POLITIQUE D'ENREGISTREMENT

Modification de la Politique de Certificats de DOCUSIGN FRANCE pour l'utilisation de la plateforme QUICKSIGN en tant que service d'inscription pour identifier les Abonnés

Version	2.11	
Statut	□ Projet	□ Finale
Auteur	Compagnie Margo	QUICKSIGN

Diffusion Liste	□ Interne	□ Externe
		Public

Histoire				
Version	Date	Auteur	Commentaires	Statut
V.1.0	27/09/2016	MC		Vérifié par XR Publié
V.1.99	28/08/2017	FV	Mise à jour pour préparer la période transitoire postérieure à l'article 51 Version préliminaire	En attente de DocuSign et de l'audit Approbation
V2.04	12/09/2019	XR	Examen avec CA et approbation de la PMA (12septembre 2019)	Approbation
V2.05	02/12/2019	XR	Examen avec l'autorité de certification de l'authentification du Demande de révocation.	Approbation
V2.10	16/02/2021	DE	Ajout d'un nouveau flux de travail avec une signature manuelle validée par un agent d'enregistrement	Modification
V2.10	23/02/2021	DE	Révision et validation avec COMME	Approbation
V2.11	06/07/2021	DE	Examen et mise à jour mineure de document	Modification et Approbation

TABLE DES MATIÈRES

Table des matières

1. Introduction

1.1. Aperçu

La présente politique d'inscription (RP) est un avenant au document « DBD_Protect et signer la signature personnelle ETSI CP » de DOCUSIGN FRANCE. Il explique comment le service d'enregistrement en ligne [QUICKSIGN Q ES ONBOARD ID] exploité par QUICKSIGN répond aux exigences définies pour les autorités d'enregistrement (RA) délivrant des certificats qualifiés avec ETSI EN 319 411-2 QCP-n-qscd.

Dans ce contexte, QUICKSIGN agit en tant qu'autorité d'enregistrement (RA) et utilisela plate-forme de QUICK SIGN comme service d'enregistrement pour identifier les abonnés demandant des signatures personnelles sur la base de certificats émis par une autorité de certification (CA).

Ce PR est basé sur :

- [CP]: DBD_Protect_and_Sign_Personal_Signature_ETSI_CP_v_1_8.
- [PSMP]: « Politique de Signature et de Gestion des Preuves, version 6 minimum qui définit le processus technique de signature électronique et d'interaction avec le Client.
- RFC 3647 « Certificate Policy and Certification Practices Framework » publié par l'Internet Engineering Task Force (IETF).
- Documents de l'ETSI :
    - [119 312]: « ETSI TS 119 312 V1.1.1 (2014-11): Signatures et infrastructures électroniques (ESI); Suites cryptographiques. »;
    - [319 401]: « ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers. »;
    - [319 411]:
        - « ETSI EN 319 411-1 V1.2.2 (2018-04) »: « Signatures électroniques et infrastructures (ESI), Politique et exigences de sécurité pour les prestataires de services de confiance émettant des certificats, Partie 1 : Exigences générales »;
        - « ETSI EN 319 411-2 V2.2.2 (2018-04) » : « Signatures et infrastructures électroniques (ESI) ; les exigences en matière de politique et de sécurité pour les fournisseurs de services de confiance qui émettent des certificats; Partie 2: Exigences applicables aux prestataires de services de confiance délivrant des certificats qualifiés de l'UE ».

- [TROUVER 319 411] :
    - « Signatures électroniques et infrastructures (ESI), Politique et exigences de sécurité pour les prestataires de services de confiance émettant des certificats, Partie 1 : Exigences générales »
    - « Signatures et infrastructures électroniques (ESI) ; les exigences en

matière de politique et de sécuritépour les fournisseurs de services de confiance qui émettent des certificats; Partie 2: Exigences applicables aux prestataires de services de confiance délivrant des certificats qualifiés de l’UE ».

La numérotation du document est conforme à la DBD_Protect et signer la signature personnelle ETSI CP.

1.2. Nom et identification du document

Dans le cadre de ce document, le DOCUSIGN FRANCE CP OID à considérer est :

- OID = 1.3.6.1.4.1.22234.2.14.3.31 : Ce profil est implémenté par la nouvelle autorité de certification DocuSign France et est qualifié eIDAS avec le nouveau profil de certificat.

Notez que le CP pour ces deux OID est identique, la prise en compte de ces informations La migration de l'OID de l'autorité de certification n'aura pas d'impact sur la stratégie d'enregistrement Quicksign.

1.3. Composants PKI

1.3.1. Autorité d'enregistrement (AR)

L'AR est détenu et exploité par QUICKSIGN.

L'AR prend en charge les services PKI suivants pour tous les cas :

- Authentification de l'Abonné via un challenge à l'aide de la Carte d'Identité ;
- Authentification et autorisation de l'autorité d'enregistrement des délégués (DRA);
- Établissement d'une relation contractuelle avec la DRA engageant la DRA à remplir ses obligations en vertu de la présente politique d'enregistrement ;
- Formation du DRA;
- Célaboration avec l'AC des activités de contrôle et d'audit dirigées vers le DRA;
- Envoi de la demande de certificat à l'autorité de certification;
- Processus d'authentification et de révocation de révocation, et en particulier l'envoi de la demande de révocation de certificat à l'autorité de certification ;
- Génération de traces de journal et enregistrement des informations d'enregistrement ;

Lors de l'exécution de l'AR exécute le protocole de consentement (cas d'utilisation noté protocole de *consentement QS* dans le document pour identifier les exigences spécifiques à cette utilisation peutse), une collecte de la signature manuscrite d'un abonné dans un processus de signature en face à face à l'aide de la tablette d'un DRA est effectuée.

1.3.2. Autorité d'enregistrement déléguée (DRA)

La DRA agit sous la supervision et les règles établies par QUICKSIGN en tant que RA.

QUICKSIGN n’entre en relation contractuelle qu’avec des DRA qui, en raison de la nature des services qu’ils fournissent, sont contraints de s’assurer que son organisation a été

formés pour respecter les exigences légales les plus récentes en matière de vérification d'identité et de rencontre en face à face, conformément aux règles de diligence raisonnable applicables aux établissements vendant des produits financiers ou à des règles équivalentes.

La DRA est auditée par l'AR ou l'Autorité de gestion des politiques(PMA) avant d'entrer en relation contractuelle avec l'AR.

Une liste des ARD, y compris la référence du contrat, le plan de vérification et les personnes de référence autorisées à traiter les demandes de révocation pour chaque ARD, est établie par l'AR.

La DRA prend en charge les services PKI suivants :

- Identification initiale et authentification de l'Abonné ;
- Le cas échéant, mise à jour de la pièce d'identité officielle et des données d'inscription (email, numéro de téléphone...) après avoir dûment vérifié que le lien entre les données d'inscription mises à jour et l'Abonné reste exact ;
- Le cas échéant, authentification de l'Abonné avec un moyen d'authentification sécurisé avec un accès à distance via un portail DRA ;
- Envoi d'une demande de certificat à l'AR;
- Envoi d'une demande de révocation de certificat à l'AR;
- Génération de traces de journal et enregistrement des informations d'enregistrement .

Toutes lesinformations échangées entre l'AR et la DRA sont échangées en toute sécurité, selon les procédures définies par l'AR dans ses spécifications techniques.

Les obligations de la DRA sont définies dans le contrat entre l'AR et la DRA.

1.4. Utilisation des certificats

La seule utilisation du certificat couverte par ce RP est de vérifier la signature électronique appliquée sur les documents à l'aide du 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 affectée au sein de l'AR pour :

- signaler tous les incidents de sécurité à l'autorité de certification;
- gérer les modifications apportées au présent document de politique d'enregistrement lors de la validation de la PMA;
- veiller à ce que les procédures opérationnelles liées à l'activité d'AR soient exécutées conformément à la présente politique d'enregistrement.

La personne à contacter est :

M Ahmed Boussadia
QUICKSIGN
19-21 rue Poissonnière
75002 PARIS

1.6. Définitions

Terme	Définition
Authentification	Processus par lequel une partie a présenté une identité et prétend être cette identité et la deuxième partie confirme que cette affirmation d'identité est vraie.
Certificat	Un certificat est une structure de données signée numériquement par une autorité de certification et qui contient les informations suivantes : • l'identité de l'autorité de certification qui l'a délivrée ; • l'identité de l'Abonné certifié ; • une clé publique qui correspond à une clé privée sous le contrôle de l'Abonné certifié ; • la période opérationnelle ; • un numéro de série ; • le format du certificat conformément à la Recommandation UIT-T X.509 version 3.
Autorité de certification	Autorité approuvée par un ou plusieurs utilisateurs pour créer et attribuer des certificats. Plus précisément, dans le contexte du présent document, l'AC est responsable de : • la délivrance de certificats; • définir les règles régissant l'identification des utilisateurs et veiller à leur respect; • assurer la fiabilité du service de signature numérique pour les tiers. L'autorité de certification exploite une plateforme de signature d'autorité de certification. Dans le cadre de ce document, l'autorité de certification est DOCUSIGN FRANCE.
Client	Une entité utilisant le service de signature de l'autorité de certification afin de demander à ses abonnés de signer numériquement un document soumis. Dans le cadre de ce document, le Client agit en tant qu'Autorité d'Enregistrement Déléguée.

Pouvoir d'enregistrement délégué	Une entité chargée, en vertu des règles de l'AR et dans le cadre d'un contrat avec l'AR, de collecter les documents d'identification de l'utilisateur, de vérifier l'identité de l'utilisateur, de collecter les coordonnées pour authentifier l'utilisateur en ligne, d'authentifier les utilisateurs en ligne pour qu'ils mettent à jour leurs documents d'identification ou

	coordonnées, et demander la révocation du certificat si nécessaire.
Documents d'identité	Les documents d'identité de l'utilisateur peuvent être soit : • une pièce d'identité officielle (passeport, carte d'identité) ; • ou tout schéma d'identification électronique 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 délivré à l'issue d'une réunion en face à face au cours de laquelle une pièce d'identité officielle a été vérifiée.
MARS	Zone de lecture automatique: une zone incluse dans un document officiel qui contient toutes les informations du document et peut être lue par une machine.
Certificat qualifié	Un certificat qui répond aux exigences énumérées à l'article 3 et à l'annexe I du règlement eIDAS.
Autorité de gestion des politiques	L'entité en charge de la gestion des composants et services PKI. La PMA approuve la politique de certification (CP) et la déclaration de pratiques de certification (CPS) utilisées pour soutenir les services de certification PKI. La PMA se réserve le droit d'auditer l'ICP comme indiqué à la section 8 du présent PR. Dans le contexte du présent document, la PMA est géré par DOCUSIGN FRANCE.
Autorité d'enregistrement	Entité responsable, sous le contrôle de l'autorité de certification et dans le cadre d'un contrat avec l'autorité de certification, de l'identification et de l'authentification des sujets des certificats. En option, l'autorité de certification peut transmettre les documents signés à l'abonné et stocker le fichier d'enregistrement de l'utilisateur. Dans le contexte de ce document, l'AR est géré par QUICKSIGN.
Agent d'enregistrement	Personnecontractuellement ou hiérarchiquement liée à la DRA, qui est responsable de l'identification et/ou de l'authentification des abonnés lors d'une réunion en face à face. La DRA s'assure que cet agent a été formé pour respecter les règles de vigilance à l'égard de la clientèle les plus récentes pour les institutions qui vendent des produits financiers ou des règles équivalentes.
Révocation	Processus par lequel la période opérationnelle d'un certificat prend fin prématurément . La période opérationnelle des certificats demandé par l'autorité de certification est défini dans la stratégie de certificat d'autorité de certification.
Dispositif de création de signature sécurisé	Un dispositif de création de signature répondant aux exigences énoncées dans la directive 1999/93/CE de la plate-forme européenne et du Conseil européen et reconnu dans le règlement eIDAS en vertu de l'article 51.
Signature électronique qualifiée Dispositifs de	Un dispositif de signature électronique qualifié est un dispositif de création de signature sécurisé certifié selon la norme ETSI EN 319-411-2 et pouvant être utilisé pour générer une signature électronique qualifiée.

création	
QUICKSIGN Protocole de consentement	Protocole de consentement exécuté par QUICKSIGN en tant que RA dans le cas de la collecte de la signature manuscrite d'un abonné dans un processus de signature en face à face à l'aide de la tablette d'un DRA.

Abonné	La personne physique recevant un certificat de la certification et l'utilisation d'une clé privée conservée dans un SSCD pour signer numériquement le document envoyé par le Client.
Tablette	Matériel fourni par l'ARD afin d'afficher et d'exécuter le protocole de consentement de manière sécurisée sous le contrôle exclusif du Agent d'enregistrement .
Numéro d'identification de la transaction	Un identificateur unique composé au hasard de lettres et de chiffres attribués à une seule demande d'identification et qui assure l'unicité du certificat.

2. Responsabilités en matière de publication et de dépôt

Ce document est publié par l'AR sur le site internet de l'entreprise : http://www.quicksign.com/.

Il peut également être publié par l'autorité de gestion des politiques en tant que modification de la politique de certificat conformément à ses propres règles de publication.

3. Identification et authentification

3.1. Nommage

La désignation des certificats demandés par l'autorité de certification est conforme à la Recommandation UIT-T X.509 ou IETF RFC 5280 et à la Politique de certification de l'autorité de certification (section 10).

3.2. Validation initiale de l'identité

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

La preuve de propriété de la clé privée correspondant au certificat d'abonné utilisé à des fins de signature est fournie parles ressources techniques et organisationnelles de la plate-forme de signature CA.

3.2.2. Authentification de l'identité de l'organisation

Cette partie n'est pas applicable. l'AR n'accepte que les demandes de personnes physiques demandant des certificats électroniques qualifiés soumis pour leur propre compte et non pour des tiers, sous réserve d'être équivalent à l'abonné. Par conséquent, le service d'enregistrement de l'AR ne comprend aucun processus pour vérifier l'association d'une personne avec une organisation ou une personne morale.

3.2.3. Authentification de l'identité physique de la personne

Tout d'abord, la DRA procède à l'authentification de l'identité de la personne physique (abonné), selon les règles de l'AR et répondant aux exigences contractuellement définies par l'AR.

La DRA vérifie au moment de l'enregistrement initial, par des moyens appropriés et conformément au droit national, l'identité et, le cas échéant, les attributs spécifiques de la personne : pour qui un certificat qualifié est délivré.

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

- par la présence naturelle de la personne physique; ou
- à distance , à l'aide de moyens d'identification électronique, pour lesquels, avant la délivrance du certificat qualifié, une présence physique de la personne physique a été assurée et qui satisfait aux exigences énoncées à l'article 8 de l'eIDAS la réglementation en ce qui concerne les niveaux d'assurance « substantiel » ou « élevé »; ou
- au moyen d'un certificat de signature électronique qualifiée ou d'un cachet électronique qualifié; ou
- en utilisant d'autres méthodes d'identification reconnues au niveau national qui offrent une garantie équivalente en termes de fiabilité à la présence physique, au

sens de l’article 24, paragraphe 1, du règlement eIDAS. L’assurance équivalente est confirmée par unorganisme d’évaluation de la diversité.

Des preuves sont fournies :

- Nom de l'abonné (y compris le nom de famille et au moins un prénom conforme aux pratiques nationales d'identification);
- 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, dans la mesure du possible, pour distinguer la personne des autres personnes portant le même nom.

Si la preuve est fournie d'un document d'identité reconnu au niveau national , la DRA vérifie que ce document est toujours valide et authentique.

Le DRA collecte la référence du document d'identité ou, éventuellement, télécharge une copie du document d'identité. La DRA recueille également le numéro de téléphone de l'Abonné ainsi que son adresse courriel. La DRA met à jour les informations d'enregistrement si elles ont changé.

Le cas échéant, la DRA met à la disposition de l'Abonné un mécanismesécurisé d'authentification géré de manière sécurisée par la DRA selon les règles de sécurité bancaire, associé de manière sécurisée à l'Abonné et considéré comme contrôlé par l'Abonné.

Le DRA enregistre les informations d'enregistrement pendant au moins 7 ans après l'expiration du certificat.

3.2.4. Validation de l'autorité

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

3.2.5. Informations sur les abonnés non vérifiées

Comme décrit ci-dessus, toutes les données et informations personnelles à stocker dans le certificat sontvérifiées par la DRA avant que l'autorité de certification n'envoie des informations à l'autorité de certification. Aucune information non vérifiée n'est utilisée par l'AR pour remplir un certificat.

3.2.6. Critères d'interopérabilité

Les certificats délivrés par les composants PKI sont gérés conformément aux règles et exigences énoncées par l'autorité de certification et le client conformément aux exigences Adobe et ETSI 319-411.

3.3. Identification et authentification pour les demandes de nouvelle clé

Dans le cas d'une demande de reclé, les données d'enregistrement de l'abonné sont mises à jour conformément à la procédure décrite au paragraphe 3.2 de la déclaration de pratiques de certification de l'AR.

3.4. Identification et authentification pour la demande de révocation

L'authentification du demandeur est effectuée par l'autorité de certification conformément à la procédure décrite dans l'énoncé des pratiques de certification.

4. Exigences opérationnelles du cycle de vie du certificat

4.1. Demande de certificat

Lors de l'authentification de l'Abonné, le DRA vérifie si l'ID utilisé lors de l'enregistrement initial est toujours valide. Si l'ID n'est pas valide, l'Abonné est invité par la DRA à mettre à jour ses informations d'identification. Dans tous les cas, la DRA n'envoie à l'AR que les informations d'identité enregistrées lors de la validation initiale de l'identité.

Dans le cas du protocole de consentement QS :

- L'Abonné effectue sur la Tablette sa signature manuscrite dans le Protocole de Consentement présenté par QUICKSIGN lors du Face-à-Face avec le Responsable Enregistrement
- Le Responsable de l'enregistrement vérifie et compare que la signature manuscrite créée sur la tablette est la même que l'image de la signature du signataire de l'abonnésur la pièce d'identité présentée par l'abonné. En cas de différence, le processus de signature est annulé. Dans le cas contraire, l'agent d'enregistrement confirme que la signature manuscrite figurant dans le protocole de consentement est la même que celle contenue dans ledocument d'identification,

Dans tous les cas, la DRA demande alors un certificat. Cette demande de certificat DRA est envoyée en toute sécurité à l'AR avec au moins les informations suivantes :

- Au moins un prénom (s) ;
- Au moins un ou plusieurs nom(s) de famille;
- Adresse e-mail actuelle ;
- Numéro de téléphone portable;
- Informations permettant d'identifier l'Abonné
    - Type d'ID
    - Numéro d'identification
    - Date d'expiration ou date d'émission de la pièce d'identité
    - Pays d'émission
    - Date de naissance
    - Soit une copie de la pièce d'identité officielle avec les informations suivantes lisibles : type d'identification, numéro d'identification, pièce d'identité expiry ou date de délivrance, pays de délivrance,
      Date de naissance
    - Option : la bande MRZ du document d'identité à vérifier par l'AR.
- Identification de l'agent DRA (nom, prénom ou numéro d'identification unique)
  Facultatif : copie de la pièce d'identité officielle ;
- Référence du DRA;
- Le document à signer.

4.2. Traitement des demandes de certificat

L'autorité de certification vérifie en outre, dans l'interface du service d'enregistrement de l'AR, l'identité de l'abonné en :

(a) demander à l'abonné de remplir un formulaire, fourni par l'interface du service d'enregistrement de l'AR, avec une contestation technique sur l'ID si la bande MRZ n'est pas fournie, ou
(b) En vérifiant la validité de la bande MRZ et la présence du document d'identité dans la bande MRZ.

Dans le cas visé au point a):

- si la demande de certificat est effectuée lors d'une rencontre en face à face, la DRA s'assure que seul l'Abonné remplit lui-même ce formulaire, avec des moyens techniques qui sont sous son contrôle exclusif, et
- Ces informations sont collectées en toute sécurité par l'AR selon ses propres procédures et sur sa propre interface. L'AR vérifie la cohérence entre les informations renseignées par l'Abonné dans l'interface RA, d'une part, et les informations d'identification transmises par le système informatique de la DRA, d'autre part.

Si ces vérifications ne peuvent pas être effectuées par l'AR, le service d'enregistrement de l'AR n'envoie aucune demande de certificat à l'autorité de certification et rejette la demande faite par l'abonné.

4.3. Émission de certificat

Afin de procéder à la délivrance du certificat, 2 cas sont possibles :

- Décrit au § 4.3.1: L'authentification de l'abonné est effectuée via un code OTP envoyé par SMS , dans ce cas, une fois le processus d'inscription terminé, et l'abonné a accepté les termes et conditions du service, l'AR appelle la plate-forme de signature CA pour soumettre une demande de certificat, en transmettant les informations suivantes du Abonné:
  - Au moins un prénom (s) ;
  - Au moins un ou plusieurs nom(s) de famille;
  - Adresse e-mail delocation actuelle ;
  - Numéro de téléphone portable.
- Décrit au § 4.3.2 : L'authentification de l'Abonné est effectuée par vérification de la signature manuelle, dans ce cas, une fois le processus d'inscription terminé, et l'abonné a accepté les termes et conditions du service, l'autorité de certification exécute le protocole de consentement et appelle en toute sécurité la plate-forme de signature de l'autorité de certification pour soumettre une demande de certificat, transmettant les informations suivantes de l'abonné:
  - Au moins un premier(s) nom(s);

- Au moins un ou plusieurs nom(s) de famille;
- Adresse e-mail actuelle .

À la fin du processus, l'AR appelle la plate-forme de signature de l'autorité de certification pour sceller le fichier d'épreuve transmettant au moins les informations de demande de certificat DRA (réf. §4.1. Demande de certificat).

Ces informations sont échangées en toute sécurité.

4.3.1. Émission de certificat en cas d'authentification de l'abonné avec un code OTP envoyé par SMS

L'autorité de certification authentifie l'AR.

L'autorité de certification exécute le protocole de consentement avec l'abonné afin de recueillir son consentement pour signer le document et le contrat d'abonné.

L'autorité de certification authentifie l'abonné à l'aide d'un code OTP envoyé par l'autorité de certification à l'abonné par SMS sur le numéro de téléphone mobile transmis par l'autorité de certification.

L'autorité de certification émet des certificats en toute sécurité pour préserver leur authenticité.

L'autorité de certification signe le document avec la clé privée de l'Abonné et supprime la clé privée de l'Abonné.

L'autorité de certification met le certificat contenu dans le document signé (contenu dans le fichier d'épreuve) à la disposition de l'autorité de certification.

L'autorité de certification collecte le fichier de preuve auprès de l'autorité de certification.

4.3.2. Émission de certificat en cas d'authentification de l'Abonné par vérification de sa signature manuelle

L'AR exécute le protocole de consentement avec l'abonné afin de recueillir son consentement pour signer le document et le contrat d'abonné.

L'AR authentifie l'Abonné en demandant à ce dernier d'apposer sa signature manuscrite sur le Protocole de Consentement sur la Tablette. L'autorité de contrôle demande ensuite à l'agent d'enregistrement de confirmer la signature de la main apposée avec la signature de la main présente sur le document d'identité utilisé pour identifier l'abonné. Si ces 2 images correspondent, le DRA Officer est invité à valider la Signature de l'Abonné. L'AR enregistre cette validation et authentifiel'abonné par cette action.

L'AR transmet le document à signer et l'identification de l'abonné à l'autorité de certification.

L'autorité de certification authentifie l'AR. L'autorité de certification héberge en toute sécurité la clé d'authentification dans un module matériel sécurisé certifié (FIPS 140-2

niveau 3 ou CC EAL 4+) qui est sous sa responsabilité.

L'autorité de certification émet des certificats en toute sécurité pour préserver leur authenticité.

L'autorité de certification signe le document avec la clé privée de l'Abonné et supprime la clé privée de l'Abonné.

L'autorité de certification met le certificat contenu dans le document signé (contenu dans le fichier d'épreuve) à la disposition de l'autorité de certification.

L'autorité de certification collecte le fichier de preuve auprès de l'autorité de certification.

4.4. Acceptation du certificat

Les termes et conditions (contrat d'abonnement) du service offert par l'AC et l'AR indiquent ce qui constitue l'acceptation du certificat. Avant d'entrer dans une relation contractuelle avec un abonné, l'autorité de certification informe l'abonné des termes et conditions du service concernant l'utilisation du certificat. Ces termes et conditions mentionnent au moins:

- La politique de certificat qualifié applicable;
- Les limitations d'utilisation du service;
- Les obligations de l'Abonné ;
- Les conditions de révocation du certificat;
- Les conditions dans lesquelles les informations d'inscription et les journaux d'événements sont enregistrés et archivés ;
- Le fait que le certificat n'est pas publié;
- Les limites des responsabilités;
- Règles de confidentialité des données .

Les conditions générales sont mises à disposition par un moyen de communication durable et signées par l'Abonné (voir section 4.3 ci-dessus).

Le nom et le prénom de l'Abonné sont mentionnés sur la page de signature comme informations à valider par l'Abonné à inclure dans le Certificat. L'Abonné accepte les conditions générales du service en cochant au moins une case (voir section 4.3 ci-dessus).

Si l'ID était valide pour la demande de certificat, l'autorité de certification met le document signé avec le certificat intégré à la disposition de l'abonné et de la DRA.

Si l'ID n'était pas valide pour la demande de certificat, l'autorité de certification ne remet pas le document signé avec le certificat incorporé à l'abonné et à la DRA. Le DRA dispose d'un délai maximum de 5 jours, juste après la délivrance du certificat, pour vérifier et vérifier le nouveau document d'identité . Si le nouveau document d'identité n'est pas valide, la DRA soumet une demande de révocation à l'AR . Si le nouveau document d'identité n'a pas été vérifié dans les 5 jours, l'autorité de certification soumet également une demande de révocation à l'autorité de certification. Dans les deux cas, le fichier de preuve n'est pas archivé par l'autorité de certification et est détruit par

l’autorité de certification. Si le nouveau document d’identité est valide, l’autorité de certification met le document signé avec lecertificat intégré à la disposition de l’abonné et de la DRA.

4.5. Utilisation de la paire de clés et du certificat

Les abonnés utilisent leurs clés privées aux fins énoncées à la section 1.4. au-dessus.

4.6. Renouvellement du certificat

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

4.7. Clé de reprise de certificat

La nouvelle clé de certificat est effectuée conformément aux procédures décrites aux paragraphes 4.1. À
4.4. Pour l'authentification de l'Abonné, le paragraphe 3.3. S' applique.

4.8. Modification du certificat

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

4.9. Révocation et suspension du certificat

4.9.1. Circonstances de la révocation

Une demande de révocation est possible pendant 8 jours après l'émission du certificat .

4.9.2. Qui peut demander la révocation

L'Abonné peut soumettre une demande de Révocation à l'AR dans les cas suivants :

- Informations DN renseignées de manière incorrecte ;
- le certificat correspondant à la clé privée a été perdu ou compromis ou est soupçonné de l'être;
- la DRA n'a pas respecté ses obligations et les règles de sécurité décrites dans le présent PR;

La DRA soumet une révocation à l'autorité de réglementation dans les cas suivants:

- Informations DN renseignées de manière incorrecte ;
- le certificat correspondant à la clé privée a été perdu ou compromis ou est soupçonné de l'être;
- le document d'identité valide requis pour effectuer une transaction à distance (dans le cas où le document d'identité qui a été utilisé pour la validation initiale de l'identité en face à face n'est pas valide): a été vérifié et n'est pas valable;

L'autorité de certification soumet une révocation à l'autorité compétente dans les cas suivants:

- Informations DN renseignées de manière incorrecte ;

- le certificat correspondant à la clé privée a été perdu ou compromis ou est soupçonné de l'être;
- la DRA n'a pas respecté ses obligations et les règles de sécurité décrites dans le présent PR.

4.9.3. Procédure de demande de révocation

Si la Révocation est demandée par l'Abonné, il adressera la demande en envoyant un courrier électronique à une adresse électronique dédiée de l'AR . L'adresse e-mail, ainsi que les informations à inclure dans la demande de révocation, sont affichées dans les termes et conditionsdu service. L'adresse e-mail est disponible 24 heures sur 24. Il n'y a pas de service client qui peut être contacté par téléphone.

Afin d'authentifier la demande de Révocation, l'Abonné doit être disponible dans les huit (8) heures ouvrables suivant sa soumission. Au cours de cette période de huit (8) heures ouvrables, il sera contacté par l'agent de révocation de l'AR au numéro de téléphone fourni pour générer le certificat désigné. Si l'abonné ne répond pas au téléphone, la demande de révocation est considérée comme invalide et l'autorité de réception ne donnera pas suite à la demande de révocation. Si l'Abonné souhaite toujours révoquer son certificat, il doit soumettre une nouvelle demande de Révocation de la mendicité.

Lorsque la demande de révocation estauthentifiée, l'autorité de certification suit la procédure décrite au paragraphe 4.9.3 de la politique de certificat. Une fois que la plate-forme de signature de l'autorité de certification a confirmé la révocation, l'autorité de certification en informe l'AR et l'abonné par e-mail dans un délai d'une heure. La révocation est effectuée en moins de 24 heures.

Si la révocation est demandée par le DRA, la DRA doit adresser **la** demande en envoyant un e-mail à une adresse e-mail dédiée de l'AR. L'adresse e-mail, ainsi que les informations à inclure dans la demande de révocation, sont affichées dans le contrat entre QUICKSIGN et le DRA. L'adresse e-mail est disponible 24 heures sur 24. Aprèsque la demande de révocation soit authentifiée, l'AR suit la procédure décrite au paragraphe 4.9.5. de la Politique de certificat. Une fois que la plate-forme de signature de l'autorité de certification a confirmé la révocation, l'autorité de certification en informe l'AR et l'abonné par e-mail dans un délai d'une heure. La révocation est effectuée en moins de 24 heures.

Si la révocation est demandée par l'AR, celle-ci doit suivre la procédure décrite au paragraphe 4.9.5 de la politique en matière de certificats. Une fois que la plate-forme de signature de l'autorité de certification a confirmé la révocation, l'autorité de certification en informe l'AR et l'abonné par e-mail dans un délai d'une heure. La révocation est effectuée en moins de 24 heures.

Les demandes de révocation et les actions suivantes sont enregistrées manuellement par l'AR.

5. Contrôles des installations, de gestion et d'exploitation

5.1. Contrôles physiques

Tous les contrôles physiques, y compris l'inspection des locaux et la construction des installations du centre de données utilisées pour exécuter le service d'enregistrement, sont vérifiés par un auditeur technique indépendant.

L'accès physique aux bureaux de l'AR est limité aux personnes autorisées seulement. 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.

Lescontrôles 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 de l'information et des installations de traitement de l'information; et pour empêcher que les actifs RA ne 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 protégé est défini pour protéger les composants critiques contre les intrusions ; L'accès à ce périmètre de sécuritéest contrôlé, notamment par des alarmes afin de détecter les intrusions.

5.2. Contrôles procéduraux

Tous les rôles à remplir au sein de l'AR et de l'ARD sont bien définis 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.

La RA et la DRA administrent l'accès utilisateur à chaque rôle. L'administration comprend la gestion des comptes d'utilisateurs et la modification ou la suppression en temps opportun de l'accès. L'accès aux informations et aux fonctions d'application est restreint 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 est responsable de ses activités via le journal des événements ou le journal classique.

5.3. Contrôles du personnel

Le personnel de la DRA et de l'AR chargé du processus d'inscription, de la gestion de l'infrastructure ou de l'assistance aux abonnés est bien qualifié et formé.

Le personnel de la DRA et de la RA qui ne travaille pas selon les règles et procédures établies est passible desanctions disciplinaires conformément au droit du travail français .

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

Le personnel applique des procédures et des processus administratifs et de gestion qui sont conformes aux procédures de gestion de la sécurité de l'information de l'AR.

Le personnel d'encadrement possède une expérience ou une formation en matière d'ingénierie et de sécurité de l'information.

Le personnel qui prend des décisions sur le processus d'inscription est libre de tout conflit d'intérêts et a le plein pouvoir de décision, sauf dans les situations de crise.

Le personnel est officiellement nommé à des rôles de confiance par la haute direction selon le principe du « moindre privilège ». Le personnel n'a accès à des rôles de confiance qu'après avoir prouvé sa qualification pour les rôles décrits. le personnel de RA prouve sa confianceen présentant son casier judiciaire ainsi que de bonnes références d'anciens employeurs.

5.4. Procédures de journalisation d'audit

Les fichiers journaux d'audit sont générés pour tous les événements liés à la sécurité et aux services RA et DRA. Dans la mesure du possible, les journaux d'audit de sécurité sont automatiquement collectés. Lorsque cela n'est pas possible, un journal de bord ou un autre mécanisme physique doit être utilisé. Tous les registres de sécurité, électroniques et non électroniques, sont conservés et mis à disposition pendant les audits de conformité.

La confidentialité des renseignements sur le sujet 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 consignés de telle sorte qu'ils ne peuvent pas être facilement supprimés ou détruits (sauf pour le transfert vers des supports à long terme) pendant la période de temps qu'ils doivent être conservés. Les journaux d'audit sont protégés de manière à rester lisibles pendant toute la durée de leur période de stockage. Les journaux d'audit et les résumés d'audit sont sauvegardés via des mécanismes de sauvegarde d'entreprise.

Une analyse des vulnérabilités sur les adresses publiques est effectuée sur une base mensuelle. Une analyse des vulnérabilités sur les adresses IP privées est effectuée chaque année.

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

5.4.1. Autorité d'enregistrement

La journalisation comprend au moins les rubriques suivantes :

- Accès physique aux installations;

- Gestion fiable des rôles;
- Accès logique ;
- Gestion des sauvegardes;
- Gestion des journaux;
- Révocation de l'authentification et de la demande;
- Collecte du dossier de preuve auprès de l'AC;
- Données d'enregistrement envoyées par la DRA ;
- Dans le cas du protocole de consentement QS: acceptation de la signature manuscrite par l'agent d'enregistrement;
- Gestion informatique et réseau.

5.4.2. Pouvoir d'enregistrement délégué

La journalisation comprend au moins les rubriques suivantes :

- l'identification et l'authentification de l'abonné, y compris les informations de la pièce d'identité de l'abonné, son adresse électronique et son numéro de téléphone;
- les circonstances de l'identification et de l'authentification de l'Abonné ;
- gestion des moyens d'authentification de l'Abonné ;
- Accès logique ;
- Gestion des sauvegardes;
- gestion des rôles de confiance;
- gestion des journaux d'accès; en particulier, la DRA doit disposer d'une liste de tous les accès autorisés à inscrire et à gérer les Abonnés;
- Gestion informatique et réseau.

5.5. Archives de documents

5.5.1. Autorité d'enregistrement

L'AR enregistre au moins:

- les informations d'inscription suivantes :
  - Identité de la DRA;
  - la méthode utilisée pour valider les documents d'identification (c.-à-d. rencontre en personne);
  - Le rôle de QUICKSIGN en tant que RA;
  - Journaux d'inscription.
- l'acceptation de l'Abonné à ses obligations :
  - consentir à la tenue d'un registre par l'AR et /ou la DRA des informations utilisées dans l'enregistrement, de tout attribut spécifique du sujet placé dans le certificat, et à la transmission de ces informations à des tiers dans les mêmes conditions que celles requises par la présente politique dans le cas où l'AR met fin à ses services;

- si, et dans quelles conditions, l'Abonné exige et le consentement du sujet à la publication du Certificat ;
- la confirmation que les informations contenues dans le certificat sont correctes.

L'enregistrement est archivé pendant au moins sept ans après l'expiration du certificat.

La confidentialité et l'intégrité des dossiers actuels et archivés concernant les certificats qualifiés sont maintenues. Les dossiers sont archivés de façon complète et confidentielle conformément aux pratiques commerciales divulguées; Ils sont mis à disposition si cela est nécessaire aux fins de fournir la 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 enregistrements RA sont protégés contre les dommages et stockés uniquement dans des zones d'accès restreint. Le support est crypté et nécessite un contrôle d'accès spécial pour être lu;

- Les médias sont supervisés par le système d'archivage pour identifier les supports en danger d'obsolescence ou de détérioration. Les supports identifiés doivent êtreéchangés par l'administrateur système en s'assurant que les données ne sont pas perdues ou récupérées à partir du 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 médias utilisés dansle système d'archivage ne peuvent pas être utilisés ou réutilisés dans un autre contexte en raison du système de fichiers crypté utilisé, différent de ceux utilisés pour stocker les données opérationnelles.

5.5.2. Pouvoir d'enregistrement délégué

La DRA enregistre les informations d'enregistrement suivantes :

- Type de document présenté par l'Abonné à l'appui de l'inscription;
- Numéro d'identification ou, le cas échéant, copie de la pièce d'identité ;
- Registres d'enregistrement;
- Lieu de stockage des copies des demandes et des documents d'identification, y compris le contrat d'abonnement signé;
- Fichiers d'épreuve pour tous les certificats générés par l'autorité de certification;
- la méthode utilisée pour valider les documents d'identification (c.-à-d. rencontre en personne); Le dossier est archivé pendant au moins sept ans après l'expiration du certificat.

La confidentialité et l'intégrité des dossiers archivés concernant les certificats qualifiés sont

maintenues. Les dossiers sont archivés de façon complète et confidentielle conformément aux pratiques commerciales divulguées; ils sont mis à disposition si cela est nécessaire auxfins de

fournir une preuve de 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 enregistrements DRA sont protégés contre les dommages et stockés uniquement dans des zones d'accès restreint. Le support est crypté et nécessite un contrôle d'accès spécial pour être lu;

- Les médias sont supervisés par le système d'archivage pour identifier les supports en danger d'obsolescence ou de détérioration. Les supports identifiés doivent être échangés par l'administrateur système en s'assurant que les données ne sont pas perdues ou récupérées à partir du miroir du système d'archivage;

- Tous les supports utilisés pour communiquerdes données personnelles sont supprimés et détruits à la fin de leur durée de vie;

- Tous les médias utilisés dans le système d'archivage ne peuvent pas être utilisés ou réutilisés dans un autre contexte en raison du système de fichiers crypté utilisé qui est différent de ceux utilisés pour stocker les données opérationnelles.

5.6. Changement de clé

La validité du certificat d'abonné est définie dans la stratégie de certificat d'autorité de certification.

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 les 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 d'autorité d'enregistrement pour l'autorité de certification, il doit :

- notifier l'AC avant la résiliation selon les procédures convenues dans le contrat commercial,
- envoyer une lettre recommandée à la PMA,
- détruire toutes les clés privées utilisées pour sécuriser la communication avec CA le lendemain du jour de la résiliation,
- stop pour livrer les demandes de certificat,
- informer les abonnés et les parties utilisatrices dans le cas où il a été compromis dans son rôle d'autorité d'enregistrement.

La décision concernant l'entité à laquelle QUICKSIGN doit fournir des enregistrements archivés doit être prise par l'autorité de certification.

5.8.2. Pouvoir d'enregistrement délégué

Si la DRA prévoit de mettre fin à son rôle d'autorité délégataire en matière d'enregistrement, elle doit :

- notifier l'autorité de réglementation avant la résiliation conformément aux procédures convenues dans le contrat commercial,
- envoyer une lettre recommandée à l'AR ,
- arrêter pour livrer les demandes de certificat,
- aviser les abonnés et les parties utilisatrices dans le cas où il a été compromis dans son rôle d'autorité d'enregistrement déléguée.

La décision concernant l'entité à laquelle la DRA doit remettre les documents archivés est définie contractuellement entre l'AR et la DRA.

6. Contrôles techniques de sécurité

6.1. Génération et installation de paires de clés

L'autorité de certification génère des clés en toute sécurité et la clé privée est secrète. L'autorité de certification vérifie que le dispositif est certifié en tant que QSCD qualifié répondant aux exigences du règlement eIDAS.

6.2. Protection des clés privées et ingénierie des modules cryptographiques

La génération de paires de clés CA est effectuée conformément au PC de l'autorité de certification.

6.3. Autres aspects de la gestion des paires de clés

D'autres aspects de la gestion des paires de clés sont effectués par l'AC selon le 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'autorité compétente conformément à ses propres principes. En particulier, il existe deux cas d'utilisation pour activer la clé privée :

- Cas d'utilisation générique : l'Abonné utilise un code OTP généré par l'AC et transmis au numéro de téléphone enregistré pour l'Abonné,
- Protocole de consentement QS : l'apposition de la signature manuelle et la validation de l'agent d'enregistrement contre l'image de la signature contenue sur la pièce d'identité présentée.

6.5. Contrôles de sécurité informatique

Les contrôles (p. ex. pare-feu) protègent les domaines de réseau interne de l'AR et de la DRA contre tout accès non autorisé. Les pare-feu sont également configurés par l'AR et la DRA pour empêcher tous les protocoles et accès non requis par l'opération concernée. L'AR et la DRA veillentà ce que l'accès au système soit limité aux personnes dûment autorisées.

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

6.6. Contrôle de la sécurité du cycle de vie

L'AR et la DRA utilisent des systèmes et desproduits fiables qui sont protégés contre toute modification et garantissent la sécurité technique et la fiabilité des processus qu'ils soutiennent.

Une analyse des exigences en matière de sécurité est effectuée au stade de la conception et de la spécification des exigences de tout projet entrepris par l'AR , en particulier pour s'assurer que la sécurité est intégrée au système informatique de la DRA.

Les procédures de contrôle des modifications s'appliquent aux versions, aux modifications et aux correctifs logiciels d'urgence pour tout logiciel opérationnel et les changements apportés à la configuration. Les procédures comprennent la documentation des changements.

L'intégrité des systèmes et des renseignements de l'AR et de la DRA est protégée contre les virus et les logiciels malveillants et non autorisés. La perted'incidents et de dysfonctionnements de sécurité est minimisée grâce à l'utilisation de procédures de signalement et de réponse aux incidents. Les supports utilisés dans le cadre de l'AR et de la DRA sont manipulés de manière sécurisée pour protéger les supports contre les dommages, le vol et l'accès non autorisé. Les procédures de gestion des médias protègent contre l'obsolescence et la détérioration des médias pendant la période pendant laquelle les documents doivent être conservés. Des procédures sont établies et mises en œuvre pour tous les rôles de confiance et administratifs qui ont une incidence sur la fourniture de 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 lesappliquer, et que les raisons de ne pas appliquer de correctifs de sécurité sont documentées et choisies par l'AR et l'équipe DRA .

6.7. Contrôles de sécurité réseau

L'AR et la DRA maintiennent et protègent tous leurs systèmes dans au moins une zone sécurisée et mettent en œuvre et configurent 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 électroniques ou manuelles sont utilisées pour maintenir l'heure du système. Pour le temps sécurisé sur les enregistrements d'audit, l'AR se synchronise régulièrement avec un service de temps.

7. Cadre pour la définition d'autres stratégies de certificat basées sur le présent document

L'AR n'a pas d'autre politique d'enregistrement que ce document.

8. Audit de conformité et autres évaluations

8.1. Fréquence ou circonstances de l'évaluation

8.1.1. Autorité d'enregistrement

Service d'enregistrement après la fin de la période transitoire (art 51 de l'eIDAS), une évaluation ETSI selon sera effectuée par un auditeur externe.

Avant d'exécuter son service, RA doit être audité par un auditeur externe par rapport à ETSI 319 411-2 (QCP-n-qscd).

La première année suivant l'audit externe, un audit peut être effectué par l'autorité de certification sur l'autorité de certification conformément au programme d'audit de la plateforme de signature de l'autorité de certification.

La deuxième année suivant un audit externe, un nouvel audit externe doit être effectué.

En cas de constatations importantes découvertes au cours d'une vérification interne effectuée par l'AC, l'AR résoudra ces problèmes et une vérification externe sera effectuée au cours de la même année.

8.1.2. Pouvoir d'enregistrement délégué

L'AR contrôle le respect par la DRA de ses engagements et de la présente politique d'enregistrement. Un plan d'audit est défini par l'AR et approuvé par l'EGR.

La DRA accepte que l'AR ou la PMA effectue une vérification de la conformité avant de commencer son rôle de DR.

L'AR accepte que l'AR et la PMA effectuent une vérification au besoin pour s'assurer qu'elle se conforme à la présente politique d'enregistrement et au PC.

Si une non-conformité majeure est révélée lors de l'un de ces audits, l'autorité d'enregistrement déléguée doit se conformer sans délai au PR et au CP. Si le problème n'est pas résolu dans un délai déterminé par l'auditeur , l'AR suspendra ses services jusqu'à ce que la conformité effective soit atteinte, dans les conditions prévues dans le contrat entre l'AR et le DRA.

8.2. Sujets couverts par l'évaluation

8.2.1. Autorité d'enregistrement

Le périmètre d'un audit de QUICKSIGN en tant qu'autorité d'enregistrement est :

- Protection, utilisation et gestion des paires de clés utilisées pour protéger la

communication avec l'autorité de certification;

- Création de la demande de certificat technique;

- les dossiers de l'AR par rapport aux exigences fixées dans le PC;
- Procédure d'enregistrement définie par l'AR pour identifier, authentifier et gérer la demande de certificat auprès de l'autorité de certification;
- Révocation procedure;
- Gestion fiable des rôles;
- Gestion des TI et des incidents;
- Sécurité physique;
- Gestion des dossiers de preuves;
- Protection et gestion des données personnelles des abonnés.

8.2.2. Pouvoir d'enregistrement délégué

Le périmètre d'un audit de la DRA est :

- Procédures d'enregistrement niveau d'exigences défini par l'autorité de réglementation au paragraphe 1.3.2 pour identifier, authentifier et gérer les demandes de certificat ;
- Protection, utilisation et gestion des moyens utilisés pour protéger la communication avec l'AR;
- Gestion des dossiers de preuves;
- Gestion fiable des rôles;
- L'authentification sécurisée de l'abonné signifie type et gestion;
- Gestion des TI et des incidents utilisée pour gérer le portail des abonnés et des DRA;
- Sécurité physique;
- Protection et gestion des données personnelles des abonnés.

9. Autres questions commerciales et juridiques

9.1. Honoraires

Ces services sont définis dans le contrat établi entre l'AR et la DRA.

9.2. Responsabilité financière

La RA maintient des niveaux raisonnables de couverture d'assurance et des ressources financières suffisantes pour maintenir ses activités. La couverture d'assurance ou de garantie est définie dans le contrat entre l'AR et la DRA.

9.3. Confidentialité des renseignements commerciaux

L'AR maintient la confidentialité des renseignements commerciaux confidentiels, y compris les données d'identité personnelle, la demande de certificat d'abonné, les résultats et les rapports d'audit, le plan de continuité des activités et le contrat avec l'ARD.

9.4. Confidentialité des renseignements personnels

9.4.1. Autorité d'enregistrement

L'AR 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'AR est documenté dans son ISSP. Ces règles sont présentées à chaque Abonné avant toute transaction dans les termes et conditions du service, qui doivent être convenus par l'Abonné en cliquant sur une case à cocher.

QUICKSIGN en tant qu'Autorité d'Enregistrement est supervisée par la Commission Nationale de l'Informatique et des Libertés (CNIL) et désigne un délégué à la Protection des Données. Ses coordonnées sont les suivantes :

David Leroy

QUICKSIGN

19-21 rue Poissonnière

75002 PARIS

9.4.2. Pouvoir d'enregistrement délégué

La DRA protège la confidentialité et l'intégrité des données d'enregistrement. L'ensemble des règles de confidentialité des données de la DRA est documenté et conforme à la législation européenne applicable en matière de confidentialité des données.

9.5. Droits de propriété intellectuelle

Cette partie n'est pas applicable. La PMA conserve la propriété intellectuelle des certificats d'autorité de certification qu'elle publie.

9.6. Déclarations et garanties

9.6.1. Autorité d'enregistrement

L'AR alerte la PMA en cas d'incident de sécurité.

L'autorité de certification informe l'abonné des conditions générales relatives à l'utilisation d'un certificat avant de soumettre une demande de certificat à l'autorité de certification. L'Abonné accepte les termes et conditions du service en cochant une case sur l'écran. L'AR envoie à l'abonné un e-mail contenant les termes et conditions du service, ou, éventuellement, met ces termes à disposition sur son site Web.

L'AR protège son système d'information et garantit la sécurité des données transmisesà l'ICP.

L'AR authentifie le DRA et l'Abonné.

L'AR approuve la procédure DRA et les moyens d'authentification sécurisés utilisés par le DRA pour l'authentification des abonnés avant d'autoriser un DRA à utiliser le service. La méthode utilisée pour autoriser un DRA est approuvée par la PMA.

L'AR établit une relation contractuelle avec une DRA engageant la DRA à remplir ses obligations conformément à la présente politique d'enregistrement.

L'AR fera de son mieux pour s'assurer qu'au fil du temps, la DRA respecte ses obligations en vertu de la présente politique d'enregistrement.

L'AR collabore avec l'AC dans le cadre des activités de contrôle et d'audit menées dans le cadre de l'AR.

L'AR informe PMA pour tous les nouveaux DRA qui souhaitent utiliser le service et transmettre une synthèse de la procédure DRA.

L'autorité de réception informe l'abonné si la clé privée de l'abonné a été perdue, volée ou potentiellement compromise en raison de la compromission des données d'activation ou pour d'autres raisons.

L'autorité de certification s'assure qu'aucun certificat n'est utilisé par l'abonné ou une partie utilisatrice, si l'autorité de certification lui a dit que le certificat de l'abonné a été compromis.

L'autorité de certification transmet uniquement les demandes de révocation authentifiées

à l’autorité de certification.

L'autorité d'évaluation apporte son soutien aux équipes d'audit de manière constructive et déploie tous les efforts raisonnables nécessaires pour mener à bien un audit et en communiquer les résultats.

Dans le cas du protocole QS Consent, l'autorité de certification exécutera le protocole de consentement et l'activation de la signature avec une tablette conformément au processus approuvé par l'autorité de certification.

9.6.2. Pouvoir d'enregistrement délégué

Les obligations de la DRA sont définies contractuellement entre l'AR et la DRA.

L'ARD s'assure que chaque abonné pour lequel une demande de certificat est soumise à l'autorité de certification par l'intermédiaire de l'autorité de certification a été identifié et authentifié correctement et que la demande de certificat a été exacte et dûment autorisée. La DRA s'assure que la demande de certificat soumise contient uniquement des informations exactes et complètes.

La DRA veille à ce que son organisation possède l'expertise, la fiabilité, l'expérience et les qualifications nécessaires et qu'elle ait reçu une formation appropriée concernant les règles de sécurité et de protection des données à caractère personnel pour l'identification et l'authentification, conformément aux règles de diligence raisonnable applicables aux établissements vendant des produits financiers ou à des règles équivalentes.

La DRA protège son système d'information et garantit la sécurité des données transmises à l'AR.

La DRA protège la confidentialité et l'intégrité des données d'enregistrement.

Le DRA doit exécuter et sécuriser la tablette conformément aux règles approuvées par l'AR et l'AC.

9.7. Exclusions de garanties

La DRA garantit la validation initiale de l'identité et l'authentification de l'Abonné . L'AR garantit qu'elle n'entrera dans une relation contractuelle qu'avec les DRA qui, en raison de la nature des services qu'elles fournissent, sont tenues de veiller à ce que ses a été formée pour respecter les exigences légales les plus récentes en matière de vérification d'identité et de rencontre en face à face conformément aux règles de diligence raisonnable pour les institutions vendant des produits financiers ou à des règles équivalentes.

L'AR garantit également qu'elle s'assurera de la capacité financière de la DRA. L'AR ne fournit aucune autre garantie, expresse ou implicite, légale ou autre et décline toute responsabilité pour la validation initiale de l'identité et l'authentification de l'Abonné.

En conséquence, sous réserve que la DRA ait rempli son rôle tel que décrit dans le présent document, l'AR garantit l'identification et l'authentification de l'Abonné. L'autorité

de certification ne fournit aucune garantie, expresse ou implicite, légale ou autre, et décline toute responsabilité quant au succès ou à l'échec du déploiement de l'ICP ou à la validité juridique ou à l'acceptation des certificats d'autorité de certification.

9.8. Limitations de responsabilité

L'autorité de réglementation ne fait aucune déclaration concernant l'adéquation ou l'authenticité des certificats délivrés en vertu de ce PR. Les parties utilisatrices ne peuvent utiliser ces certificats qu'à leurs propres risques. L'AR n'assume aucune responsabilité en ce qui concerne l'utilisation du certificat pour toute autre utilisation que celle décrite dans le présent document.

La DRA est responsable de l'exactitude de toutes les informations d'enregistrement, sous réserve des termes du contrat entre l'AR et la DRA. L'AR n'est pas responsable de tout retard, non-livraison, non-paiement, erreur de livraison ou interruption de service causé par un tiers, y compris le DRA.

9.9. Indemnités

L'autorité de réglementation ne fait aucune déclaration concernant l'utilisabilitéou l'authenticité des certificats délivrés en vertu de ce PR. Il n'y a aucune obligation d'effectuer des paiements concernant les coûts associés au dysfonctionnement ou à l'utilisation abusive des données personnelles vérifiées pour une demande de certificat.

9.10. Durée et résiliation

Le PR et les versions ultérieures entrent en vigueur dès leur approbation par la PMA.

Si l'autorité de surveillance cesse de fonctionner, elle suit la procédure décrite au paragraphe 5.8 du présent document.

9.11. Avis individuels et communications avec les participants

QUICKSIGN, en tant qu'autorité d'enregistrement, fournit une nouvelle version de cette politique d'enregistrement via son site Web.

9.12. Amendements

L'AR examine ce document et son énoncé des pratiques de certification au moins une fois par an. Des examens supplémentaires peuvent être effectués à tout moment à la discrétion de l'AR. Toute modification est approuvée par la PMA.

9.13. Dispositions relatives au règlement des différends

Les dispositions relatives au règlement des différends entre le DA et la DRA 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'applicabilité, l'interprétation et la validité de la présente politique, indépendamment du contrat ou de tout autre choix de dispositions légales et sans qu'il soit nécessaire d'établir un lien commercial en FRANCE.

Cette disposition de la loi applicable s'applique uniquement à la politique d'enregistrement. Les contrats avec un client faisant référence à cette politique peuvent avoir leurs propres dispositions de droit applicable, à condition que cette section régisse l'applicabilité, l'interprétation et la validité de cette politiqueindépendamment des termes de ces autres accords.

9.15. Respect de la loi applicable

La présente politique d'enregistrement est soumise aux lois, règles, règlements, ordonnances, décrets et arrêtés français et européens applicables . La DA et la DRA conviennent de se conformer aux lois et règlements applicables dans leurs contrats.

9.16. Dispositions diverses

Ce PR constitue l'intégralité de l'entente entre les parties et remplace toutes les autres conditions, expresses ou implicites par la loi. Aucune modification du présent PR n'a force de faire à moins d'être faite par écrit et signée par un signataire autorisé. Le défaut d'appliquer tout ou partie de ces articles dans un cas particulier ne constitue pas une renonciation ou n'empêche pas l'application ultérieure. Toutes les dispositions de ce RP qui, par nature, prolongent la durée d'exécution des services (par exemple les informations confidentielles et les droits de propriété intellectuelle) servent ces conditions et s'appliquent au successeur de toute partie.

Si une section de ce PR est incorrecte ou invalide, les autres sections de ce PR restent en vigueur jusqu'à ce que le PR soit mis à jour.