

Politique d'enregistrement, de signature électronique et de gestion de la preuve pour Arkéa Banque Privée

Version 2021

Sommaire

SOMMAIRE	2
AVERTISSEMENT	3
I – CONTEXTE ET OBJECTIFS	4
II – CHAMP D’APPLICATION	5
III – IDENTIFICATION DE LA PESGP	8
IV - ACTEURS ET ROLES	9
1. CLIENT.....	9
2. LA BANQUE	9
3. AUTORITE D’ENREGISTREMENT (« AE »)	10
4. AUTORITE D’ENREGISTREMENT DELEGUEE (« AED »)	11
5. OPERATEUR D’ENREGISTREMENT (« OE »)	11
6. AUTORITE DE CERTIFICATION ET DE GESTION DE LA PREUVE (« ACGP »)	11
V – OBLIGATIONS DES ACTEURS	12
1. LE SIGNATAIRE.....	12
1.1 Identification et authentification.....	12
1.2 Environnement de l’application de signature.....	12
1.3 Outils de signature utilisé	12
1.4 Type de certificat utilisé	13
2. LA BANQUE	13
1.1 Obligations métiers	13
1.2 Type de certificat utilisé	14
VI – IDENTIFICATION ET AUTHENTIFICATION	14
1. IDENTITES UTILISEES	14
2. AUTHENTIFICATION, CREATION, MISE A JOUR DE L’IDENTITE DU CLIENT	14
VII – SIGNATURE ET VALIDATION	16
1. DOCUMENT METIER	16
2. PROTOCOLE DE CONSENTEMENT	16
2.1 Identification	16
2.2 Documents métier et documents Client.....	16
2.3 Navigation et action Client	17
3. SIGNATURE CLIENT.....	17
3.1 Normes de signature	18
3.2 Algorithmes utilisables pour la signature	18
4. VALIDATION.....	18
VIII – POLITIQUE DE CONFIDENTIALITE	18
1. CLASSIFICATION DES INFORMATIONS.....	18
2. COMMUNICATION DES INFORMATIONS A UN TIERS	18
IX – MISE A DISPOSITION DE L’EXEMPLAIRE SIGNE	19
X – CONSERVATION DE LA PREUVE	19

Avertissement

La présente PESGP, après finalisation et validation par les instances ad hoc, a pour objectif d'être portée à la connaissance du signataire, ou du moins être mise à sa disposition, afin de lui permettre de comprendre le sens de l'engagement pris en signant de cette manière.

Elle s'adresse aussi aux éventuels destinataires des documents signés qui seront ainsi informés des conditions dans lesquels les signataires ont été identifiés et authentifiés et la manière dont les signatures ont été recueillies et conservées.

Elle ne se substitue pas aux conditions générales de banque ni à la convention de signature électronique mais vient en complément des documents pré-contractuels d'usage.

Elle est utilement référencée via un N° OID (Object Identifier) dans les documents métier pré-contractuels et contractuels.

I – Contexte et objectifs

Dans le cadre de son activité commerciale de gestion patrimoniale, via la structure Arkéa Banque Privée, Federal Finance (« la Banque ») déploie des outils de souscription de produits bancaires ou d'assurance, en ligne ou en face à face, par voie électronique.

Lorsque le service de signature électronique est mis à disposition des clients signataires, ces derniers doivent avoir connaissance du contexte dans lequel leur signature est produite et conservée mais aussi du rôle des acteurs en présence et de leur responsabilité.

Ce document présente la Politique d'Enregistrement, de Signature et de Gestion de la Preuve (« PESGP ») que la Banque doit fournir à ses clients lors de l'utilisation de ces services (« le Service »).

La présente PESGP décrit les règles que les clients de la Banque doivent respecter pour s'identifier et s'authentifier puis signer électroniquement les documents proposés. La constitution et la conservation des éléments de preuves relatifs aux transactions électroniques réalisées entre les parties ont vocation à démontrer ultérieurement l'existence et l'intégrité de la (ou des) signature(s) des documents et ainsi engager les parties sur les termes les concernant.

Le présent document est destiné principalement aux personnes signataires :

- Le client qui s'identifie auprès des services de la Banque et appose son consentement sur un document métier.
- La Banque qui émet le document et met en œuvre le Service ;

Ce document d'adresse aussi aux éventuels destinataires des documents signés afin de leur permettre de prendre connaissance des conditions dans lesquelles ces signatures ont été réalisées.

Enfin, ce document vient compléter les documents suivants :

- La Politique de certification du service de signature électronique de l'AC Docusign
(OID : 1.3.6.1.4.1.22234.2.14.3.33)
- La Politique d'horodatage [...] non certifiée de l'AC Docusign (OID : 1.3.6.1.4.1.22234.2.6.5.7)
- La Politique de certification du service de cachet électronique de l'AC Docusign
(OID : 1.3.6.1.4.1.22234.2.9.3.9)
- La Politique d'archivage du PSAE CDC Arkhinéo (OID : 1.3.6.1.4.1.29371.1.1.3.2)
- Les Conditions Générales de Banque
- La Convention de signature électronique

II – Champ d’application

La présente PESGP couvre la signature électronique des contrats bancaires ou d’assurance que la Banque propose à la souscription, en ligne ou lors d’un face à face sur support électronique, à ses clients personnes physiques ou morales.

Cette PESGP couvre les signatures simple et avancée.

La présente PESGP s’applique à toutes les transactions métiers que la Banque propose à la signature à ses clients au moyen d’un terminal d’affichage.

Les signatures électroniques créées par le Service sont admises à titre de preuve au même titre qu’un écrit sur support papier conformément à l’article 1366 du Code Civil dans la mesure où :

- Le signataire est clairement identifié ;
- L’acte est établi et conservé dans des conditions de nature à en garantir l’intégrité ;
- L’écrit est lié de façon indissociable à la signature.

Le Service, pour la partie signature électronique, s’appuie sur une Autorité de Certification (« AC ») qualifiée.

Il est toutefois précisé que les signatures simples et avancées générées par le Service ne sont pas qualifiées au sens du décret 2017-1416 du 28 septembre 2017 (pris pour application de l’article 1367 du Code Civil) de sorte que la Banque se réserve le droit de constituer un ensemble de preuves destinées à rendre vraisemblable la signature aux yeux de la juridiction compétente vu les dispositions de l’article 1368 du Code Civil.

La conservation de la preuve auprès du Prestataire de Service d’Archivage Électronique (« PSAE ») n’a d’autre objectif que de fournir, sur demande express d’une juridiction compétente, des éléments permettant de régler un litige déclaré entre la Banque et le Client.

Par ailleurs, la Banque archive un exemplaire de la transaction signée à des fins de gestion de sa relation client.

Enfin, il est fortement conseillé au Client de ne pas détruire l’exemplaire de la transaction signée qui lui est confié.

Ce document vise à répondre à plusieurs contextes :

- Contexte bancaire :
 - o La Banque, s’appuie sur la Direction des Flux du groupe Crédit Mutuel ARKEA (« DFL ») qui, conjointement avec la Direction des Produits Bancaires (« DPB »), définit l’ensemble des briques techniques et les schémas fonctionnels permettant de donner une valeur contractuelle à une procédure électronique mettant en œuvre le service Protect&Sign de l’AC Docusign,inc.
 - o Cette infrastructure doit notamment répondre aux besoins métiers de vente en ligne, à distance ou en face à face et de non matérialisation des contrats.

- Contexte fonctionnel :
 - L'identification et l'authentification du Client, comme préalable à la signature, peut se faire (i) soit en face à face avec un Opérateur d'Enregistrement (« OE ») pour les Autorités d'Enregistrement (« AE ») disposant d'un réseau d'agences ou de caisses locales ou encore au travers d'un Intermédiaire en Opération de Banque et de Service de Paiement (« IOBSP ») qui tiendra le rôle d'Autorité d'Enregistrement Délégué (« AED ») ; (ii) soit à distance, pour les entités (AE ou AED) proposant un espace client sur Internet.
 - En plus de l'authentification du signataire et du recueil de son consentement propre à la signature papier, le procédé de signature électronique exige la mise en œuvre d'un procédé fiable d'identification garantissant le lien entre la signature électronique et l'acte auquel elle s'attache.
 - Le certificat client portant son identité est ainsi apposé dans un délai court (5 minutes) après son consentement en utilisant un certificat éphémère (à la volée, ou à usage unique) délivré par l'Autorité de Certification.
- Contexte réglementaire :
 - Le processus de signature électronique mis en œuvre doit répondre à la réglementation en vigueur notamment celle qui découle du règlement européen N°910/2014 du 23 juillet 2014 (dit « règlement eIDAS ») mais aussi aux exigences des articles 1366, 1367 et 1375 du Code Civil. Pour cela, la DFL a eu recours aux conseils de la Direction Juridique du Groupe Crédit Mutuel ARKEA et s'est notamment appuyée sur un cabinet d'avocats spécialisés dans le domaine des services de confiance.
 - La mise en place d'une veille juridique permet d'assurer les adaptations nécessaires des infrastructures et des processus fonctionnels.

Abréviations et Sigles :

AC	Autorité de Certification
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
DFL	La Direction des Flux
ETSI	European Telecommunications Standards Institute
KYC	En angl. « Know Your Customer » : Base de données client respectant les articles L 561-1 et suivants du Code Monétaire et Financier
LCP	Lightweight Certificate Policy : Certificat de sign. électronique non qualifiable.
OE	Opérateur d'Enregistrement
OID	Object Identifier (ou Identifiant universel)
PSAE	Prestataire de Service d'Archivage Électronique
PSCE	Politique de Service de Confiance électronique
QCP	Qualified Certificate Policy : Certificat qualifié de signature électronique

Glossaire :

Banque	Désigne l'entité du Groupe Crédit Mutuel ARKEA qui distribue en son nom des produits bancaires ou d'assurance.
eIDAS	Règlement européen n° 910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur adopté le 23 juillet 2014 par le Parlement européen et le Conseil de l'Union européenne
probant	Qui fait preuve devant un juge et est susceptible d'emporter son intime conviction.
protocole de consentement	Suite d'étapes faisant partie du tunnel de souscription et dédiées spécifiquement à la signature électronique du client final.
Service	Ce terme couvre indifféremment l'horodatage, la signature ou le cachet électronique délivré par la DFL
signataire ou client final	C'est la personne physique cliente ou mandataire de la Banque.

III – Identification de la PESGP

Identification de la Politique de Signature

La présente PESGP est identifiée par l'OID : 1.3.6.1.4.1.55871.1.170.1.

La présente PESGP est par ailleurs, signée électroniquement par la Banque. La date de la mise en œuvre de ce procédé autonome de signature électronique permet ainsi de justifier de la version de la PESGP en vigueur.

Le numéro d'OID, ainsi que la date de la version de la PESGP doivent obligatoirement figurer dans les actes signés.

Lors de toute communication ultérieure, l'OID et la date de signature seront utilisés pour référencer la présente

PESGP accompagné de l'empreinte de ce document et de la mention de l'algorithme utilisé pour produire cette empreinte.

Publication de la Politique de Signature

Avant toute publication, la présente PESGP devra être validée par le « Comité de validation » constitué de représentants des parties prenantes au processus de signature électronique :

- Federal Finance en tant que MOA de la signature électronique mise en œuvre par sa structure commerciale Arkéa Banque Privée ;
- La Maîtrise d'Ouvrage du Département Gestion Documentaire appartenant à la Direction des Flux au sein du Pôle Innovation et Opérations en tant que Maîtrise d'Ouvrage de la Plateforme de Signature Electronique.

En cas de modification substantielle de la PESGP, le « Comité de validation » sollicitera également les directions concernées du Crédit Mutuel ARKEA conformément aux normes du Groupe.

La présente Politique de signature est publiée par Federal Finance pour mise à disposition des utilisateurs de fonctions de signature ou de son service de validation de signature.

Ce document peut être distribué à ses utilisateurs finaux, soit par courrier électronique soit en le mettant en ligne.

Cette politique est publiée à l'adresse : <https://www.arkeabanqueprivée.fr/banque/assurance/federal-finance/infos-consommateurs>

Point de contact et prise en compte des remarques

Les demandes d'information ou questions concernant la présente politique sont à adresser par courriel au Service Relation Clients de Federal Finance par courriel à l'adresse suivante : contact@arkeabanqueprivée.fr

Les remarques et demandes d'évolutions formulées sont examinées par le « Comité de validation » qui engage si nécessaire le processus de mise à jour de la présente PESGP.

Une signature électronique est toujours valide, au regard de la PESGP qui s'appliquait au moment de sa création. Toutes les versions de la PESGP et leur durée respective de validité sont conservées par Federal Finance et accessible sur demande.

Méthode de gestion de cette politique

La présente PESGP est maintenue par Federal Finance en tant que MOA de la signature électronique mise en œuvre par Arkéa Banque Privée, et la Maîtrise d'Ouvrage du Département Gestion Documentaire appartenant à la Direction des Flux au sein du Pôle Innovation et Opérations en tant que Maîtrise d'Ouvrage de la Plateforme de Signature Electronique.

Circonstances rendant une mise à jour nécessaire

La mise à jour de la PESGP est un processus impliquant tous les acteurs. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, tenir compte des évolutions du cadre juridique ou réglementaire.

La présente PESGP est réexaminée lors de toute modification majeure de la Plateforme de Signature Electronique ou lors de toute évolution significative des processus de signature électronique.

Information des acteurs

Lorsqu'une mise à jour de la PESGP est décidée, les informations relatives à cette évolution sont mises en ligne à l'adresse de publication de la PESGP. Indépendamment de ce mode de communication, Federal Finance avise les principaux destinataires des Documents métiers signés, des modifications apportées à la présente PS par tous moyens à sa convenance, en fonction de la portée des modifications.

La publication d'une nouvelle version de la PESGP est réalisée sous la responsabilité de Federal Finance, après validation par le « Comité de validation », et consiste à archiver la version précédente et mettre en ligne à l'adresse prévue à cet effet le document au format PDF et l'OID du document.

Entrée en vigueur des nouvelles versions

La nouvelle version de la PS entre en vigueur dès sa publication à l'adresse identifiée au paragraphe « Publication de la Politique de Signature » ci-dessus. La nouvelle version reste valide jusqu'à la publication de la version suivante.

IV - Acteurs et Rôles

1. Client

Le Client désigne la personne, physique ou morale, qui réalise une transaction portant sur un (ou plusieurs) document(s) métier(s) qui lui est (sont) présenté(s) par la Banque sur un terminal d'affichage. Dans le cas d'une personne morale, elle est représentée par son représentant légal ou toute personne désignée avec la chaîne de pouvoirs adéquate et qui aura été portée à la connaissance de la Banque.

L'identité du Client doit être validée préalablement par la Banque en sa qualité d'Autorité d'Enregistrement. Pour ce faire, il sera invité à présenter, à minima, l'original d'un justificatif d'identité en cours de validité et déclarer, de bonne foi, toutes informations complémentaires permettant à l'AE de l'identifier avec certitude.

Dans certains cas le Client se verra remettre, à l'issue de l'enregistrement, un identifiant avec mot de passe sous forme de code ou de carte pour lui permettre de s'authentifier auprès des services de la Banque à distance.

Au cours de la transaction, le Client manifeste son consentement pour le (les) document(s) métier(s) en le(s) signant au moyen du Service suivant le protocole de consentement défini par la Banque sur le terminal d'affichage.

A l'issue de la transaction, le Client se voit remettre par la Banque un exemplaire du (des) documents(s) signé(s) sur un support durable conformément à l'article 1375 du Code Civil.

2. La Banque

La Banque propose à la souscription des produits bancaires ou d'assurance et élabore les documents métiers (contrats).

La Banque dispose d'un certificat de cachet (ou cachet serveur) pour signer, en tant que personne morale, le document métier. Ce procédé permet d'en assurer l'authenticité et l'intégrité ; il apporte aussi, de fait, l'approbation de la Banque quant à son contenu.

Le certificat de cachet est sous la responsabilité d'une personne physique ayant un lien contractuelle avec la Banque : c'est le responsable de certificat de cachet.

3. Autorité d'Enregistrement (« AE »)

La Banque porte la responsabilité des processus d'identification et d'authentification du Client : c'est l'Autorité d'Enregistrement.

Elle est responsable :

- De la définition d'une politique d'enregistrement, de signature et de gestion de la preuve et doit s'y conformer ;
- De l'enregistrement du Client, c'est-à-dire de procéder à son identification et son authentification préalablement à la signature électronique. Elle doit garder trace de cette étape dans sa base client (KYC),
- Et le cas échéant, de la délégation de l'enregistrement à une entité tierce à travers un lien hiérarchique ou contractuel (cf. « AED »).
- Du contrôle régulier et formalisé de l'accès aux applications métiers par les Opérateurs d'Enregistrement (« OE ») dans le cadre de sa procédure SSI ;
- De la formation et de l'information régulière de ces OE sur les procédures d'enregistrement ;
- De définir et délivrer les moyens d'identification et d'authentification au Client ;
- De la définition du protocole de consentement avec l'Autorité de Certification (Cf. « AC ») ;
- Le cas échéant, du recueil des documents Client complémentaires à la signature ;
- Du recueil du consentement du Client sur le document métier présenté pour signature à l'issue du protocole de consentement ;

Pour s'assurer de l'identité alléguée par le Client, l'AE s'appuie notamment sur la présentation d'un document officiel d'identité en cours de validité et en conserve une copie dans le dossier KYC du Client.

Pour la signature simple ou avancée, le recueil du consentement du Client se fait par l'AE par tout moyen qui lui semble approprié. Le protocole de consentement requière cependant au minimum les éléments suivants :

- En face à face : L'identification et l'authentification du Client par un opérateur d'enregistrement dûment habilité par l'entité au travers d'un lien hiérarchique ou contractuel ;
- A distance : L'authentification dynamique du client lors de la mise en œuvre du protocole de consentement par la saisie d'un code ANR (Authentification non rejouable).

4. Autorité d'Enregistrement Déléguée (« AED »)

L'Autorité d'Enregistrement Déléguée désigne l'entité légale extérieure à la Banque en charge d'identifier et d'authentifier le Client pour le compte de la Banque.

Cette mission lui est confiée dans un cadre contractuel explicite qui impose :

- De respecter la présente PESGP ;
- De permettre un audit régulier ou ponctuel des processus d'enregistrement et d'authentification des clients pour le compte de la Banque ;
- Le contrôle régulier et formalisé de l'accès aux applications métier par les Opérateurs d'Enregistrement dans le cadre de sa procédure SSI ;
- La formation et l'information régulière de ces OE sur les procédures d'enregistrement ;
- Le cas échéant, du recueil des documents Client complémentaires à la signature ;
- Le recueil du consentement du Client sur le document métier présenté pour signature à l'issue du protocole de consentement.

5. Opérateur d'Enregistrement (« OE »)

L'OE est une personne physique ayant un lien hiérarchique ou contractuel avec l'AE. Il applique les processus d'identification et d'authentification conformément à la Politique d'Enregistrement établie par l'AE.

Il doit être clairement identifié et régulièrement contrôlé.

6. Autorité de Certification et de Gestion de la Preuve (« ACGP »)

Dans le cadre de la présente PESGP, le rôle d'ACGP fait partie du service délivré par la DFL pour le compte de la Banque. La DFL agit sous sa responsabilité via un lien contractuel et conformément à sa Politique d'utilisation des Services de Confiance Électronique (« PSCE »).

L'ACGP assure la génération et la révocation des certificats à partir des demandes que lui envoie l'AE. L'ACGP assure la mise en œuvre de l'ensemble des opérations cryptographiques nécessaires à la création et la gestion du cycle de vie des certificats.

L'ACGP a en charge la création d'un fichier de preuve permettant d'attester de la signature électronique d'un document métier lors d'une transaction en ligne conclue entre la Banque et le Client, afin d'être en mesure de démontrer ultérieurement son existence, à partir d'une date et d'une heure certaines (contremarque de temps), son intégrité et la validation du document métier signé (conservation de l'original dans un fichier de preuve).

Le contrat de prestation en vigueur porté par la DFL s'appuie sur l'AC Docusign, Inc. faisant partie de la liste des Prestataires de Services de Confiance Électronique (PSCE) tenue au niveau nationale par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Le contrat de prestation inclus aussi le recours à un Prestataire de Service d'Archivage Électronique (PSAE) via CDC Arkhinéo. C'est une entité extérieure à la Banque. Elle est chargée de la conservation des éléments de preuve et met à la disposition de la Banque un coffre-fort électronique à cette fin, garantissant ainsi, en conformité avec les dispositions des articles 1366 et 1367 du Code Civil, leur pérennité et leur intégrité pendant la durée d'archivage définie par contrat. Le PSAE est certifiée NF 461.

V – Obligations des acteurs

1. Le signataire

1.1 Identification et authentification

Préalablement à l'utilisation du service de signature, le Client signataire est soumis aux obligations détaillées dans le §VI. *Identification et Authentification*.

1.2 Environnement de l'application de signature

Dans le cas d'une signature électronique réalisée en ligne sur le site de la Banque, l'environnement utilisé par le signataire doit lui permettre de se connecter à son espace client, de s'authentifier puis d'accéder au processus de signature. Le signataire s'engage à :

- ⇒ Assurer la confidentialité de ses données de connexion (identifiant, mot de passe) à la banque en ligne et à ne pas les communiquer à des tiers.
- ⇒ S'assurer de la sécurité du terminal d'affichage dont il se sert pour interagir avec le Service ;
- ⇒ Alerter la Banque en cas de problème constaté lors de la mise en œuvre du Service ;
- ⇒ Alerter la Banque en cas de perte, de vol ou de compromission des moyens d'identification qui lui ont été remis.

Le terminal d'affichage du signataire doit disposer d'un logiciel permettant l'affichage de documents au format PDF.

Dans le cas d'une signature électronique réalisée en agence, l'environnement utilisé par le signataire est un environnement mis à sa disposition par la Banque. Cet environnement est conforme aux règles de sécurité de la Banque et dispose d'une protection physique et technique de ses accès. Cet environnement permet l'affichage de documents au format PDF.

Dans tous les cas, aucun outil réalisant les opérations de signature ne doit être installé sur les terminaux, l'ensemble de ces opérations étant réalisé sur les infrastructures du tiers de confiance, prestataire de service de confiance électronique certifié.

1.3 Outils de signature utilisés

Le Client doit prendre connaissance du contenu des documents métiers qui lui sont présentés sur le terminal d'affichage au cours du protocole de consentement et avant d'apposer sa signature. A ce titre, il doit :

- Lire les documents présentés dans l'ordre de présentation
- Accepter les conditions générales d'utilisation du Service
- Accepter formellement l'opération de signature

Le processus de signature n'est modifiable ni par le Client ni par la Banque.

1.4 Type de certificat utilisé

Le Client met en œuvre un certificat éphémère pour réaliser l'opération de signature via l'AC « DocuSign Cloud Signing SII » référencée sous le code OID : 1.3.6.1.4.1.22234.2.14.3.33.

Les mesures de protection et de révocation du certificat sont détaillées dans cette politique publique.

2. La Banque

1.1 Obligations métiers

La Banque, en plus des obligations qui découle de son statut d'AE, est soumise aux obligations suivantes. Elle est responsable :

- De la conception et de la génération du document métier ainsi que de son format électronique ;
- De la mise en œuvre du service de signature électronique auprès de l'ACGP ;

Elle doit :

- Identifier et habilitier explicitement les salariés qui peuvent accéder à la base KYC ;
- Identifier les applications qui mettent en œuvre le Service ;
- Mettre à disposition du Client au moins un moyen simple de déclarer la perte, le vol ou la compromission de ses moyens d'authentification ;
- Mettre à disposition du Client une interface de consultation claire afin d'assurer la bonne lisibilité des documents métiers ;
- Permettre au Client une navigation aisée dans le protocole de consentement et lui permettre d'abandonner ce protocole à tout moment ;
- Restituer un exemplaire des documents métiers signés sur un support durable ;
- Garantir la sécurité informatique des données transmises par la Client ;

- S'assurer du respect de la législation en vigueur par ses différents prestataires et de leurs niveaux de conformité.

1.2 Type de certificat utilisé

La Banque met en œuvre un certificat de cachet d'une durée de validité de 3 ans via l'AC « KEYNECTIS ICS Advanced Class 3 CA » conformément à la Politique de certification de l'AC Docusign Inc. référencée sous le code OID : 1.3.6.1.4.1.22234.2.9.3.9.

Les mesures de gestion, de protection et de révocation du certificat sont détaillées dans cette politique publique.

VI – IDENTIFICATION ET AUTHENTIFICATION

1. Identités utilisées

Les identités qui sont utilisées dans le cadre de la signature électroniques sont les suivantes :

- Identité de la personne morale : Elle correspond au nom de la personne morale figurant sur un document officiel d'immatriculation (Extrait K-Bis, ...) et qui a vocation à engager sa responsabilité sur le contenu du document transactionnel. L'identification de cette entité morale se traduit par l'apposition, en son nom, d'un cachet serveur au sens eIDAS.
- Identité du client personne physique : Elle correspond au(x) nom(s) et prénom(s) figurant sur le document d'identité officiel en cours de validité présenté à l'AE ou à l'AED.

Il est à noter que, dans le cas où la transaction concerne deux personnes morales, seule la Banque apposera son cachet, la personne morale cliente devant être représentée par une (ou plusieurs) personne(s) physique(s) dûment mandatée(s) à cette effet.

2. Authentification, création, mise à jour de l'identité du Client

Le statut d'établissement financier propre à la Banque impose un contrôle l'identité lors de l'enregistrement du Client dans le dossier KYC qui soit conforme aux exigences des articles L. 561-1 et suivant du Code Monétaire et Financier relatif à la lutte anti-blanchiment dans les établissements financiers en France.

Cet enregistrement se déroule de plusieurs manières selon les cas.

Les processus détaillés ci-après ne reprennent que les étapes strictement nécessaires à la mise en œuvre de la signature électronique sans reprendre l'ensemble des actions exigées dans le cadre de la lutte anti-blanchiment et du financement du terrorisme ni les actions recommandées dans le cadre d'une approche commerciale.

Ce mode opératoire est tenu à jour dans le logiciel documentaire interne et accessible aux collaborateurs de Federal Finance.

- L'opérateur d'Enregistrement (OE) est obligatoirement sous contrat avec la Banque ;
- L'OE doit disposer des habilitations aux logiciels nécessaires à l'opération par délégation de son Directeur;
- Ces habilitations font l'objet d'une revue annuelle formalisée dans l'outil Ector et contrôlées par le service de Contrôle Périodique rattachée à la Direction de l'Inspection Générale.
- L'enregistrement se fait sur la base des documents collectés auprès du Client ;
- L'image de l'original de la pièce d'identité officielle en cours de validité est archivée dans l'outil (CNI, Passeport, Permis de conduire français de moins de 15 ans, carte de séjour française, carte de résident française) ;
- Un contrôle visuel est effectué par l'opérateur en cours d'entretien en particulier sur la validité du document ;
- Un contrôle automatique est réalisé, entre autre, sur la piste MZH et la cohérence entre les données extraites du document et les données déclaratives recueillies en cours d'entretien. Le résultat de ce contrôle est archivé dans le dossier KYC.
- Le numéro de téléphone portable est demandé au Client et renseigné dans la fiche KYC ainsi qu'un justificatif d'adresse de moins de 3 mois.

A l'issue de la création de l'identité du Client dans la base KYC, un code d'accès personnalisé et anonymisé à son espace internet privé est remis au Client au format papier accompagné d'un code de connexion à usage unique.

A la première connexion, il est du ressort du Client de créer un mot de passe suffisamment robuste en s'aidant des conseils de création affichés et de la jauge de couleur dynamique qui accompagne la zone de saisie. Le Client peut désormais s'identifier sur son espace personnalisé.

A tout moment, le Client peut déclarer la perte, le vol ou la compromission de ses identifiants de connexion et/ou de son numéro de téléphone portable en appelant « SOS Cartes/chéquiers (opposition, vol ...) » au 02.98.28.42.28 (depuis l'étranger : +33 2.98.28.42.28). Ces numéros sont disponibles sur le site public de la Banque, sur les automates en accès public 24h/24h ainsi que sur la documentation remise au Client lors de l'entrée en relation.

A tout moment, le Client peut demander l'envoi par courrier à l'adresse déclarée d'un nouveau code d'accès à usage unique afin de réinitialiser son indetification.

Le dossier KYC du Client fait l'objet de mise à jour régulière grâce à un contrôle automatique du logiciel KYC sur les dates de péremption des justificatifs d'identité en mémoire. L'OE est alors prévenu qu'une mise à jour est nécessaire via un rappel sur la fiche client. Le Client est prévenu par courrier où sur son espace internet qu'il doit procéder à la mise à jour de ce document.

VII – Signature et validation

1. Document métier

Le document métier présenté à la signature électronique contient toute information nécessaire à l'exécution du contrat par les parties.

Toutes les signatures d'un même contrat devront être électroniques. Si un des signataires souhaite signer sur support papier, la signature électronique est rendu définitivement impossible pour l'ensemble des parties prenantes au contrat elles devront toutes passer sur support papier.

Le document métier au format électronique est valable au sens de l'article 1365 du Code Civil.

Les parties sont engagées à l'issue du protocole de consentement et après acceptation.

Un exemplaire du document signé est remis au Client sur un support durable conformément à l'article 1375 du Code Civil.

2. Protocole de consentement

2.1 Identification

Le protocole de consentement fait suite à l'identification du Client sur le Service :

- Dans le cas d'une signature concomitante à la première identification, en face à face ou à distance, c'est l'OE qui procédera à cette identification après analyse des justificatifs présentés par le Client ;
- Dans le cas d'une signature postérieure à l'identification, c'est le Client lui-même en utilisant le code d'accès fourni par la Banque et son code secret.

2.2 Documents métier et documents Client

Le protocole de consentement consiste en une succession d'étapes de présentation au Client des documents métiers au format électronique afin d'en permettre la lecture. L'impression des documents présentée par le Client est possible à des fins d'archivage personnel mais n'aura en aucun cas de valeur probante. Seul le document électronique certifié possède une valeur probante.

Selon le produit souscrit et les options choisies préalablement à la signature, le protocole de consentement présenté au Client sera adapté par la Banque pour exclure les documents sans objet.

La Banque impose une signature de la part du Client sur les documents contractuels.

Dans certains cas, il sera demandé au Client de télécharger les images de certains documents en sa possession (le recto et le verso d'un justificatif d'identité en cours de validité, un justificatif d'adresse de

moins de 3 mois, un ou plusieurs bulletins de salaires, etc...). Ces documents ne seront pas tenus disponibles à la consultation par la suite afin d'éviter toute possibilité d'usurpation d'identité. Le service d'étude qui est en charge de vérifier la complétude du dossier Client se réserve le droit de renouveler une demande de téléchargement pour un document périmé, illisible ou litigieux.

Dans certains cas, il sera demandé au Client de compléter un questionnaire déclaratif en ligne.

La Banque conservera, au titre de preuve, l'ensemble des documents présentés au Client au cours du protocole de consentement même s'ils ne contiennent pas de signature ainsi que les documents téléchargés par le Client.

2.3 Navigation et action Client

Au cours du protocole de consentement, le Client sera invité à suivre les instructions de navigations jusqu'au terme du protocole. Sur chaque écran, l'abandon est possible et provoquera l'annulation des données saisies préalablement.

Certaines étapes, au cours du protocole de consentement, sont bloquantes.

- ⇒ Certaines pages comportent des contrôles de saisie ou des contrôles de complétude provoquant le blocage du protocole jusqu'à correction.
- ⇒ Il sera demandé au Client de reconnaître, en cliquant sur une case à cocher, certains éléments en fonction du produit souscrit, notamment :
 - Avoir pris connaissance de l'ensemble des documents précontractuels et contractuels qu'il s'apprête à signer, et les accepter sans réserve.
 - Que sa signature électronique emporte reconnaissance pleine et entière de sa part, de la validité des informations recueillies et stockées sous forme électronique qui pourront être utilisées par la Banque notamment en cas de litige et d'une valeur juridique de ces documents électroniques identique à celle d'un acte sous seing privé établi sur papier.
 - L'exactitude et la sincérité des renseignements communiqués dans le cadre de la présente souscription/adhésion.

L'action qui consiste à cocher la case débloque ainsi le processus de souscription en ouvrant l'accès au bouton de navigation suivant.

3. Signature Client

Une authentification dynamique est la dernière étape de la signature. Elle consiste à recueillir, selon les cas :

- La signature manuscrite du Client sur un écran tactile ;
- Un code à usage unique que le Client recevra sur le téléphone portable déclaré auprès de la Banque et qui devra être saisie dans la zone prévue à cet effet.

Le bouton demandant la signature du Client porte un libellé sans équivoque : « Signer » ou « Je signe ». Son activation finalise le processus de signature et manifeste le consentement du Client.

3.1 Normes de signature

La signature mise en œuvre est de type PDF enveloppées (aussi appelé « signature embarquée ») basée sur la norme PAdES (ETSI TS 102 778).

3.2 Algorithmes utilisables pour la signature

Algorithme d’empreinte (hash) : L’empreinte des données signées est effectuée avec l’algorithme SHA-256.

Algorithme de chiffrement : L’algorithme de chiffrement utilisé est RSA Encryption.

4. Validation

Un document métier signé est considéré comme valide lorsque l’ACGP retourne à la Banque l’accusé de réception attestant de la réalisation et de la validation de la signature électronique et de la constitution de la preuve conformément aux dispositions de sa Politique de Signature et de Gestion de Preuve.

VIII – Politique de confidentialité

1. Classification des informations

Les informations suivantes sont considérées comme confidentielles :

- Les données secrètes associées au certificat (clé privée),
- Les rapports d’audit sur la plateforme de signature électronique et sur les différents composants de l’infrastructure.

2. Communication des informations à un tiers

On entend par tiers, tout organisme n’étant pas dans la chaîne de traitement des informations. La diffusion d’information à un tiers ne peut intervenir qu’après acceptation de la Banque.

IX – Mise à disposition de l'exemplaire signé

Un exemplaire du document signé est remis à chaque signataire sur un support durable conformément à l'article 1375 du Code Civil.

La mise à disposition de l'exemplaire signé peut se faire au sein de l'espace sécurisé du Client accessible au moyen du code d'accès remis par la Banque et du mot de passe confidentiel défini par le Client ou par envoi en pièce jointe d'un e-mail sur sa messagerie personnelle.

Pour mémoire : L'impression papier d'un contrat électronique signé est sans valeur juridique.

L'exemplaire signé est conservé dans cet espace au moins 10 ans après l'échéance du contrat.

X – Conservation de la preuve

Les éléments de preuve conservés par le PSAE peuvent être sollicités à tout moment par une juridiction compétente soit au format électronique, soit au format papier après une opération de matérialisation mise en œuvre par le PSAE sur demande expresse auprès de la Banque.