Politique de signature

Service de signature avancée avec identification en face à face

V1.0 – Décembre 2020

IDEMIA

Introduction

Le présent document est la politique de signature du service de signature avancé avec certificat obtenu avec vérification d'identité en face-à-face mis en œuvre par IDEMIA. Lorsqu'une fonction de signature est mise à disposition d'utilisateurs, il est important que ces derniers aient connaissance du contexte dans lequel cette signature électronique est produite, des rôles, obligations que chaque acteur endosse, et des conditions dans lesquelles cette signature sera ultérieurement traitée, conservée et rendue disponible pour vérification.

L'objet de la présente politique de signature est justement de décrire :

- Les conditions dans lesquelles sont réalisées, traitées, conservées ces signatures électroniques
- Les conditions et contextes dans lesquels ces signatures électroniques seront ultérieurement consultables, utilisables et vérifiables.

Ce document est destiné aux :

- Signataires, pour leur permettre de comprendre la portée et le sens de l'engagement pris en signant
- Destinataires des documents signés, qui doivent non seulement s'assurer du sens de ces signatures, mais aussi d'avoir les moyens de s'assurer de leur validité (technique et juridique)
- Éventuels prestataires participant à ces échanges ; par exemple, les développeurs chargés de mettre en œuvre la vérification des signatures électroniques conformément aux exigences de la politique de signature.

L'historique de ce document est le suivant :

Numéro de version	Auteur	Commentaire
V1.0	PRO	Version initiale du document.

Table des matières

1 / Introduction

1.1 > Champ d’application

Conformément à l’article 1367 du Code Civil, une signature, qu’elle soit manuscrite ou électronique, « manifeste le consentement des parties aux obligations qui découlent de cet acte. (…) Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. (…) ».

La signature électronique permet donc :

- De garantir l’intégrité des données signées,
- D’identifier celui qui l’appose
- De manifester son consentement aux obligations qui découlent de cet acte de signature

Le présent document, Politique de signature de la plate-forme IDEMIA, s’applique aux transactions électroniques entre les partenaires de la société IDEMIA et les clients de ces derniers, signataires des documents. Le service de signature avancé d’IDEMIA permet aux signataires de réaliser une signature électronique à l’aide d’un certificat de signature électronique au sens du Règlement eIDAS, obtenu après vérification d’identité en face à face.

Le présent document, Politique de signature avancée avec identification en face-à-face, décrit les conditions dans lesquelles les documents contractuels émis par les partenaires d’IDEMIA à destination de leurs clients signataires sont produits et signés.

1.2 > Identification

La présente politique de signature est identifiée de manière non ambiguë par un OID qui identifie de façon unique le présent document ainsi que le processus qui lui est associé. La présente politique de signature est identifiée par l’OID : 1.3.6.1.4.1.54916.3.2.2.1.

2 / Gestion de la politique de signature

2.1 > Publication du document

La présente politique de signature est publiée à l'adresse suivante :

URL de publication :	https://pki.trust.idemia.io/sp/idemia-eidas-sp-advanced-ncp.pdf

2.2 > Processus de mise à jour

2.2.1 > Circonstance rendant une mise à jour nécessaire

La mise à jour d'une politique de signature est un processus impliquant tous les acteurs et faisant l'objet d'une démarche rigoureuse. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique ou combler des lacunes. La présente politique est réexaminée lors de toute modification majeure de l'application.

2.2.2 > Prise en compte des mises à jour

Avant toute publication officielle, la politique de signature est validée par le Comité d'Approbation d'IDEMIA. Ce comité est placé sous la responsabilité du responsable des services de confiance d'IDEMIA. Tous les remarques ou souhaits d'évolutions sur la présente politique sont à adresser au point de contact mentionné ci-après.

IDEMIA	
Personne à contacter	PKI Information contact
Adresse postale	IDEMIA 2 Place Samuel de Champlain 92400 Courbevoie
Numéro de téléphone	+33 1 78 14 70 00
Adresse électronique	info@idemia.com
Site internet:	http://pki.trust.idemia.io

Ces remarques et souhaits d'évolution sont examinés par le Comité d'Approbation, qui engage si nécessaire le processus de mise à jour de la présente politique de signature. Toutes les versions des politiques de signature et leurs durées respectives de validité sont conservées par IDEMIA et accessibles sur demande à l'adresse e-mail précédente.

2.2.3 > Information des acteurs pour donner suite à une mise à jour

Lorsqu'une mise à jour a été planifiée, les informations relatives à cette évolution sont mises en ligne sur les lieux de publication. Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du point de contact susmentionné pour obtenir plus d'informations.

La publication d'une nouvelle version de la politique de signature consiste à archiver la version précédente et mettre en ligne dans le répertoire prévu à cet effet (voir 2.1 >), les éléments suivants :

- Document au format PDF
- OID du document
- Date d'entrée en vigueur

Le document sera scellé électroniquement par IDEMIA à l'aide, a minima, d'un certificat de scellement avancé

2.2.4 > Entrée en vigueur de la nouvelle version et période de validité

Lorsqu’une nouvelle version de la politique de signature est mise en ligne, un message électronique est diffusé auprès de tous les utilisateurs inscrits pour les informer de la nature et de la date et heure du changement. La nouvelle version de la politique de signature entre en vigueur 15 jours ouvrés après sa mise en ligne et reste valide jusqu'à la publication d'une nouvelle version.

3 / Acteurs et rôles

3.1 > Listes des acteurs

Les différents acteurs impliqués dans le processus de signature sont :

- IDEMIA, qui opère le service de signature, ainsi que les différents services de confiance (A.C., A.H.) nécessaire au service de signature ;
- Le partenaire, client d'IDEMIA, qui prépare le document à signer et réalise les opérations d'enregistrement du signataire ; ce partenaire peut être l'émetteur du document à signer, mais également un intermédiaire entre l'émetteur du contrat et le signataire (dans le cas d'un courtier par exemple) ;
- Le signataire ;
- Le destinataire éventuel du document signé.

3.2 > Rôles et obligations des différents acteurs

3.2.1 > Rôle et obligations du signataire

→ Environnement de signature

L'environnement de signature est réalisé à distance, de ce fait, le signataire n'a besoin que d'un navigateur internet compatible pour accéder à l'application de signature.

Il est recommandé au signataire de prendre toutes les précautions nécessaires à la sécurisation de son poste de travail. Cet environnement de signature peut être son matériel personnel, mais il peut être également être mis à disposition du signataire par le partenaire ou un intermédiaire sous la responsabilité du partenaire.

→ Contrôle des documents signés

Le signataire doit contrôler, avant d'apposer sa signature, les données qui lui sont présentées.

→ Moyen d'authentification

Le signataire s'authentifie, avant signature, à l'aide d'un moyen d'authentification à double facteur. Ce moyen d'authentification peut être opéré :

- Soit directement par IDEMIA,
- Soit être partiellement (un facteur) ou totalement (deux facteurs) opéré par le partenaire d'IDEMIA avec des moyens d'authentification validés par IDEMIA.

Au cours de la session de signature, l'utilisation des deux facteurs pour l'authentification peut être conjointe ou bien décalée dans le temps. Par exemple, une authentification avec le premier facteur peut avoir lieu au début de l'ouverture de la session puis l'authentification avec le second facteur aura lieu au moment du déclenchement de la signature. En tout état de cause,

- Les deux authentifications doivent avoir lieu au sein de la même session, la fin d'une session nécessitant nécessairement une réauthentification.
- Au moins l'un des facteurs doit être vérifié immédiatement avant le déclenchement de la signature.

→ Type de certificat utilisé

Le certificat de signature est fourni par l'autorité de certification NCP+ IDEMIA. Il s'agit d'un certificat de signature avancée au sens du Règlement eIDAS conforme à la norme ETSI 319 411-1 pour le niveau NCP+. Au titre de l'émission du certificat, en tant que porteur de certificat, le signataire doit respecter les obligations qui lui incombent telles que définies dans la politique de certification de l'AC NCP+ IDEMIA. Le signataire ne peut utiliser un autre type de certificat dans le cadre de ce processus de signature.

3.2.2 > Rôle et obligations d'IDEMIA

→ Conformité entre le document signé et le document présenté au signataire

Dans le cadre du processus de signature, IDEMIA s'engage à ne réaliser aucune altération du document en dehors des strictes opérations nécessaires à la création de la signature électronique. En particulier, IDEMIA s'engage à ce que le document reçu du partenaire soit strictement identique au document présenté au signataire et strictement identique au document sur lequel sera réalisée l'opération d'apposition de signature.

→ Protection de la clé privée du signataire

IDEMIA s'engage à assurer la protection de la clé privée du signataire et à la maintenir sous son contrôle exclusif. Pour cela :

- La clé privée est créée et opérée dans un module sécurisé conforme à la norme EAL4+, dans un environnement sécurisé.

- La clé privée ne peut être utilisée pour la création de signatures électroniques qu'après authentification du signataire suite à la présentation du document à signer.

En cas de révocation du certificat associé, IDEMIA rendra inopérante la clé privée du signataire.

→ Horodatage

IDEMIA appose un horodatage qualifié de façon systématique sur chacune des signatures créées. La politique d'horodatage identifiée est, au choix du partenaire

- la politique d'horodatage qualifiée IDEMIA identifiée de façon unique par l'OID 1.3.6.1.4.1.54916.2.1.1.1.
- la politique d'horodatage non qualifiée IDEMIA identifiée de façon unique par l'OID 1.3.6.1.4.1.54916.2.1.2.1.

→ Vérification de la signature

La vérification de la signature créée n'est pas systématique dans le cadre de la présente politique. Elle est réalisée optionnellement à la demande du partenaire. Dans le cas de l'utilisation d'un format étendu de signature (voir 5.2 >), celle-ci est réalisée automatiquement.

→ Journalisation et création du fichier de preuve

IDEMIA s'engage à conserver les traces des différentes opérations et appels techniques du processus de signature et de les centraliser dans un fichier de preuve de la transaction. Ce fichier de preuve est scellé par IDEMIA pour en assurer l'intégrité.

IDEMIA s'engage à n'opérer aucune altération des traces inscrites dans le fichier de preuve.

Le fichier de preuve est décrit plus en détail dans la section 7 /

→ Archivage

L'archivage sous la responsabilité du partenaire, qui décide des moyens d'archivage et de préservation des signatures en fonction de son contexte métier et de la durée de conservation cible.

3.2.3 > Rôle et Obligation du partenaire

→ Préparation du document à signer

Le partenaire est en charge de la préparation du document à signer et de sa fourniture, via une interface informatique sécurisée, au service de signature IDEMIA. Le partenaire est responsable de la constitution, du format et du contenu du document.

→ Validation de l'identité du signataire

Le partenaire, en tant qu'autorité d'enregistrement déléguée d'IDEMIA, s'engage à réaliser les vérifications d'identité nécessaires à l'émission d'un certificat qualifié, telles que décrites dans la politique de certification. En particulier, un opérateur autorisé et formé du partenaire a rencontré le signataire lors d'un face-à-face physique durant lequel l'identité du signataire a été vérifiée vis-à-vis d'une pièce d'identité originale en cours de validité.

Le détail des engagements sur la validation initiale de l'identité est décrit dans la politique de certification.

→ Remise du document signé au signataire

En fin de processus de signature, IDEMIA remet au partenaire le document signé. Ce dernier est en charge de le mettre à disposition du signataire.

3.2.4 > Rôle et obligations des destinataires

Les destinataires doivent mettre en œuvre les moyens leur permettant de s'assurer de l'origine du document signé, de son intégrité et de l'identité de du signataire.

Pour se faire, les destinataires peuvent mettre en œuvre par eux-mêmes des moyens de vérification des signatures électroniques des informations reçues, en s'appuyant sur les informations fournies dans le présent document.

3.3 > Limitation de responsabilité d'IDEMIA

IDEMIA n'est pas responsable :

- Du contenu des informations signées
- D'une mauvaise utilisation des certificats, ou d'une inadéquation entre le certificat mis-en-œuvre et l'usage auquel il est destiné
- D'une mauvaise utilisation de la plate-forme de signature par le signataire.

Certaines données, notamment les listes de révocations, sont mises à jour quotidiennement et toutes les heures en cas de révocation. Par conséquent, il se peut qu'une signature soit déclarée valide si elle est réalisée entre le moment où la demande de révocation a été acceptée par IDEMIA et le moment où sa révocation a été publiée par l'autorité de certification et prise en compte par la plate-forme de validation. IDEMIA ne peut être alors tenue responsable de cet état de fait.

4 / Description de l'environnement de signature

4.1 > Caractéristiques techniques de l'environnement de signature

Les serveurs hébergeant la plate-forme de IDEMIA sont protégés selon les normes de sécurité en vigueur en conformité avec les recommandations de la norme ETSI 319 401. L'accès physique et technique à ces équipements et aux informations confidentielles qui s'y trouvent est contrôlé, par exemple : protection par pare-feu, installation des seuls logiciels utilisés pour effectuer les tâches du service, antivirus, mots de passe non partagés, mise à jour systématique des logiciels, ...

La clé privée du signataire est générée et protégée dans un module cryptographique de niveau CC EAL 4+.

4.2 > Données signées

Les données signées par le signataire sont des documents contractuels au format PDF soumis à sa signature par le partenaire d'IDEMIA.

Ces données sont présentées et acceptées par le signataire durant le processus de signature

Les documents PDF peuvent, antérieurement ou postérieurement à la signature, être scellés électroniquement, typiquement par le partenaire ou par un tiers autorisé par le partenaire, afin de garantir l'origine du document. Les documents pourront également être signés par un cocontractant.

En plus de l'empreinte du document, la signature technique peut contenir différents attributs de signature peuvent être ajoutés à la signature et feront partie des données signées :

Attribut de signature	Optionnel ou obligatoire	Signification et commentaires
SignedData.certificates	obligatoire	Certificat utilisé pour la signature (Certificat du signataire)

signature-policy-identifier	Optionnel	Identifiant unique de la présente politique de signature
Service: provide claimed time of signing	Obligatoire	Date présumée de signature. Il s'agit de la date de signature lue sur le serveur au moment où celle-ci est réalisée. Un horodatage qualifié est ensuite ajouté quelques instants plus tard.
Location	Optionnel	Champ optionnel indiquant le lieu présumé de signature tel que déclaré par le signataire (par exemple : à Paris)
Reason	Optionnel	Champ optionnel permettant d'indiquer des éléments d'engagements complémentaires à la signature (par exemple « lu et approuvé »)
ContactInfo	Optionnel	Champ optionnel permettant d'indiquer des éléments de contact complémentaires à la signature (par exemple l'adresse email ou le téléphone du signataire)

Les champs optionnels ne peuvent être ajoutés que s'ils ont été présentés au signataire.

4.3 > Processus de signature

Le processus de signature peut présenter, selon le partenaire, certaines variations, par exemple, sur le nombre de documents à signer ou la présentation préalable de documents précontractuels. Cependant, l'ensemble des processus obéissent au schéma global suivant :

1. Pré-authentification, le cas échéant avec un premier facteur (voir 3.2.1 >)
2. L'application métier du partenaire prépare une enveloppe de signature contenant :
    a. L'ensemble des documents à signer ou présenter pour approbation au signataire ;
    b. Les caractéristiques de l'enveloppe de signature (ordre de présentation des documents, contenu des messages d'approbation) ;
    c. Les caractéristiques du signataire.
3. La plate-forme de signature IDEMIA prépare le processus de signature en s'appuyant sur les éléments de l'enveloppe de signature (préparation des écrans de signature).
4. Lors de la connexion du signataire sur la plate-forme, les écrans lui sont présentés. En particulier, pour chaque document à signer, le document PDF est présenté tel qu'il

a été soumis par le partenaire (à l'exception d'éventuelles modifications techniques n'altérant pas le fond du document tel que l'ajout du champ de signature, la réalisation d'opérations techniques de mise en forme), et la plate-forme IDEMIA offre la possibilité au signataire de le consulter dans son intégralité.

5. L'application recueille alors explicitement le consentement du signataire par une action explicite et non -ambiguë (typiquement case à cocher d'approbation et clic sur un bouton « signer »). Le document est alors envoyé au service de signature.
6. Une authentification du signataire est alors réalisée par le service de signature selon la modalité définie en 3.2.1 >
7. Si l'authentification a réussi, le service de signature appose la signature électronique avancée du signataire à l'aide du certificat qualifié.
8. Le document signé est ensuite envoyé au service d'horodatage qualifié d'IDEMIA, qui appose un horodatage qualifié sur le document.
9. S'il existe plusieurs signataires, le processus est répété pour chacun des signataires
10. Une fois la transaction terminée, le ou les documents signés ou leurs hachés sont inclus, avec l'ensemble des traces de transaction, dans l'enveloppe de preuve. L'enveloppe de preuve est alors scellée par IDEMIA pour assurer son intégrité.

5 / Caractéristiques des signatures

5.1 > Type de signature

La signature électronique est intégrée au document signé (signature PDF).

5.2 > Norme de signature

L'ensemble des signatures créées sont conformes à la norme PAdES-T (Signature PDF).

Optionnellement, à la demande du partenaire, un format étendu de signature avancé pourra être utilisé, incluant les informations de révocation du certificat et la chaîne complète de celui-ci.

Conformément à la norme, les propriétés signées contiennent a minima les éléments suivants :

- Le certificat du signataire
- La date et l'heure de signature (celle-ci s'appuie sur l'heure du service de signature, synchronisé avec l'observatoire de Paris à intervalle régulier et au moins une fois toutes les 24h)
- Optionnellement, la référence au présent document et l'OID de la présente politique

Ces informations peuvent être complétées d'autres données signées. Voir section 4.2 > pour le détail des attributs de signature.

Le fichier signé est immédiatement horodaté et complété par l'usage du profil de signature PAdES-T, intégrant la signature électronique et un jeton d'horodatage qualifié au sens du Règlement eIDAS, permettant de déterminer la date et l'heure exacte de la signature.

5.3 > Certificat de signature

Le certificat de signature est un certificat de signature avancée au sens du Règlement eIDAS émis par l'AC NCP+ IDEMIA selon la politique de certification 1.3.6.1.4.1.54916.1.3.2.1.

5.4 > Date et heure de signature

La date et l'heure de signature sont antérieures à l'heure donnée par le jeton d'horodatage.

5.5 > Algorithme de signature

L'empreinte des données signées est effectuée avec l'algorithme SHA-256 ou un algorithme de robustesse équivalente ou supérieure. Le document est ensuite signé avec la clé RSA 2048 bits (ou une clé d'une robustesse équivalente ou supérieure) associée au certificat du signataire.

5.6 > Autres caractéristiques

Afin d'améliorer l'expérience utilisateur, un « visuel » de signature, matérialisant visuellement la signature du ou des signataires, peut optionnellement être ajouté au document PDF. Le contenu de ce visuel, laissé au choix du partenaire

- contient l'identité du signataire ;
- reprends des éléments les plus pertinents de la signature tels que la date et le fournisseur de la solution de signature (IDEMIA) ;
- peut inclure des éléments visuels tels qu'une capture de la signature manuscrite.

6 / Vérification de la signature

Cette section est le pendant de la partie précédente décrivant le processus et le format d'une signature électronique.

6.1 > Condition pour déclarer valide le fichier signé

La vérification consiste implicitement à vérifier qu'un document signé est conforme au format décrit, mais certains détails doivent être précisés ici, comme, par exemple, l'utilisation d'un service OCSP ou la liste des autorités d'horodatage reconnues.

6.2 > Procédure de vérification de signature

La vérification de la signature porte sur:

- La vérification du respect de la norme de signature, en particulier que la signature créée correspond bien au document signé.
- La vérification du certificat du signataire et de tous les certificats de la chaîne de certification (validité temporelle, statut, signature cryptographique).

6.2.1 > Vérification de l'empreinte du document et de la signature

Cette vérification permet de l'assurer que ni le document, ni la signature, ni le certificat du signataire n'ont été altérés durant le processus de signature. Cette étape consiste à :

- Recalculer le haché des données signées du document PDF et le comparer avec le haché contenu dans la signature. Deux hachés identiques signifient que le document n'a pas été altéré depuis l'apposition de la signature.
- Recalculer le haché des données signées et le vérifier avec la signature cryptographique elle-même à l'aide de la clé publique contenue dans le certificat du signataire. Cette opération permet de s'assurer que les données signées sont bien liées à la clé publique du signataire, et donc à son certificat.

Ces vérifications permettent de s'assurer que :

- Le document est intègre
- Que le document a bien été signé à l'aide de la clé privée du signataire.

La seconde étape de vérification consiste à s'assurer que le certificat du signataire n'était pas révoqué au moment de la création de la signature.

6.2.2 > Vérification de la chaîne de certificats

La vérification du statut des certificats est réalisée en s'appuyant sur les statuts émis par les autorités de certification concernées. La signature est valide vis-à-vis de cette politique de signature si, en plus des éléments de vérification de la section précédente, les éléments suivants sont établis :

- Le certificat de signature est intègre et a bien été émis par l'AC NCP+ d'IDEMIA selon l'OID 1.3.6.1.4.1.54916.1.3.2.1
- Le statut du certificat n'est pas révoqué à la date de signature donnée par l'horodatage.
- L'ensemble des certificats de la chaîne de certificats sont valides et non révoqués jusqu'à l'AC Racine IDEMIA
- L'ensemble des horodatages et des certificats de la chaîne d'horodatage sont valides et n'ont pas fait l'objet de révocation au moment de la date d'émission de l'horodatage.

7 / Création du fichier de preuve

IDEMIA garde des traces de chacune des étapes de la transaction de signature afin de constituer un fichier de preuve.

7.1 > Format et contenu du fichier de preuve

Le fichier de preuve est un dossier au format zip contenant :

- L'ensemble des éléments signés ou présentés et validés par les différents signataires (ou leur haché)
- L'ensemble des traces techniques de la transaction
- Un scellement horodaté de l'ensemble des fichiers de son contenu par IDEMIA permettant de garantir son origine et son intégrité

Le fichier de preuve s'appuie uniquement sur des formats ouverts et n'utilise aucune technologie propriétaire.

7.2 > Traces contenues dans le fichier de preuve

L'ensemble des traces de la transaction sont conservées dans le fichier de preuve sous forme de fichier XML. Les événements suivants sont tracés :

- Création de la transaction
- Ajout d'un document à l'enveloppe de preuve
- Génération de clé de signature et demande de certificat.
- Signature d'un document ou scellement d'un document
- Ajout d'un horodatage
- Validation d'une signature ou d'un scellement
- Calcul d'un affichage du document
- Accès d'un signataire à la plate-forme de signature
- Authentification d'un signataire
    - si l'authentification est prise en charge par IDEMIA, les traces sont automatiquement intégrées
    - si le partenaire d'IDEMIA réalise lui-même l'authentification, l'ajout des traces est réalisé par lui au moyen de l'interface IDEMIA mise à sa disposition et sous

sa responsabilité. IDEMIA est alors en charge de l’ajout des traces transmises dans le fichier de preuve.

- Acceptation d’un document par le signataire)
- Abandon ou fin de la transaction
- Erreur durant la transaction

Le partenaire peut, via l’interface mise à sa disposition par IDEMIA, ajouter tout type de document de son choix dans le fichier de preuve. Cet ajout de fichier se fait sous la responsabilité du partenaire, en particulier dans le respect du Règlement sur les données à caractère personnel.

7.3 > Scellement du fichier de preuve

Le scellement du fichier de preuve est réalisé à l’aide d’un certificat de cachet IDEMIA. La signature est au format XAdES détaché.

7.4 > Conservation du fichier de preuve

La durée et les conditions de conservation du fichier de preuve sont sous la responsabilité du partenaire. Celles-ci doivent être cohérentes avec la durée de conservation légale du document signé.

8 / Autres aspects

8.1 > Politique de confidentialité

8.1.1 > Informations considérées comme confidentielles

Les informations suivantes sont considérées comme confidentielles :

- Les données secrètes associées au certificat du signataire (clé privée, mot de passe, code d'authentification),
- Les journaux de l'application
- Les fichiers de preuves générés
- Les documents signés
- Les rapports d'audit sur cette application et sur les différents composants de l'infrastructure.

8.1.2 > Communication à des tiers

Les informations ne sont pas communiquées à des tiers.

8.2 > Dispositions juridiques

8.2.1 > Droit applicable

Le présent document est régi par la loi française.

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux de Nanterre.

8.2.2 > Propriété intellectuelle

Tous les logiciels participants à la constitution et à la validation des informations métiers signées sont mis à disposition des signataires par IDEMIA. Les signataires ne disposent d'aucun droit de propriété intellectuelle sur ces différents éléments.

8.2.3 > Données personnelles

Les processus de signature d’IDEMIA sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la Loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et du Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

www.idemia.com