Politique d'enregistrement, de signature électronique et de gestion de la preuve en vigueur au sein du Crédit Mutuel du Sud-Ouest

Avertissement

Ce document représente la Politique d’Enregistrement, de Signature et de Gestion de la Preuve du pôle Banque de Détail du groupe Crédit Mutuel Arkea conformément aux recommandations de la norme ETSI 102 041 v1.1.1.

La présente politique s’adresse aux destinataires des documents signés qui seront ainsi informés des conditions dans lesquelles les signataires ont été identifiés et authentifiés et la manière dont les signatures ont été recueillies et conservées.

Elle doit être portée à la connaissance du signataire afin de lui permettre de comprendre le sens de l’engagement pris en signant de cette manière.

Elle est utilement référencée via un N° OID (Object Identifier) dans les documents métiers précontractuels et contractuels.

I. CONTEXTE ET OBJECTIFS

Dans le cadre son activité commerciale, le Crédit Mutuel de Bretagne (CMB), désigné ci-après comme « 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 (« le Service ») 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 que la Banque met à disposition de ses clients sur son site web.

La présente politique 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 s'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 :

- Les Politiques de Certification de service de signature électronique :
  Pour Docusign : OID 1.3.6.1.4.1.22234.2.14.3.(33/41)
  (Pour Universign, le service de signature simple s'appuie en fait sur un simple cachet électronique Universign et non sur un service de signature au sens eIDAS.)

- Les Politiques d'horodatage certifiées qualifiées :

  Pour l'AC Docusign : OID 1.3.6.1.4.1.22234.2.6.5.8

  Pour l'AC UNIVERSIGN (SIGNATURIT GROUP) : OID 1.3.6.1.4.1.15819.5.2.(2/3)

- Les Politiques de certification de service de cachet électronique :

  Pour l'AC Docusign : OID 1.3.6.1.4.1.22234.2.14.3.37.

Il est certifié EN 319 411-1, niveau LCP.

Pour l'AC Universign (SIGNATURIT GROUP) : OID 1.3.6.1.4.1.15819.5.1.3.4

- La Politique d'archivage du PSAE Arkhinéo (OID : 1.3.6.1.4.1.29371.1.1.3.2)
- Les Conditions Générales de Banque

II. CHAMP D'APPLICATION

La présente politique couvre :

- La signature électronique avancée 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.
- 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 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 confiée.

Ce document vise à répondre à plusieurs contextes :

- 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 règlementaire :
    - Le processus de signature électronique mis en œuvre doit répondre à la réglementation découlant du règlement européen N°910/2014 du 23 juillet 2014 (dit « règlement eIDAS ») et aux exigences des articles 1366, 1367 et 1375 du Code Civil.
    - 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
DST	La Direction des Services Transverses
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 d'utilisation des Services 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 Direction des Services Transverses
Signataire ou client final	C'est la personne physique cliente ou mandataire de la Banque.

III. IDENTIFICATION DE LA PESGP

A. Identification de la Politique de Signature

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

B. Publication de la Politique de Signature

La présente PESGP est publié sur le site public de la banque

IV. ACTEURS ET RÔLES

A. client

Le client désigne la personne physique 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.

L'identité du client doit être vérifiée préalablement par la Banque en sa qualité d'Autorité d'Enregistrement.

Dans certains cas, le client se verra remettre, à l'issu de l'enregistrement, un identifiant et 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.

B. 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 du responsable de certificat de cachet (RCC) qui est une personne physique ayant un lien contractuel avec la Banque.

C. 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 au contrôle d'authenticité des justificatifs présentés, préalablement à la signature électronique. Elle doit garder trace de cette étape dans sa base client.
- Et le cas échéant, de la délégation de l'enregistrement à une entité tierce à travers un lien contractuel (cf. « D. 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 de gérer le cycle de vie des moyens d'identification du 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 ;

Le recueil du consentement du client se fait par l'AE par tout moyen qui lui semble approprié. Le protocole de consentement requiert 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).

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

L'Autorité d'Enregistrement Déléguée désigne l'entité légale extérieure à la Banque chargée 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 politique ;
- De permettre un audit régulier ou ponctuel des processus d'enregistrement et d'authentification des clients pour le compte de l'AE ;
- 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.

E. Opérateur d'Enregistrement (« OE »)

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

Il doit être clairement identifié.

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

Dans le cadre de la présente politique, le rôle d'ACGP fait partie du service délivré par la Direction des Service Transverses pour le compte de la Banque. La Direction des Service Transverses 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).

Les contrats de prestation en vigueur, porté par Arkea Solution Informatiques, s'appuient sur les AC Docusign, Inc. et Universign faisant partie de la liste des **P**restataires de **S**ervices de **C**onfiance **É**lectronique (**PSCE**) tenue au niveau nationale par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Le contrat de prestation inclut aussi le recours à un **P**restataire de **S**ervice d'**A**rchivage **É**lectronique (**PSAE**) via Arkhinéo. C'est une entité extérieure à la Banque. Elle est chargée de la conservation des éléments de preuve via un coffre-fort électronique 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 certifié NF 461.

V. OBLIGATIONS DES ACTEURS

A. Le signataire

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*.

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 soit (i) une tablette tactile mise à disposition par la Banque, soit (ii) son propre ordiphone.

Ces dispositifs sont conformes aux règles de sécurité de la Banque, ils permettent l'affichage des documents au format PDF.

Dans tous les cas, aucun outil supplémentaire réalisant des opérations de signature ne doit être installé sur les terminaux (clés USB, carte à puce), l'ensemble de ces opérations étant réalisé sur les infrastructures du tiers de confiance, prestataire de service de confiance électronique certifié.

3. Outils de signature utilisé

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.

4. Type de certificat utilisé

Le client met en œuvre un certificat éphémère (à la volée) pour réaliser l'opération de signature via l'ACGP. Les mesures de protection et de révocation du certificat sont détaillées dans la politique publique de l'AC mise en œuvre.

B. La Banque

1. Obligations métiers

La Banque, en plus des obligations qui découlent 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 habiliter explicitement les salariés qui peuvent accéder à la base connaissance client.

- 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.

2. Type de certificat utilisé

La Banque met en œuvre un certificat de cachet d'une durée de validité de 3 ans via l'ACGP.

Les mesures de protection et de révocation du certificat sont détaillées dans la politique publique de l'AC mise en œuvre.

VI. IDENTIFICATION ET AUTHENTIFICATION

A. Identités utilisées

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

- Identité de la personne morale : Elle correspond au nom ou à la raison sociale figurant sur un document officiel attestant de son enregistrement et qui a vocation à engager sa responsabilité sur le contenu du document transactionnel. L'identification de cette personne morale se traduit par l'apposition, en son nom, d'un cachet serveur au sens eIDAS.
- Identité de la 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 cet effet.

B. Authentification, création, mise à jour de l'identité du client

Le statut d'établissement financier propre à la Banque impose un contrôle d'identité lors de l'enregistrement des données client dans son dossier, 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.

Le mode opératoire est tenu à jour dans le logiciel documentaire interne et accessible à l'ensemble des salariés.

- 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 d'une personne habilitée;
- Ces habilitations font l'objet d'une revue annuelle contrôlée par le service de contrôle permanent rattachée à l'Inspection générale.
- L'enregistrement se fait en face à face par le conseiller ou depuis une interface en ligne à disposition du client ;
- L'enregistrement se fait sur la base des éléments recueillis auprès du client.
- Les images des pièces d'identité officielles sont archivées dans le système d'information.
- Un contrôle automatique est réalisé, entre autres, sur la piste MRZ[1] et la cohérence entre les données extraites du document et les données déclaratives recueillies. Le résultat de ce contrôle est archivé dans le dossier client.
- Le numéro de téléphone portable et/ou fixe est demandé au client et renseigné dans le dossier client.

S'agissant des clients Personne Morale (PM), les éléments recueillis portent sur :

1. L'identité et le statut juridique de la PM
2. L'identité du ou des représentants légaux
3. L'identité du ou des bénéficiaires effectifs
4. L'identité du ou des participants au contrat
5. La délégation de pouvoir des personnes habilitées

A l'issue de l'identification du client dans le système d'information, pour accéder à son espace de banque à distance, un identifiant personnalisé et anonymisé est transmis au client ainsi que ses codes de connexion.

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 les numéros 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.

[1] La MRZ, ou zone lisible par machine , est une zone particulière d'un document d'identité (passeport, carte d'identité ou permis de séjour en particulier) qui contient les données du titulaire du document.

A tout moment, le client peut demander un nouveau code d’accès à usage unique afin de réinitialiser son identification.

VII. SIGNATURE ET VALIDATION

A. 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 rendue 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.

B. Protocole de consentement

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 procède 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 son accès sécurisé préalablement fourni par la Banque .

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 présentés par le client est possible à des fins d'archivage personnel mais n'aura en aucun cas de valeur probatoire. Seul le document électronique certifié possède une valeur probatoire.

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 peut être demandé au client de télécharger les images de certains documents en sa possession Ces documents ne seront pas tenus disponibles à la consultation par la suite afin d'éviter toute possibilité d'usurpation d'identité. Dans certains cas, il peut être demandé au client de compléter un questionnaire déclaratif en ligne.

Les documents précontractuels et contractuels devront être téléchargés par le client afin de passer à l'étape suivante.

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.

3. Navigation et action client

Au cours du protocole de consentement, le client sera invité à suivre les instructions de navigation 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 :

    1. Avoir reçu et pris connaissance de l'ensemble des documents précontractuels et contractuels qu'il s'apprête à signer, les accepter sans réserve ni conditions et les avoir téléchargés et/ou imprimés pour pouvoir s'y reporter ultérieurement

2. 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.
3. 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.

Le déroulement des étapes du protocole de consentement est consigné dans le fichier de preuve qui permet également, a posteriori, de rejouer le protocole de consentement, c'est-à-dire de faire défiler les écrans vus par le client et de visualiser les documents précontractuels et contractuels consultés lors du processus de signature du contrat.

C. 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 un téléphone déclaré auprès de la Banque et qui devra être saisie dans la zone prévue à cet effet;
- Une identification biométrique;

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.

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).

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.

D. 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

B. 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.

C. 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.

D. Données à caractère personnel

Conformément à la politique de protection des données personnelles de la Banque, disponible sur les sites internet de chacune de ses entités, les données à caractère personnel utilisées pour la signature électronique sont traitées dans le respect de cette politique.

E. 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 envoie 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 selon les durées de conservation en vigueur après l’échéance du contrat.

F. 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.