POLITIQUE D'ENREGISTREMENT

Extension de la Politique de Certification de DOCUSIGN FRANCE pour le service d’Autorité d’Enregistrement avec l'utilisation de la plateforme QUICKSIGN comme service d'enregistrement pour l'identification des souscripteurs dans le cadre d’une entrée en relation bancaire.

Version	0.9	
Statut	☒ Draft	☐ Final
Auteur	Ahmed Boussadia	QUICKSIGN

Liste de diffusion	☐ Interne	☒ Externe
		Public

Histoire				
Version	Date	Auteur	Commentaires	Statut
V.0.9	16/06/2022	A.Boussadia	Création du document	Draft
V.0.91	30/11/2022	A.Bedeau	Mise à jour du document	Draft
V1.0	23/10/2023	A.Boussadia	Relecture et intégration des remarque de la conformité DocuSign France et validation du document	Validée

TABLE DES MATIERES

1. Introduction

1.1. Vue d'ensemble

Cette politique d'enregistrement (PE) complète le document "Protect_and_Sign_Personal_Signature_PC_Utilisateur" de DocuSign France pour la partie service d'enregistrement de l'Autorité d'Enregistrement. Elle explique comment le service d'enregistrement d'un Client opéré par QuickSign remplit les conditions requises pour les Autorités d'Enregistrement (AE) émettant des certificats avancés.

Dans ce contexte, le Client de QuickSign agît en tant qu'Autorité d'Enregistrement (AE) et utilise la plateforme de QuickSign comme service d'enregistrement pour identifier les Souscripteurs demandant des signatures personnelles basées sur des Certificats émis par l'Autorité de Certification (AC), « DOCUSIGN CLOUD SIGNING CA - SI1 », de DocuSign France.

Ce RP est basé sur :

- [PC] : Protect_and_Sign_Personal_Signature_PC_Utilisateur_V_2_6 (disponible ici : https://www.docusign.fr/fr-fr/mentiones-legales/politiques-de-certifications/ et identifiée par l'OID 1.3.6.1.4.1.22234.2.14.3.33).
- [PSMP] : " Proof Signature and Management Policy ", version 1.7 minimum qui définit le processus technique de signature électronique et d'interaction avec l'AE.
- RFC 3647 " Certificate Policy and Certification Practices Framework " publié par l'Internet Engineering Task Force (IETF).

La structure du document est conforme à la PC Protect_and_Sign_Personal_Signature_PC_Utilisateur_V_2_6.

1.2. Nom et identification du document

Dans le contexte de ce document, l'OID DOCUSIGN FRANCE CP à considérer est :

- OID = 1.3.6.1.4.1.22234.2.14.3.33 : Ce profil est implémenté par la nouvelle AC « DOCUSIGN CLOUD SIGNING CA - SI1 » de DocuSign France et est conforme à l'article 26 de eIDAS.

1.3. Composants de l'Infrastructure de Gestion de Clé (IGC)

1.3.1. Autorité d'enregistrement (AE)

L'AE, qui est le Client de QuickSign, est un établissement qui est soumis à la législation d'anti-blanchiment et de financement du terrorisme. C'est un établissement supervisé par une autorité de régulation bancaire comme par exemple l'ACPR en France.

L'AE s’appuie sur la plateforme du Prestataire Technique d’AE qui est détenue et exploitée par QUICKSIGN.

L'AE prend en charge les services IGC suivants pour tous les cas :

- Définir les règles d’entrée en relation avec le Signataire conforme aux exigences du régulateur bancaire ;
- Identification et authentification initiales du Souscripteur conforme aux règles établies dans la présente PE ;
- La collecte, la vérification et la conservation des documents d’identité (par exemple une carte nationale d’identité) et informations de contact (par exemple email et numéro de téléphone portable) utilisés pour identifier le Signataire ;
- La collecte et la conservation des Fichier de Preuves générés par le Prestataire Technique d’AE ;
- La mise en œuvre du Protocole de Consentement en utilisant le Prestataire Technique d’AE ;
- Le cas échéant, mise à jour du document d'identité officiel et des données d'enregistrement (email, numéro de téléphone...) après avoir dûment vérifié que le lien entre les données d'enregistrement mises à jour et l'Signataire reste exact ;
- Le cas échéant, l'authentification du souscripteur par un moyen d'authentification sécurisé avec un accès à distance via un portail de l’AE ;
- Établissement d'une relation contractuelle avec un ou des prestataires techniques en charge de la réalisation de contrôles sur la vérification d’identité ;
- Création d'un journal de bord et enregistrement des informations d'enregistrement.

1.3.2. Prestataire technique d’Autorité d'enregistrement

Le Prestataire technique d’AE est QUICKSIGN.

Le prestataire technique exécute dans les conditions de sécurité conforme à cette PE les traitements définis par l’AE.

Le prestataire technique prend en charge les services suivants :

- Envoyer de la demande de certificat et les documents à signer à l'AC ;
- Créer le Fichier de Preuve et le faire sceller et horodater ;
- Mettre à disposition pour l’AE le Fichier de Preuve ;
- Déployer le Protocole de Consentement ;
- Récupérer les informations de contacts et d’identité du Signataire.

Toutes les informations échangées entre l'AE et son prestataire le sont de manière sécurisée, selon les procédures définies par l'AE dans ses spécifications techniques.

Les obligations du prestataire sont définies dans le contrat entre l'AE et le prestataire.

1.4. Utilisation du certificat

Le seul usage du Certificat couvert par cette PE est la vérification de la signature électronique apposée sur les documents utilisant le service d'enregistrement de QUICKSIGN. QUICKSIGN n'est pas responsable de toute autre utilisation.

1.5. Administration des politiques

Une personne de référence a été désignée au sein de l'AE pour :

- Signaler tous les incidents de sécurité à au prestataire technique d'AEAE ;
- Le prestataire Technique d'AE s'engage à notifier l'AC de tout incident de sécurité
- Gérer les changements dans ce document de politique d'enregistrement en cas de changement majeure sur les règles de vérification d'identité ;
- S'assurer que les procédures opérationnelles liées à l'activité d'AE sont réalisées conformément à la présente politique d'enregistrement.

La personne à contacter est :

Ahmed Boussadia,
QUICKSIGN,
19 Rue Poissonnière, 75002 Paris.

1.6. Définitions

Terme	Définition
Agent d'enregistrement	Une personne liée contractuellement ou hiérarchiquement à l'AE, qui est chargée d'identifier et/ou d'authentifier les souscripteurs lors d'une rencontre en face à face ou via la validation des éléments transmis par le souscripteur. L'AE s'assure que cet agent a été formé au respect des règles de pointe en matière de vigilance à l'égard de la clientèle pour les institutions vendant des produits financiers ou des règles équivalentes.
Authentification	Processus par lequel une partie a présenté une identité et prétend être cette identité et la seconde partie confirme que cette affirmation d'identité est vraie.
Autorité de certification	Une autorité à laquelle un ou plusieurs utilisateurs font confiance pour créer et attribuer des certificats. Plus précisément, dans le contexte de ce document, l'AC est responsable de : • L'émission de certificats ; • Garantir la fiabilité du service de signature numérique pour les tiers. L'AC exploite une plateforme de signature d'AC. Dans le cadre de ce document, l'AC est DocuSign FRANCE.
Autorité d'enregistrement	Entité chargée, d'identifier et d'authentifier les sujets des certificats. Optionnellement, l'AE peut transmettre les

	documents signés à un souscripteur et stocker le fichier d'enregistrement des utilisateurs. Dans le cadre de ce document, l'AE est gérée par QUICKSIGN.
Autorité de gestion des politiques	L'entité en charge de la gestion des composants et services de l'IGC. La PMA approuve la politique de certification (PC) et la déclaration des pratiques de certification (DPC) utilisées pour soutenir les services de certification de l'IGC. La PMA se réserve le droit d'auditer l'IGC comme indiqué dans la section 8 de cette PE. Dans le contexte de ce document, le PMA est géré par DocuSign FRANCE.
Certificat	Un certificat est une structure de données qui est signée numériquement par une autorité de certification et qui contient les éléments d'information suivants : • L'identité de l'autorité de certification qui le délivre ; • L'identité du souscripteur ; • Une clé publique qui correspond à une clé privée sous le contrôle exclusif du souscripteur ; • La date limite de validité ; • Un numéro de série ; • Le format du certificat conformément à la recommandation UIT-T X.509 version 3.
Certificat avancé	Un certificat qui répond aux exigences énumérées à l'article 26 du règlement eIDAS.
Client	Une entité utilisant le service de signature de l'AC et la plateforme technique du Prestataire Technique d'AE de QuickSign afin de demander à ses souscripteurs de signer numériquement un document soumis. Dans le contexte de ce document, le Client agit en tant qu'Autorité d'Enregistrement.
Documents d'identité	Les documents d'identité de l'utilisateur peuvent être soit : • Une pièce d'identité officielle (passeport, carte d'identité) ; • Ou tout système d'identification électronique qui a été notifié par un État membre à la Commission européenne conformément à l'article 9 du règlement eIDAS (règlement n°910/2014) ; Ou tout autre document d'identification électronique qui a été délivré après un entretien en face à face au cours duquel un document d'identité officiel a été vérifié.
Fichier de Preuve (QS)	Désigne un fichier généré par QuickSign, scellé au nom de QuickSign et horodaté (avec un horodatage qualifié) par DocuSign France, qui contient toutes les informations relatives aux opérations de signature et d'identification d'un ou plusieurs Signataire(s). Un Fichier de Preuve dédié sera joint à chaque transaction dans le but de prouver la validité de la signature électronique en cas de procédure judiciaire ou d'enquête. Le Fichier de Preuve est uniquement mis à disposition de l'AE. Le

	Fichier de Preuve contient le ou les nom(s) du ou des Document(s) objet de la transaction.
Fonction de hachage	Fonction cryptographique qui transforme une chaîne de caractères de taille quelconque en une chaîne de caractères de taille fixe et généralement inférieure. Cette fonction satisfait entre autres deux propriétés : • la fonction est « à sens unique » : il est difficile pour une image de la fonction donnée de calculer l'antécédent associé ; • la fonction est « sans collision » : il est difficile de trouver deux antécédents différents de la fonction ayant la même image.
Hash	Résultat d'une fonction de hachage
HSM (Hardware Security Module)	Ressource cryptographique matérielle certifié CC EAL 4+ ou FIPS 140-2 level 3 qui est utilisée par l'AC pour générer, utiliser et gérer les clés des Signataires.
LCBFT	Lutte contre le Blanchiment et le Financement du terrorisme
Numéro d'identification de la transaction	Un identifiant unique composé de façon aléatoire de lettres et de chiffres attribués à une seule demande d'identification et qui garantit l'unicité du Certificat.
Prestataire technique d'Autorité d'Enregistrement	Une entité qui est responsable, selon les règles de l'AE et dans le cadre d'un contrat avec l'AE, de la collecte des documents d'identification de l'utilisateur (si applicable), de la vérification de l'identité de l'utilisateur (si applicable), de la collecte des coordonnées pour authentifier l'utilisateur en ligne (si applicable) et de la transmission de la demande de certificat à l'AC.
Protocole de consentement	Désigne l'ensemble des règles de recueil de consentement géré par l'AE et le Prestataire Technique de l'AE pour une opération de signature dans le cadre d'une transaction donnée à savoir (i) la définition des actions à réaliser par le Signataire pour signer le ou les Document(s), (ii) les informations utilisées pour la création de l'identité Signataire, (iii) les modalités de visualisation du Document présenté et du message d'acceptation (ou de refus) associé. Le Protocole de consentement est mise en œuvre par l'AE en s'appuyant sur le Prestataire Technique de l'AE.
Révocation	Un processus par lequel la période opérationnelle d'un certificat est terminée prématurément. La période opérationnelle des certificats demandés par l'AE est définie dans la politique de certification de l'AC. Non applicable dans le contexte de cette PE.
Signataire	La personne physique qui reçoit un certificat de l'autorité de certification et qui utilise une clé privée conservée dans un HSM pour signer numériquement le document envoyé par l'AE. Le Signataire est le Porteur au sens de la Politique de Certification (aussi appelé un signataire).

2. Responsabilités en matière de publication et d'archivage

Ce document est publié par l'AE sur le site web de l’entreprise [https://quicksign.com].

Elle peut également être publiée par l'Autorité de gestion des politiques en tant que modification de la politique de certification selon ses propres règles de publication.

3. Identification et authentification

3.1. Nommer

Le nommage dans les certificats demandés par l'AE est conforme à la recommandation UIT-T X.509 ou à la RFC 5280 de l'IETF et à la politique de certification de l'AC (section 10).

3.2. Validation initiale de l'identité

3.2.1. Méthode pour prouver la possession d'une clé privée

La preuve de la propriété de la clé privée correspondant au certificat du souscripteur utilisé à des fins de signature est fournie par les ressources techniques et organisationnelles de la plate-forme de signature de l'AC.

3.2.2. Authentification de l'identité de l'organisation

Cette partie n'est pas applicable. L'AE accepte uniquement les demandes de personnes physiques demandant des certificats électroniques qualifiés en leur propre nom et non pour des tiers, le sujet étant équivalent au souscripteur. Par conséquent, le service d'enregistrement de l'AE ne comprend aucun processus permettant de vérifier l'association d'une personne avec une organisation ou une personne morale.

3.2.3. Authentification de l'identité de la personne physique

L'AE vérifie au moment de l'enregistrement initial, par des moyens appropriés et conformément à la législation nationale, l'identité et, le cas échéant, les attributs spécifiques de la personne à laquelle un certificat est délivré.

La preuve de l'identité d'une personne physique est vérifiée soit :

- Par la présence en face à face ou de la personne physique et la présentation d'une pièce d'identité valide ;
- À distance, par la collecte sécurisée d'une copie d'un document d'identité, d'un contrôle biométrique sur le détenteur de la carte et via une validation de ce document par des contrôles antifraudes conformes au référentiel PRADO ;
- A distance, selon une méthode de vérification d'identité validée par une autorité locale en terme d'entrée en relation[1] en accord avec la réglementation en vigueur découlant de la directive UE 2018/843 LCBFT[2].

[1] Par exemple, le régulateur en France est l'ACPR : https://acpr.banque-france.fr/
[2] En France, la transposition en droit national de la directive LCBFT

Les informations d'identité et de contacts suivantes sont enregistrées par l'AE :

- Nom du souscripteur (comprenant le nom de famille et au moins un prénom conforme aux pratiques nationales d'identification) ;
- Email ;
- Numéro de téléphone ;
- Si applicable : La date et le lieu de naissance, la référence à un document d'identité reconnu au niveau national, ou d'autres attributs qui peuvent être utilisés pour, dans la mesure du possible, distinguer la personne des autres personnes portant le même nom.

La preuve étant fournie d'un document d'identité reconnu au niveau national, l'AE vérifie que ce document est toujours valide et authentique. Ce contrôle peut être fait de façon automatique.

L'AE collecte la référence de la pièce d'identité, ou, en option, télécharge une copie de la pièce d'identité. L'AE collecte également le numéro de téléphone du souscripteur ainsi que son adresse électronique. Le DRA met à jour les informations d'enregistrement si elles ont changé.

Le cas échéant, l'AE fournit au souscripteur un moyen d'authentification sécurisé géré par l'AE selon les règles de sécurité bancaire, associé de manière sécurisée au souscripteur et considéré comme contrôlé par le souscripteur.

L'AE enregistre les informations d'enregistrement (fichier de preuve) pendant un temps conforme à la réglementation bancaire en matière d'entrée en relation et au moins 5 ans.

3.2.4. Validation de l'autorité

Cette partie n'est pas applicable. L'AE accepte uniquement les commandes de personnes demandant des certificats électroniques soumis en leur propre nom et non pour des tiers. Par conséquent, le service d'enregistrement de l'AE ne comprend aucun processus permettant de vérifier l'association d'une personne avec une organisation ou une personne morale.

3.2.5. Informations non vérifiées sur le souscripteur

Comme décrit ci-dessus, tous les détails personnels et les informations à stocker dans le certificat sont vérifiés par l'AE (nom prénom). Aucune information non vérifiée n'est utilisée par l'AE pour remplir un certificat.

3.2.6. Critères d'interopérabilité

Les certificats délivrés par les composants PKI sont gérés selon les règles et les exigences énoncées par l'AC et le client, conformément aux exigences d'Adobe.

3.3. Identification et authentification pour les demandes de renouvellement

Non applicable car les certificats ont une durée de vie de 5 minutes plus 1 heure.

Un nouveau Certificat ne peut pas être fourni au Signataire sans renouvellement de la bi-clé correspondante. La procédure pour un nouveau Certificat est soit égale à la procédure initiale (Cf. § 3.2) soit de niveau équivalent. Le Client peut par exemple authentifier une première fois le Signataire et lui remettre des moyens de connexion à son portail Client qui permette d'être assuré que c'est bien le Signataire qui se connecte. En ce cas, il faudra s'assurer régulièrement, que l'Identité du Signataire (nom et prénom, au moins tous les 10 ans pour l'identité) et que les moyens utilisés pour le Protocole de Consentement sont toujours valides (email et numéros de téléphones).

3.4. Identification et authentification pour la demande de révocation

Non applicable car les certificats ont une durée de vie de 5 minutes plus 1 heure.

4. Exigences opérationnelles du cycle de vie des certificats

4.1. Demande de certificat

L'AE demande un certificat à la suite de la collecte des informations du Signataire (Cf. § 3.2). Cette demande de certificat est envoyée de manière sécurisée au Prestataire Technique d'AE avec au moins les informations suivantes :

- Au moins un prénom(s) ;
- Au moins un nom de famille ;
- Adresse électronique actuelle ;
- Numéro de téléphone mobile ;
- Si applicable une copie de la pièce d'identité officielle avec les informations suivantes lisibles : Type de pièce d'identité, numéro de pièce d'identité, date d'expiration ou de délivrance de la pièce d'identité, pays de délivrance, date de naissance.
- Le document à signer.

4.2. Traitement des demandes de certificat

L'AE vérifie les informations collectées au § 3.2 suivant ses propres règles. L'AE peut définir des règles de validation de demande de certificat automatique qui permettent de générer des certificats avancés sans une validation humaine. Ces règles doivent faire l'objet de contrôle par l'AE. La validation de l'identité du Signataire est réalisée par l'AE avant ou après la demande de Certificat et donc le processus de signature. Dans tous les cas, les informations de contact et d'identité du Signataire doivent être récupéré par l'AE avant de transmettre la demande de Certificat.

Ces contrôles sont documentés dans des documents internes de l'AE, ils sont effectués par des moyens techniques propres à l'AE ou via son prestataire technique.

4.3. Délivrance du certificat

Afin de procéder à la génération du Certificat, l'authentification du souscripteur est réalisée via un code OTP envoyé par SMS. Les Documents à signer, les informations du Signataire et son consentement à signer est réalisée dans le cadre du Protocole de Consentement mise en œuvre par l'AE à l'aide de la plateforme du Prestataire Technique d'AE, une fois le processus d'inscription terminé, et le Signataire ayant accepté les termes et conditions du service, le prestataire d'AE appelle la plateforme de signature de l'AC pour soumettre une demande de Certificat, en transmettant les informations suivantes du souscripteur :

- Au moins un prénom(s) ;
- Au moins un nom de famille ;

- Le hash du ou des Documents à signer.

Ces informations sont échangées de manière sécurisée.

4.3.1. Processus de délivrance du certificat

L'AC authentifie le prestataire d'AE.

L'AC (a) génère un Certificat, (b) signe le ou les hash des Documents à signer, avec la clé privée du Signataire, (c) supprime ensuite la clé privée du Signataire, (d) horodate, et (e) le cas échéant appose un cachet électronique selon le choix du Prestataire Technique de l'AE.

L'AC met le certificat ainsi que le résultat de la signature à disposition du prestataire d'AE.

Le prestataire d'AE récupère le certificat généré par l'AC ainsi que les hash signé et génére un document au format PDF conforme à la norme PDF/A.

A la fin du processus le prestataire d'AE génère un fichier de preuve contenant les traces des événements et le scelle., le prestataire technique d'AE appelle la plateforme de signature de l'AC pour sceller et horodater le Fichier de Preuve en transmettant au moins les informations de demande de certificat (réf § 4.1. Demande de certificat).

Le prestataire d'AE met à disposition le Fichier de Preuve à l'AE.

L'AE doit dans tous les cas récupérer le Fichier de Preuve pour tous les Signataires et le conserver (Cf. § 5.5).

4.4. Acceptation du certificat

Avant d'entrer dans une relation contractuelle avec un Souscripteur, l'AE collecte le consentement du souscripteur dans le cadre du Protocole de Consentement.

Le nom et le prénom du souscripteur sont mentionnés sur la page du Protocole de Consentement comme informations à valider par le souscripteur pour figurer dans le Certificat. Le Souscripteur donne son consentement en cochant au moins une case.

Si l'identité du Souscripteur était considérée comme valide pour la demande de certificat selon les règles de l'AE, l'AE met le document signé avec le certificat intégré à la disposition du Souscripteur.

Dans le cas contraire, l'AE ne remet pas le document signé avec le certificat intégré au souscripteur et le détruit.

4.5. Utilisation de la paire de clés et du certificat

Les souscripteurs utilisent leurs clés privées dans le but énoncé à la section 1.4. ci-dessus.

4.6. Renouvellement de certificat

Cette partie n'est pas applicable, conformément à la politique de certification de l'AC.

4.7. Re-key du certificat

La re-key du certificat est effectuée selon les procédures décrites aux paragraphes §4.1. à §4.4. Pour l'authentification du souscripteur, le paragraphe 3.3. s'applique.

4.8. Modification du certificat

Cette partie n'est pas applicable, conformément à la politique de certification de l'AC.

4.9. Révocation et suspension des certificats

Cette partie n'est pas applicable, conformément à la politique de certification de l'AC.

5. Contrôles des installations, de la gestion et des opérations

5.1. Contrôles physiques

L'accès physique aux locaux hébergeant le système d'information et les personnes mettant en œuvres les services de l'AE et du Prestataire Technique de l'AE est réservé aux seules personnes autorisées. Les personnes non autorisées doivent toujours être accompagnées par du personnel autorisé et leur accès aux bureaux doit être enregistré. L'accès aux principaux centres de données est limité aux seules personnes autorisées.

Des contrôles sont mis en œuvre pour éviter la perte, l'endommagement ou la compromission des actifs et l'interruption des activités commerciales ; pour éviter la compromission ou le vol d'informations et d'installations de traitement de l'information ; et pour empêcher que les actifs de l'AE et du Prestataire Technique de l'AE soient pris sans autorisation. Ces contrôles sont décrits dans le processus d'évaluation et de gestion des risques ainsi que dans le plan de continuité des activités.

Un périmètre de sécurité est défini pour protéger les composants critiques contre les intrusions ; l'accès à ce périmètre de sécurité est contrôlé, notamment par des alarmes afin de détecter les intrusions.

5.2. Contrôles de procédure

Tous les rôles de confiance au sein de l'AE et du Prestataire Technique de l'AE sont bien identifiés de manière à ce que la séparation des tâches soit mise en œuvre. Chaque rôle est décrit et documenté et chaque personne affectée à un rôle est identifiée nominativement.

L'AE et du Prestataire Technique de l'AE administre l'accès de chaque rôle. L'administration comprend la gestion des comptes utilisateurs et la modification ou la suppression de l'accès en temps opportun. L'accès aux informations et aux fonctions des systèmes d'application est limité conformément à la politique de contrôle d'accès. Le personnel est identifié et authentifié avant d'utiliser les applications critiques du service d'enregistrement, et doit rendre compte de ses activités par le biais du journal des événements ou du journal classique.

5.3. Contrôles du personnel

Le personnel de l'AE et du Prestataire Technique de l'AE chargé du fonctionnement de l'infrastructure ou de la mise en œuvre de la présente PE est qualifié et formé.

Le personnel de l'AE et du Prestataire Technique de l'AE qui ne respecte pas les règles et les procédures établies s'expose à des sanctions disciplinaires conformément au droit du travail français.

Les rôles et responsabilités en matière de sécurité sont documentés dans les descriptions de poste et sont mis à la disposition de tout le personnel concerné. Le personnel est conscient de la séparation des tâches et du moindre privilège, en fonction de la sensibilité du poste.

Le personnel applique des procédures et des processus d'administration et de gestion qui sont conformes aux procédures de gestion de la sécurité de l'information de l'AE et du Prestataire Technique de l'AE.

Le personnel d'encadrement possède une expérience ou une formation en matière de signature électronique et de sécurité des informations.

Le personnel qui prend les décisions relatives au processus d'entrée en relation est libre de tout conflit d'intérêts et dispose d'un plein pouvoir de décision, sauf en cas de crise.

Le personnel est officiellement nommé à des rôles de confiance par l'AE et du Prestataire Technique de l'AE selon le principe du "moindre privilège". Le personnel n'a accès aux rôles de confiance qu'après avoir prouvé sa qualification pour les rôles décrits. Le personnel de l'AE et du Prestataire Technique de l'AE prouve sa fiabilité en présentant son casier judiciaire ainsi que de bonnes références d'anciens employeurs.

5.4. Procédures de journalisation des audits

Des fichiers journaux d'audit sont générés pour tous les événements liés à la sécurité et aux services d'AE et du Prestataire Technique de l'AE. Dans la mesure du possible, les journaux d'audit de sécurité sont collectés automatiquement. Lorsque cela n'est pas possible, un journal de bord ou un autre mécanisme physique est utilisé. Tous les journaux de sécurité, qu'ils soient électroniques ou non, sont conservés et mis à disposition lors des audits de conformité.

La confidentialité des informations sur les sujets est préservée.

Les journaux d'audit sont protégés de manière à ce que seuls les utilisateurs autorisés puissent y accéder et/ou les utiliser. Les journaux d'audit sont enregistrés de manière à ce qu'ils ne puissent pas être facilement supprimés ou détruits (sauf pour être transférés sur un support à long terme) pendant la période où ils doivent être conservés. Les journaux d'audit sont protégés de manière à rester lisibles pendant toute la durée de leur période de conservation. Les journaux d'audit et les résumés d'audit sont sauvegardés via des mécanismes de sauvegarde d'entreprise.

Une analyse de vulnérabilité sur les adresses IP privées et publiques est effectuée sur une base mensuelle.

Les journaux d'audit fournissant des informations sur les activités malveillantes potentielles sont examinés régulièrement par l'administrateur système. Si un système de sécurité alerte

l'administrateur système sur un problème de sécurité potentiel, les journaux sont examinés immédiatement.

5.4.1. Autorité d'enregistrement

La journalisation comprend au moins les sujets suivants :

- Accès aux installations physiques ;
- Gestion des rôles de confiance ;
- Accès logique ;
- Gestion des sauvegardes ;
- Gestion des journaux ;
- Collecte du fichier de preuve ;
- Gestion des données d'enregistrement ;
- Gestion de l'informatique et des réseaux ;
- Identification et l'authentification du souscripteur ;
- Les circonstances de l'identification et de l'authentification du souscripteur ;
- Gestion des moyens d'authentification du souscripteur ;
- Gestion des rôles de confiance ;

5.5. Archivage des documents

5.5.1. Autorité d'enregistrement

L'AE enregistre au moins :

- La méthode utilisée pour valider l'identité du Souscripteur ;
- Les documents servant à vérifier l'identité du Signataire ;
- Les informations d'identité et de contact du Signataire ;
- Le consentement du Souscripteur.

Le dossier et le Fichier de Preuve est archivé, que le Signataire veuille ou non des produits issus des Documents signés et que l'identité du Signataire soit valide ou non, pendant une période conforme à la réglementation bancaire et ce pendant au moins 5 ans pour être conforme à la PC.

La confidentialité et l'intégrité des dossiers actuels et archivés concernant les certificats sont maintenues. Les enregistrements sont archivés de manière complète et confidentielle conformément aux pratiques commerciales divulguées ; ils sont mis à disposition si cela est nécessaire pour fournir une preuve de la certification aux fins d'une procédure judiciaire. En particulier, le système d'archivage et les méthodes appliquées garantissent que :

- Tous les supports utilisés pour l'archivage des documents d'AE sont protégés contre les dommages et stockés uniquement dans des zones à accès restreint. Le support est chiffré et nécessite un contrôle d'accès spécial pour être lu ;

- Les supports sont surveillés par le système d'archivage afin d'identifier ceux qui risquent d'être obsolètes ou de se détériorer. Les supports identifiés doivent être échangés par l'administrateur du système en veillant à ce que les données ne soient pas perdues ou récupérées sur le miroir du système d'archivage ;
- Tous les supports utilisés pour stocker des données personnelles sont supprimés et détruits à la fin de leur durée de vie ;
- Tous les supports utilisés dans le système d'archivage ne peuvent pas être utilisés ou réutilisés dans un autre contexte en raison du système de fichiers chiffré utilisé, qui est différent de ceux utilisés pour stocker les données opérationnelles.

5.6. Changement de clé

La validité du certificat du souscripteur est définie dans la politique de certificat de l'AC.

5.7. Compromission et reprise après sinistre

QUICKSIGN dispose d'un plan de continuité des activités. Il identifie les risques et décrit les actions et mesures pour faire face aux incidents et autres événements compromettants.

5.8. Terminaison

5.8.1. Autorité d'enregistrement

Si QUICKSIGN prévoit de mettre fin à son rôle et du Prestataire Technique de l'AE pour l'AC, elle devra appliquer la clause de réversibilité définie dans le contrat entre l'AC et le prestataire d'AE.

Si l'AE prévoit de mettre fin à son rôle d'AE, alors l'AE conserve ses Fichier de Preuve conformément aux règles de la présente PE et les rend disponible sur demande de l'AC pendant 5 ans, pour des raisons d'audit et d'enquête issues d'une autorité administrative française, à compter de la fin de contrat.

6. Contrôles de sécurité techniques

6.1. Génération et installation de paires de clés

L'AC gère les clés des Signataires conformément à la PC de l'AC.

6.2. Protection des clés privées et ingénierie des modules cryptographiques

Le Signataire active sa clé privé de signature grâce à un code OTP reçu sur son téléphone portable qui doit être saisit dans l'interface du Protocole de Consentement.

6.3. Autres aspects de la gestion des paires de clés

Les autres aspects de la gestion de la paire de clés sont exécutés par l'AC conformément à la PC de l'AC.

6.4. Données d'activation

Le protocole de consentement, y compris la génération, l'installation et la protection des données d'activation, est mis en œuvre par l'AE selon les procédures du Prestataire Technique d'AE.

Le code OTP est généré par le Prestataire dAE et remis par le Prestataire d'AE au Signataire. Un code différent est nécessaire pour chaque transaction.

6.5. Contrôles de sécurité informatique

Des contrôles (par exemple, des pare-feu) protègent les domaines de réseau internes de l'AE et du Prestataire Technique de l'AE contre tout accès non autorisé. Les pares-feux sont également configurés par l'AE et le Prestataire Technique de l'AE pour empêcher tous les protocoles et accès non requis par les opérations pertinentes. L'AE et le Prestataire Technique de l'AE s'assure que l'accès au système est limité aux personnes dûment autorisées.

Les données sensibles sont protégées contre la divulgation par des objets de stockage réutilisés accessibles à des utilisateurs non autorisés.

6.6. Contrôle de la sécurité pendant le cycle de vie

L'AE et le Prestataire Technique de l'AE utilise des systèmes et des produits dignes de confiance, protégés contre toute modification et garantissant la sécurité technique et la fiabilité des processus qu'ils soutiennent.

Une analyse des exigences de sécurité est effectuée au stade de la conception et de la spécification des exigences de tout projet entrepris par l'AE et le Prestataire Technique de l'AE.

Les procédures de contrôle des changements s'appliquent aux versions, aux modifications et aux corrections logicielles d'urgence pour tout logiciel opérationnel et aux changements de la configuration. Ces procédures comprennent la documentation des changements.

L'intégrité des systèmes et des informations de l'AE et du Prestataire Technique de l'AE est protégée contre les virus, les logiciels malveillants et non autorisés. Les dommages causés par les incidents et les dysfonctionnements de sécurité sont minimisés par l'utilisation de procédures de rapport et de réponse aux incidents. Les supports utilisés au sein de l'AE et du Prestataire Technique de l'AE sont manipulés de manière sécurisée afin de les protéger contre les dommages, le vol et l'accès non autorisé. Les procédures de gestion des supports protègent contre l'obsolescence et la détérioration des supports pendant la période de conservation des documents. Des procédures sont établies et mises en œuvre pour tous les rôles de confiance et administratifs qui ont un impact sur la fourniture des services de certification.

Des procédures sont spécifiées et appliquées pour garantir que les correctifs de sécurité sont appliqués dans un délai raisonnable après leur mise à disposition, que les correctifs de sécurité ne sont pas appliqués s'ils introduisent des instabilités qui l'emportent sur les avantages de leur application, et que les raisons de ne pas appliquer de correctifs de sécurité sont documentées et choisies par l'AE et le Prestataire Technique de l'AE.

6.7. Contrôles de sécurité des réseaux

L'AE et le Prestataire Technique de l'AE maintient et protège ses systèmes dans au moins une zone sécurisée et met en œuvre et configure une procédure de sécurité qui protège les systèmes et les communications entre les couches du système à l'intérieur des zones sécurisées.

6.8. Horodatage

Des procédures automatiques (synchronisation NTP par exemple) ou manuelles sont utilisées pour maintenir l'heure du système. Pour sécuriser l'heure sur les enregistrements d'audit, l'AE et le Prestataire Technique de l'AE se synchronise régulièrement avec un service de temps.

7. Profil de Certificat, CRL et OCSP.

Cf. PC de l’AC.

8. Audit de conformité et autres évaluations

8.1. Fréquence ou circonstances de l'évaluation

Le service d'enregistrement est audité de façon régulière par les autorités bancaires applicable à l'AE.

En cas d'incident de sécurité critique ou de la demande d'un régulateur et conformément à la PC de l'AC, l'AE et le Prestataire Technique de l'AE peuvent être audité par DocuSign France afin de vérifier le respect de la présente PE et de la PC.

8.2. Sujets couverts par l'évaluation

L'AC peut effectuer des contrôles de l'activité d'enregistrement en cas de suspicion de fraude détectée par l'AC ou dans le cadre d'un audit de l'AE et du Prestataire Technique de l'AE comme défini dans la PC de l'AC. Cet audit aura pour seul but de vérifier que les règles de la présente PE et des contrats qui l'instancient sont bien maîtrisés et implémentés correctement.

9. Autres affaires et questions juridiques

9.1. Droits d'inscription

Ces services sont définis dans le contrat établi entre l'AE et le prestataire technique d'AE.

9.2. Responsabilité financière

L'AE maintient des niveaux raisonnables de couverture d'assurance et des ressources financières suffisantes pour maintenir les opérations. La couverture d'assurance ou de garantie est définie dans le contrat entre l'AE et le prestataire technique d'AE.

9.3. Confidentialité des informations commerciales

L'AE maintient la confidentialité des informations commerciales confidentielles, y compris les données d'identité personnelle, la demande de certificat du souscripteur, les résultats et les rapports d'audit, le plan de continuité des activités et le contrat avec le prestataire d'AE.

9.4. Confidentialité des informations personnelles

L'AE et le Prestataire Technique de l'AE protège la confidentialité et l'intégrité des données d'enregistrement, conformément à la législation européenne applicable en matière de confidentialité des données. L'ensemble des règles de confidentialité des données de l'AE et du Prestataire Technique de l'AE est documenté dans leur PSSI. Ces règles sont présentées à chaque souscripteur avant toute transaction dans les conditions générales du service, qui doivent être acceptées par le souscripteur en cliquant sur une case à cocher.

QUICKSIGN en tant que Prestataire Technique de l'AE et l'AE respecte la loi informatique et liberté et le RGPD. QuickSign désigne un délégué à la protection des données. Ses coordonnées sont les suivantes :

dpo@quicksign.comQUICKSIGN

19 Rue Poissonnière, 75002 Paris

9.5. Droits de propriété intellectuelle

Cette partie n'est pas applicable. La PMA conserve la propriété intellectuelle des certificats d'AC qu'il publie.

9.6. Déclarations et garanties

L'AE alerte le Prestataire Technique d'AE en cas d'incident de sécurité.

Le Prestataire Technique de l'AE alerte l'AC en cas d'incident de sécurité.

L'AE collecte le consentement du Souscripteur. Le Souscripteur accepte les conditions générales du service en cliquant sur une case à cocher sur l'écran.

L'AE protège son système d'information et garantit la sécurité des données transmises au prestataire technique d'AE.

L'AE établit une relation contractuelle avec le Prestataire Technique d'AE, engageant ce dernier à remplir ses obligations conformément à la présente politique d'enregistrement.

L'AE respecte ses obligations en vertu de la présente politique d'enregistrement.

L'AE s'assure que chaque Souscripteur pour lequel une demande de certificat est soumise à l'AC via le prestataire d'AE a été identifié et authentifié conformément à ses procédures et que la demande de certificat a été exacte et dûment autorisée.

L'AE s'assure que son organisation possède l'expertise, la fiabilité, l'expérience et les qualifications nécessaires et a reçu une formation adéquate concernant les règles de sécurité et de protection des données personnelles pour l'identification et l'authentification conformément aux règles de diligence raisonnable pour les institutions vendant des produits financiers ou des règles équivalentes.

L'AE protège son système d'information et garantit la sécurité des données collectées.

L'AE protège la confidentialité et l'intégrité des données d'enregistrement.

L'AE conserve tous les Fichiers de Preuve de tous les Signataires pendant 5 ans minimum.

L'AE garantit la conformité des règles de validation du processus d'entrée en relation avec un Signataire au regard de son régulateur bancaire et de la présente PE.

9.7. Exclusion des garanties

Non applicable.

9.8. Limitations de la responsabilité

L'AE n'assume aucune responsabilité en relation avec l'utilisation du certificat pour tout autre usage que celui décrit dans le présent document.

L'AE est responsable de l'exactitude de toutes les informations d'enregistrement, sous réserve des termes du contrat entre l'AE et le prestataire technique d'AE. L'AE n'est pas responsable des retards, de la non-livraison, du non-paiement, de la mauvaise livraison ou de l'interruption de service causés par un tiers, y compris le prestataire technique d'AE.

9.9. Indemnités

Les indemnités en cas de responsabilité de l'AE sont définies dans les conditions générales d'utilisation du service de l'AE que le Signataire accepte avant de pouvoir signer conformément à la présente PE.

9.10. Durée et résiliation

La PE et ses versions ultérieures entrent en vigueur dès leur approbation par l'AE.

Dans le cas où l'AE cesse de fonctionner, l'AE doit suivre la procédure décrite au paragraphe 5.8. du présent document.

9.11. Avis individuels et communications avec les participants

QUICKSIGN fournit une nouvelle version de cette politique d'enregistrement via son site web.

9.12. Amendements

QUICKSIGN révise ce document au moins une fois par an. Des révisions supplémentaires peuvent être effectuées à tout moment à la discrétion de QUICKSIGN.

9.13. Dispositions relatives au règlement des différends

Les dispositions relatives au règlement des différends entre l'AE et le Prestataire Technique d'AE sont énoncées dans le contrat applicable entre les parties.

9.14. Loi applicable

Sous réserve de toute limitation de la loi applicable, les lois de la FRANCE régissent l'exécution, la construction et la validité de la présente police, indépendamment des dispositions contractuelles ou de tout autre choix de loi et sans qu'il soit nécessaire d'établir un lien commercial en FRANCE.

La présente disposition relative au droit applicable s'applique uniquement à la politique d'enregistrement. Les contrats avec un client faisant référence à la présente politique peuvent avoir leurs propres dispositions en matière de droit applicable, à condition que la présente section régisse l'applicabilité, l'interprétation et la validité de la présente politique indépendamment des conditions de ces autres accords.

9.15. Conformité avec la loi applicable

Cette politique d'enregistrement est soumise aux lois, règles, règlements, ordonnances, décrets et arrêtés français et européens applicables. L'AE et le prestataire d'AE s'engagent à respecter les lois et règlements applicables dans leurs contrats.

9.16. Dispositions diverses

La présente PE constitue l'intégralité de l'accord entre les parties et remplace tous les autres termes, qu'ils soient exprimés ou implicites par la loi. Aucune modification de la présente PE n'a de force ou d'effet, sauf si elle est faite par écrit et signée par un signataire autorisé. Le fait de ne pas appliquer l'une ou l'ensemble de ces sections dans un cas particulier ne constitue pas une renonciation et n'empêche pas une application ultérieure. Toutes les dispositions de la présente PE qui, par nature, s'étendent au-delà de la durée d'exécution des services (par exemple, les informations confidentielles et les droits de propriété intellectuelle) sont applicables au successeur de l'une des parties.

Si une section de cette PE est incorrecte ou invalide, les autres sections de cette PE restent en vigueur jusqu'à ce que la PE soit mise à jour.