

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

10.3 Porteur : 1.3.6.1.4.1.22234.2.8.3.8

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	CN = KEYNECTIS K.Websign CDS OU = KEYNECTIS for Adobe O = KEYNECTIS C = FR		
NotBefore	YYYY/MM/DD HH:MM:SS Z (date d'émission du Certificat)		
NotAfter	YYYY/MM/DD HH:MM:SS Z plus 5 minutes		
Subject	**Attribute type**	**Attribute value**	**Directory String3**
	DN	Cf. 3.1.1.4	PrintableString
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		ae 17 c5 29 d1 d9 51 e5 f9 04 d2 68 5a 28 92 e7 8f df 67 d7
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Extended Key Usage	**FALSE**	
Documents Acrobat authentiques		1.2.840.113583.1.1.5
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.8.3.8
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		This certificate has been issued in accordance with the Adobe CPS, OpenTrust Certificate Policy and OpenTrust PSGP 1.3.6.1.4.1.22234.2.4.6.1.6
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		This certificate has been issued also in accordance with the Adobe CPS.
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		N/A
CRL Distribution Points	**FALSE**	
distributionPoint		http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_KWebsign_CDS.crl
Reasons		n/a

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

Extensions	Criticality (True/False)	Value
cRLIssuer		n/a
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.certificat.com/keynectis-kwebsign-cds
Subject Alternative Name	**FALSE**	
rfc822Name		<adresse de courrier électronique du Porteur>
Time stamping	**FALSE**	http://tsp.certificat.com/tsa-cds

10.4 Porteur : 1.3.6.1.4.1.22234.2.8.3.10

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	CN = KEYNECTIS K.Websign CDS OU = KEYNECTIS for Adobe O = KEYNECTIS C = FR		
NotBefore	YYYY/MM/DD HH:MM:SS Z (date d'émission du Certificat)		
NotAfter	YYYY/MM/DD HH:MM:SS Z plus 5 minutes		
Subject	**Attribute type**	**Attribute value**	**Directory String[4]**
	DN	Cf. 3.1.1.4	PrintableString
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		ae 17 c5 29 d1 d9 51 e5 f9 04 d2 68 5a 28 92 e7 8f df 67 d7
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)
Key Usage	**TRUE**	
Digital Signature		Set
Extended Key Usage	**FALSE**	
Documents Acrobat authentiques		1.2.840.113583.1.1.5
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.8.3.10
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		This certificate has been issued in accordance with the Adobe CPS, OpenTrust Certificate Policy and OpenTrust PSGP 1.3.6.1.4.1.22234.2.4.6.1.5
policyIdentifier		1.2.840.113583.1.2.1

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

Extensions	Criticality (True/False)	Value
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		This certificate has been issued also in accordance with the Adobe CPS.
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		N/A
CRL Distribution Points	**FALSE**	
distributionPoint		http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_KWebsign_CDS.crl
Reasons		n/a
cRLIssuer		n/a
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.certificat.com/keynectis-kwebsign-cds
Subject Alternative Name	**FALSE**	
rfc822Name		<adresse de courrier électronique du Porteur>
Time stamping	**FALSE**	http://tsp.certificat.com/tsa-cds