Politique de signature

« Souscription dématérialisée à distance »

Date et l'heure: 23/12/2021 11:23:09

Définitions

Acte dématérialisé
Tout document proposé à l'Adhérent par voie dématérialisée tels que demande d'adhésion, document de gestion, fiche d'information précontractuelle, etc.

Adhérent
Personne physique manifestant son consentement à l'Acte dématérialisé auquel il souscrit en ligne via le Portail web GPMA.

GPM Assurances
Personne morale organisme assureur proposant une signature électronique à un Acte dématérialisé et assurant la garantie souscrite.
GPM Assurances - Société Anonyme régie par le Code des assurances au capital de 55 555 750 euros régie - RCS Paris n°412 887 606 – 1 Boulevard Pasteur – CS 32563 – 75724 PARIS Cedex 15

Authentification
Processus permettant de vérifier l'identité déclarée d'une personne ou de toute autre entité, ou de garantir l'origine de données reçues.

Autorité d'archivage
Autorité chargée de procéder à l'archivage des adhésions signées.

Autorité d'horodatage
Autorité chargée de procéder à l'horodatage.

Autorité de certification
Autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer des certificats.

Bi clé
Un bi clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques.

Certificat
Clé publique d'un utilisateur, concaténée à d'autres informations rendues infalsifiables par signature avec la clé privée de l'autorité de certification qui l'a délivré.

Certificat d'AC
Certificat d'une autorité de certification.

Comité d'Approbation
Le Comité d'Approbation est composé de la Direction Juridique, de la Direction Commerciale et de la Direction des Systèmes d'Information de GPMA.

Déclaration des pratiques de certification
Déclaration des pratiques mises en œuvre par une autorité de certification pour émettre et gérer des certificats.

Données d'activation
Données privées associées à un porteur permettant d'initialiser ses éléments secrets.

Hébergeur
Personne morale spécialisée dans les prestations d'hébergement

Infrastructure de gestion de Clés
Ensemble de composantes fournissant des services de gestion de Clés et de Certificats au profit d'une communauté d'utilisateurs. Etant précisé que la liste de Clés et des Certificats Révoqués contient des identifiants des Clés et des Certificats Révoqués ou Invalides

GIE GPS
Groupement d'intérêt économique dont GPM Assurances est membre, lui permettant d'accéder à des services support notamment informatique.

Plate-forme
La Plate-forme assure la transmission des informations d'identité nécessaires à la demande de Certificats vers l'Autorité de certification, la préparation des informations et la transmission du document PDF et la Signature électronique par GPM Assurances de l'Acte dématérialisé PDF signé électroniquement par l'Adhérent.

Politique de certification
Ensemble de règles relative à l'applicabilité d'un Certificat à une communauté et / ou à une classe d'applications ayant des besoins de sécurité communs.

Portail web GPM ASSURANCES
Site web de GPM Assurances permettant à l'Adhérent de souscrire en ligne à des Actes dématérialisés.

Signature électronique
Désigne tout moyen cryptographique utilisant un procédé fiable d'identification qui garantit son lien avec l'acte (article 1316-4 alinéa 2 du Code civil).
Il s'agit d'une clé sécurisée au moyen d'un dispositif de création de signature électronique (Décret n°2002-272 du 30 mars 2001, Article 1er).
La vérification de cette signature repose sur l'utilisation d'un certificat électronique (Décret du 30 mars 2001, Article 6). Cette certification de la signature est réalisée par un organisme ayant reçu un agrément ministériel (Décret du 30 mars 2001, Article 7).

Téléconseiller GPM ASSURANCES
Personne physique ayant pour fonction d'assister par téléphone l'Adhérent lors de la souscription à une garantie proposée par GPM Assurances, en saisissant les informations relatives aux Adhérents dans l'application de Souscription directe avant transmission à l'Adhérent pour signature.

1. Objet du document

GPM Assurances (GPMA) propose à ses Adhérents de dématérialiser le processus de souscription en leur permettant de remplir les formulaires d'adhésion et de recueillir leur consentement en ligne, via Internet avec, le cas échéant, possibilité de se faire assister par un téléconseiller

La souscription dématérialisée permet à l'Adhérent et à GPM Assurances de signer électroniquement des Actes dématérialisés. L'Adhérent est conscient et informé qu'il s'agit uniquement et seulement d'une demande de souscription. Le contrat étant conclu avec l'entrée en vigueur des garanties à la suite de l'accord de l'GPM Assurances et/ou de la transmission de documents nécessaires à la prise de garantie.

Le présent document a pour objet de décrire les conditions de création et de validation d'une Signature électronique dans le cadre des opérations de souscription et de gestion des Actes dématérialisés.

L'objet de ce document « Politique de Signature » est ainsi de décrire notamment :

- les conditions dans lesquelles sont réalisées, traitées, conservées ces Signatures électroniques ;
- les conditions et contexte dans lesquels ces Signatures électroniques seront ultérieurement consultables et vérifiables.

Ces Actes dématérialisés signés sont ensuite horodatés et conservés par GPMA. Ces Actes dématérialisés sont vérifiables et lisibles par les Adhérents sur des supports PDF.

Ce document est destiné aux :
- Adhérents afin d'assurer la transparence des opérations de signature des Actes dématérialisés ;
- éventuels destinataires ultérieurs de ces Actes dématérialisés, ayant besoin d'en connaître.

La présente Politique de Signature concerne les Adhérents (signataires d'Actes dématérialisés) et le dispositif de Signature électronique.

La structure de ce document est conforme aux documents normatifs suivants :
- *ETSI TR 102 041 V1.1.1 (2002-02) : Signature Policies Report*
- *RFC 3125 - Electronic Signature Policies*

Cette « Politique de Signature » est accessible sous format PDF.

2. Contexte

Dans la loi n°2000-230 du 13 mars 2000 paru au journal officiel du 14 mars 2000, l'écrit sous forme électronique est admis comme preuve au même titre que l'écrit sur support papier. Deux niveaux de validité juridique sont reconnus dans le décret 2001-272 du 30 mars 2001 permettant de distinguer la signature électronique dite « simple » et la signature électronique « présumée fiable ».
GPM Assurances a choisi d'appliquer une signature électronique dite « simple » en mettant en œuvre les meilleures pratiques s'approchant de la signature électronique « présumée fiable » en s'appuyant sur les éléments suivants :
- la mise en place d'un OTP transmis au Client par SMS avant la signature ;
- l'utilisation d'algorithmes de cryptographie conformes aux standards pour assurer l'intégrité des Actes dématérialisés ;
- l'utilisation d'une infrastructure sécurisée de gestions des Clés ;
- la mise en œuvre d'une infrastructure de gestion de preuve pour faire face à toute contestation éventuelle.

La Signature électronique reprend les deux fonctions de la signature manuscrite, à savoir l'authentification et l'expression du consentement de l'Adhérent. En outre, la Signature électronique permet également une identification fiable ainsi qu'un lien entre la Signature électronique et l'Acte dématérialisé sur lequel elle est apposée.

Cette Signature électronique est réalisée à partir d'un Certificat émis au nom de l'Adhérent, généré directement par l'Autorité de certification.

Pour créer une Signature électronique, l'Adhérent doit disposer d'un Certificat électronique qui l'identifie personnellement. Le Certificat électronique est délivré à travers une procédure sécurisée qui est décrite dans la politique de certification de l'AC.

3. Politique de Signature électronique

3.1. Champ d'application

La présente Politique de signature est applicable à l'Acte dématérialisé auquel l'Adhérent souscrit de manière dématérialisée, à distance. Les échanges électroniques sont réalisés par l'intermédiaire des Portails web GPM Assurances et d'une Plate-forme de Signature électronique.

3.2. Validation de la Politique de signature

Avant toute publication officielle, la Politique de signature est validée par le Comité d'Approbation.

3.3. Processus

Dans le cadre de la souscription dématérialisée, la présente Politique de signature est accessible préalablement à toute souscription, à l'adresse suivante :

http://www.gpm.fr/images/juridique/1.3.6.1.4.1.40706.1.2.v03GApdf

Dans le cadre de la souscription, une fiche d'information de la garantie d'assurance à laquelle l'Adhérent demande de souscrire est accessible préalablement à toute souscription.

L'Adhérent peut renoncer à la souscription à l'Acte dématérialisé si la présente Politique de signature ou la fiche d'information ne lui conviennent pas. De manière générale, l'Adhérent peut renoncer à tout moment au cours du déroulement du processus à adhérer.

La souscription de l'Adhérent s'effectue selon le formalisme suivant :

- l'Adhérent renseigne en ligne, sur le Portail web de souscription à distance de GPM Assurances, l'ensemble des informations nécessaires à l'établissement et à la gestion de son adhésion à l'Acte dématérialisé. Toutes les informations sont obligatoires.
  Il est impératif de suivre les instructions mentionnées à chaque étape de souscription sur le Portail web de souscription à distance de GPM Assurances, et notamment de renseigner tous les champs obligatoires et de valider les informations renseignées à chaque étape au moyen des boutons de validation prévus à cet effet.

- L'Adhérent peut également souscrire par téléphone en étant en contact direct avec un Téléconseiller qui va renseigner les informations nécessaires à l'établissement et à la gestion de l'adhésion de l'Adhérent à l'Acte dématérialisé en se connectant au Portail web de souscription directe de GPM Assurances. L'Adhérent recevra un courrier électronique à l'adresse qu'il aura communiqué au Téléconseiller. Ce courrier électronique contient un lien qui redirigera l'Adhérent vers la Plate-forme de souscription en ligne.

Tout au long du processus, l'Adhérent ou le Téléconseiller peut effectuer des corrections en revenant aux étapes antérieures ou renoncer à la souscription à l'Acte dématérialisé.

La souscription est établie d'après les déclarations de l'Adhérent. Toute fausse déclaration intentionnelle entraîne la nullité du contrat (article 113-8 du code des assurances).

Le cas échéant, l'Adhérent sera invité à transmettre les documents justificatifs par téléchargement sur le Portail web ou par voie postale.

- A l'issue de ces étapes de renseignement, l'Adhérent est invité à prendre connaissance de l'ensemble des documents (fiches d'information, conditions contractuelles, politique de signature) constituant l'Acte dématérialisé et à cocher la case confirmant qu'il en a bien pris connaissance. Cette étape est obligatoire. Il est possible pour l'Adhérent de télécharger ou d'imprimer ces documents.

- L'Adhérent est ensuite invité à prendre connaissance et à accepter la présente Politique de Signature électronique. Cette étape est obligatoire. L'Adhérent peut ensuite procéder à la signature de sa souscription :

    - L'Adhérent vérifie que toutes les informations renseignées dans les différents documents contractuels sont exactes, complètes et sincères ;
    - Il clique sur le bouton « valider» qui génère l'envoi d'un code par SMS

- L'Adhérent renseigne le code numérique reçu par SMS dans la zone prévue à cet effet sur la Plateforme de souscription en ligne :

    - L'adhérent clique sur le bouton « signer»

- La signature telle que décrite ci-dessus manifeste la volonté du Client ou du futur Client de contracter et déclenche la génération d'un Certificat par l'Autorité de certification au nom du Client ou du futur Client, qui est directement apposé sur l'Acte dématérialisé.

L'Adhérent est informé par GPM Assurances que la souscription a pris effet par l'envoi d'un courriel contenant notamment son bulletin d'adhésion sous la forme d'un fichier PDF. Ce fichier est scellé par l'intermédiaire des Signatures électroniques de l'Adhérent et de GPM Assurances, garantissant l'intégrité des documents ainsi produits, aux fins de conservation par ce dernier des documents contractuels par lesquels il est engagé.

- Une fois l'Acte dématérialisé signé l'Adhérent, celui-ci est signé par GPMA, horodaté et archivé.

Les certificats de signature sont visibles dans les documents signés ; l'Adhérent peut en prendre connaissance et vérifier l'identité des signataires et la validité des Certificats utilisés, en cliquant sur l'icône du Certificat et en déroulant chaque Certificat au moyen de la flèche devant chacun des Certificats.

En cas d'interruption dans le processus de signature, l'Adhérent doit reprendre le processus depuis sa première étape.

Si des inexactitudes ou erreurs ne sont pas identifiées (ex.: fautes d'orthographe, mauvaise saisie, etc.) et ne bloquent pas la souscription dématérialisée, elles pourront néanmoins être rectifiées ultérieurement auprès des Services de GPM Assurances-Prévoyance, par téléphone, fax ou e-mail.

3.4. Identification

La présente « Politique de signature - **Souscription dématérialisée à distance** » est identifiée, au sein du référentiel documentaire de GPM Assurances, par un numéro d'identification unique, l'OID :
1.3.6.1.4.1.40706.1.2v03GA

Les signatures respectant la présente Politique, la référenceront en utilisant ce numéro d'identification unique « OID », accompagné de l'empreinte de ce document et de la mention de l'algorithme utilisé pour produire cette empreinte.

3.5. Composition du Comité d'approbation

Le Comité d'Approbation est composé de la Direction Juridique, de la Direction Commerciale et de la Direction des Systèmes d'Information du GIE GPS. Ce dernier approuve la Politique de signature.

3.6. Processus de mise à jour

La mise à jour de la présente Politique de signature peut avoir pour origine, l'évolution du droit, la modification de l'état de l'art, l'apparition de nouveaux risques et de nouvelles mesures de sécurité ou des modifications dans le processus de signature.

La présente Politique est réexaminée périodiquement.

La validité d'une Signature électronique est appréciée conformément à la Politique de signature applicable au moment de ladite signature.

Toutes les versions des Politiques de signature et leur durée respective de validité sont donc conservées par GPM Assurances et accessibles sur demande.

Après mise à jour, la Politique de signature révisée est mise en ligne à l'adresse indiquée *supra*.

La publication d'une nouvelle version de la Politique de Signature consiste à archiver la version précédente et à mettre en ligne les éléments suivants :

- document au format PDF incluant,
    - l'OID associé,
    - son horodatage électronique,
    - la date et heure exacte d'entrée en vigueur.

3.7. Entrée en vigueur de la nouvelle version et période de validité

La nouvelle version de la Politique de signature entre en vigueur dès sa publication.

3.8. Cohérence de la documentation

Le Comité d'Approbation s'assure de la cohérence du référentiel documentaire dont fait partie la présente Politique de signature.

3.9. Convention de preuve

L'Adhérent reconnaît que l'architecture technique du processus de Signature électronique, notamment en termes de sécurité et de confidentialité, est suffisante pour garantir l'authenticité des documents échangés entre les parties ou créés via la souscription ainsi que l'intégrité de leur contenu.

En conséquence, la procédure de création, de contrôle et de transmission de tous documents est réputée fiable par les parties, qui renoncent par avance à contester ultérieurement un document qui aura été dûment créé, modifié, contrôlé, adressé par l'intermédiaire de la Plateforme en ligne au seul motif que la création, la modification, le contrôle et/ou la transmission auront eu lieu par voie électronique via la Plateforme en ligne.

Les registres informatisés conservés par le GIE GPS dans des conditions raisonnables de sécurité sont considérés comme intègres et fiables, valant ainsi preuve littérale entre les parties.

4. Acteurs et rôles

4.1. Les acteurs

Les acteurs concernés par le processus de création et de vérification de la signature électronique sont les suivants :

- l'Adhérent qui signe électroniquement les Actes dématérialisés ;
- l'Autorité Morale (GPM Assurances) qui signe électroniquement les Actes dématérialisés ;
- L'Autorité de certification, l'Autorité d'horodatage, l'Autorité d'archivage, l'Hébergeur qui sont des prestataires de confiance en charge des prestations de certifications, d'horodatage, d'archivage ainsi que de l'hébergement de la Plate-forme ;
- Eventuellement, le Téléconseiller GPM Assurances.

4.2. L'Adhérent

À l'occasion du processus de souscription dématérialisée, l'Adhérent transmet à AGMF une copie de l'un de ses documents d'identité ainsi que les autres documents justificatifs nécessaires à la souscription dématérialisée

Le rôle de l'Adhérent est de vérifier que les informations contenues sur le document à signer sont exactes avant de donner son consentement et de signer électroniquement le document depuis les sites web GPM Assurances.

A l'occasion de la souscription dématérialisée, l'Adhérent :

- respecte les règles de fonctionnement concernant les étapes de signature ;
- reste à proximité du terminal par lequel il signe électroniquement le document jusqu'à la fin du processus de souscription ;
- l'Adhérent s'engage à avoir au moment de la réalisation de sa souscription son téléphone portable sur lequel sera envoyé un SMS.

Les informations communiquées par l'Adhérent doivent être en cours de validité à la date de la souscription dématérialisée et ce dernier certifie leur exactitude.

4.3. L'Autorité Morale

4.3.1. Gestion du processus de signature électronique

Le GIE GPS est le développeur et l'opérateur technique du système informatique utilisé dans le cadre de la présente Politique.

Le GIE GPS et ses prestataires reconnus sur le marché hébergent et maintiennent le système informatique, conformément à l'état de l'art stable et actuel.

4.3.2. Sécurité du processus de Signature électronique

Le GIE GPS met en œuvre les moyens nécessaires, conformément à l'état de l'art stable et actuel, pour assurer la protection du processus de Signature électronique. Les mesures prises concernent :

- l'hébergement sécurisé des infrastructures (protection physique, protection logique, alimentation secourue, détection et protection incendie, etc.) ;
- la restriction des accès logiques aux équipements ;
- la protection réseaux en assurant une authentification forte et la confidentialité des échanges d'informations ;
- la sensibilisation et le suivi des procédures dans le processus de Signature électronique.

4.3.3. Journalisation

DOCAPOST assure une traçabilité et une conservation des traces relatives :

- aux différents échanges sur les réseaux et systèmes d'informations ;
- aux traitements des données échangés.

L'Autorité d'archivage s'assure que les éléments constituant la Signature électronique sont conservés pendant la durée prévue aux conditions contractuelles qui sont applicables à l'Acte dématérialisé auquel l'Adhérent a souscrit.

4.3.4. Type de certificat utilisé

GPM Assurances utilise un certificat délivré par l'Autorité de certification CERTINOMIS. Ce certificat est émis conformément à la politique de certification Cachet Serveur, R.G.S. 1 étoile (OID : 1.2.250.1.86.2.2.1.22.1).

4.3.5. Protection du support de Certificat

Le GIE GPS prend toutes mesures nécessaires pour protéger l'accès à son certificat et aux données secrètes associées, notamment le support qui lui a été remis (carte à puce, clé USB) et le code PIN associé.
Le GIE GPS se conforme à l'usage décrit dans « Conditions générales d'utilisation de CERTINOMIS». À ce titre, le certificat électronique est stocké sur un dispositif cryptographique qui doit être qualifié au minimum au niveau FIPS 140-2 Level 2 ou CWA 14169 (SSCD), et être conforme aux exigences du chapitre 12.1 de la politique de certification CERTINOMIS citée en 3.3.2.3 du présent document.
GPM Assurances s'engage à protéger l'accès à son certificat électronique, à ne pas communiquer son code PIN ou ses mots de passe associés, excepté pour ses préposés ayant besoin d'en connaître.

4.3.6. Révocation du Certificat

GPM Assurances s'engage à demander la révocation de son Certificat de signature en cas de perte, de vol, de compromission ou de simple suspicion de compromission de sa Clé privée et se conformer ainsi aux « Conditions générales d'utilisation des certificats » de l'Autorité de certification Certinomis.

4.3.7. Mise à jour des données utilisées

Certaines données, notamment les listes de révocations, ne peuvent être mises à jour en temps réel et il s'écoule plusieurs heures (24 heures au maximum) avant la publication de ces données par l'Autorité de certification.
Dans ces conditions, il se peut qu'une Signature électronique soit déclarée valide si elle est réalisée entre le moment où le Certificat a été révoqué et le moment où sa révocation a été publiée par l'Autorité de certification et prise en compte par GPMA.
GPM Assurances ne peut être alors tenue responsable de cet état de fait considérant cette « période de caution » inhérente à ce type de système.

4.3.8. Vérification de signature électronique

GPM Assurances effectue une vérification de la qualité de la Signature électronique préalablement à l'archivage de l'Acte dématérialisé auquel l'Adhérent a souscrit.

Pour la vérification des Signatures électroniques apposées sur les Actes dématérialisés, GPM Assurances utilise les données à sa disposition, notamment les données publiques relatives au Certificat de GPM Assurances, telles que les listes de révocations.

Les Actes dématérialisés signés font l'objet d'un horodatage permettant :

- de s'assurer de la traçabilité des informations de date et heure de signature de ces Actes dématérialisés;
- de déterminer la liste de révocation à utiliser pour valider la souscription dématérialisée.

L'arrêt de la validation empêche temporairement l'archivage électronique de l'Acte dématérialisé mais n'impacte en rien la validité de cet Acte, une fois horodaté.
GPM Assurances *s'assure de mettre en œuvre les procédures et dispositifs techniques permettant de lancer une nouvelle vérification de l'Acte dématérialisé lorsque ce service technique sera de nouveau disponible ; cette relance est automatique tant que le service est indisponible.*

4.3.9. Responsabilité

GPM Assurances ne pourra être tenue responsable des retards et conséquences dommageables dus à des événements qui ne lui sont pas attribuables ou qui résulteraient du fait de l'Adhérent, notamment en cas d'utilisation d'éléments inexacts ou incomplets mis à disposition par l'Adhérent.

GPM Assurances ne pourra être tenue responsable des retards et conséquences dommageables dus à des cas de force majeure.

La responsabilité de GPM Assurances ne peut être engagée au titre d'un dommage indirect.

La responsabilité totale de GPM Assurances, sur la base d'une faute dûment prouvée, est limitée au montant total H.T. des sommes versées par l'Adhérent au titre de l'Acte dématérialisé auquel il souscrit, toutes causes et tous sinistres confondus, et ce quel que soit le fondement juridique de la réclamation et la procédure employée pour la faire aboutir.

L'action en réparation devra être engagée dans l'année suivant la survenance de l'événement dommageable.

L'Adhérent s'oblige à prendre toutes mesures, dont notamment des sauvegardes, pour éviter qu'un dommage quelconque ne résulte pour lui d'une éventuelle atteinte aux fichiers, mémoires, documents ou tous autres éléments qu'il aurait pu confier dans le cadre de souscription dématérialisée.

GPM Assurances ne saurait être tenu d'indemniser l'Adhérent du fait de la destruction totale ou partielle de ses données ou fichiers qu'il appartient à l'Adhérent de sauvegarder.

4.3.10. Assistance aux Adhérents

Les Adhérents peuvent signaler tout dysfonctionnement à l'adresse suivante : souscriptiondirecte@gpm.fr

5. Signature électronique et vérification

La présente section a pour objet d'expliciter les processus de mise en œuvre des signatures électroniques qui sont apposées sur l'Acte dématérialisé, à savoir :

- La signature électronique de l'Adhérent qui correspond à une signature électronique dite « à la volée » ;
- La signature électronique de GPM Assurances qui correspond à une signature électronique autonome et qui est apposée.

5.1. Signature électronique de l'Adhérent

5.1.1. Caractéristiques du serveur de signature

Le serveur utilisé pour produire la Signature électronique de l'Adhérent est un serveur Windows hébergé chez le prestataire d'hébergement. Le serveur envoie une requête pour effectuer la Signature électronique mais la production de la signature est générée par Docapost.

5.1.2. Données signées par l'Adhérent

La Signature électronique de l'Adhérent est apposée sur l'Acte dématérialisé auquel il souscrit dans sa forme définitive, c'est-à-dire après production par le système d'information de GPM Assurances du document PDF exploitable par l'Adhérent et par les services internes de GPM Assurances.

5.1.3. Opération de signature

L'opération de Signature électronique de l'Adhérent est effectuée de façon automatique par le serveur GPM Assurances dès réception des Actes dématérialisés à signer.

GPM Assurances ne saurait s'engager sur des délais impératifs, notamment compte tenu du fait que la réception des Actes dématérialisés à signer est soumise aux réseaux de télécommunications.

5.2. Signature électronique de GPM Assurances

5.2.1. Caractéristiques du serveur de signature

Le serveur utilisé pour produire la signature électronique de l'Adhérent est un serveur hébergé chez Docapost. Le serveur du prestataire envoie une requête pour effectuer la signature électronique mais la production de la signature est générée par Docapost.

5.2.2. Acte dématérialisé signés par GPMA

La Signature électronique de GPM Assurances est apposée sur l'Acte dématérialisé auquel souscrit l'Adhérent dans sa forme définitive, c'est-à-dire après production par le système d'information du GIE GPS du document PDF exploitable par l'Adhérent et par les services internes de GPM Assurances.

5.2.3. Opération de signature

L'opération de signature électronique est effectuée de façon automatique par le serveur du GIE GPS dès réception des Actes dématérialisés à signer.

GPM ASSURANCES ne saurait s'engager sur des délais impératifs, notamment compte tenu du fait que la réception des Actes dématérialisés à signer est soumise aux réseaux de télécommunications.

5.2.4. Type de signature

Le cachet de certification est une signature cachet serveur au nom du Tiers de confiance DOCAPOST BPO et qui scelle le document
La signature minute est réalisée au nom du client final avec un certificat (autorité de certification AC4CONTRALIA) généré à la volée
Le cachet fournisseur est une signature cachet serveur pour le compte de l'organisme assureur

5.2.5. Norme de signature

Les signatures respectent la norme PAdES (ETSI TS 102778)

Conformément à cette norme, les propriétés signées (SignedProperties / SignedSignatureProperties) contiennent les éléments suivants :

- le certificat du signataire (Signing Certificate) ;
- l'identité du signataire
- la date et l'heure de signature (SigningTime) ;
- l'identifiant de l'émetteur (Issuer Serial) ;

Une fois signé :

- 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, permettant de déterminer la date et l'heure de la signature ;

- il ne fait ensuite plus l'objet d'aucun transcodage, et transite dans le système d'information du GIE GPS sous la forme d'un flux binaire, avant d'être stocké dans le SI du GIE GPS

5.2.6. Algorithmes utilisables pour la signature

- *Algorithme de condensation :* L'algorithme de condensation supporté est SHA-256.
- *Algorithme de chiffrement :* L'algorithme de chiffrement à utiliser est RSA Encryption.

- *Mise en forme canonique :* Sans objet.

5.2.7. Horodatage de la signature

Le jeton d'horodatage intégré au fichier signé est conforme à la norme RFC3161.
Il est produit par l'Autorité d'Horodatage DOCAPOST selon sa Politique d'horodatage identifiée par l'OID 1.2.250.1.229.1.3.

5.2.8. Conditions pour valider le fichier signé

Un fichier signé et horodaté est considéré comme valide par GPM Assurances à l'issue de la réception de l'acquittement produit par le Système d'information du GIE GPS utilisé pour conserver ces fichiers, garantissant ainsi que ces fichiers seront bien conservés de façon sécurisée et exploitables ultérieurement.

5.2.9. Vérification de la signature

À l'issue de l'opération de signature électronique, l'Adhérent est informé que GPM Assurances est en capacité de réaliser des opérations de vérifications de ces signatures électroniques.

La vérification de la signature électronique porte sur :

- la vérification du respect de la norme de signature ;
- la vérification de l'appartenance du certificat du signataire à la famille de certificat citée en 3.3.4 du présent document. ;
- la vérification du certificat de GPM Assurances et de tous les certificats de la chaîne de certification:
    - validité temporelle,
    - statut,
- la vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue ;
- la vérification du Certificat de GPM Assurances et de la signature électronique apposés sur le fichier

6. Contrôle de conformité

6.1. Objectif du contrôle

Le procédé de Signature électronique s'appuie sur un ensemble d'exigences et de règles de sécurité devant favoriser la confiance. GPM Assurances effectuera donc en ce sens des contrôles réguliers de conformité et de bon fonctionnement permettant de valider que la Signature électronique est conforme aux politiques de signature et de certification.

6.2. Fréquence du contrôle de conformité

GPM Assurances procède annuellement à un contrôle de conformité.

6.3. Choix du contrôleur

Le contrôle est effectué à la demande de GPM Assurances par une équipe d'auditeurs externes compétents en sécurité des systèmes d'information et indépendante.

6.4. Communication des résultats

Les résultats des audits de conformité contiennent des informations sensibles. Ils sont communiqués à un nombre restreint de personnes dans les entités concernés par l'audit en fonction des résultats.

6.5. Plan d'action

À l'issue d'un contrôle de conformité, les auditeurs externes rendent un avis et proposent un plan d'action afin de corriger le cas échéant les non-conformités détectées. Le plan d'action est communiqué aux seules personnes directement concernées.

7. Confidentialité

Les informations suivantes sont considérées comme confidentielles :

- les Clés privées associées aux Certificats ;
- le dossier de souscription de l'Adhérent;
- le dossier d'archivage de tous les éléments électroniques de l'Adhérent;
- les journaux d'évènements de la plate-forme de médiation de signature ;
- les procédures internes ;
- les rapports d'audits.

Les informations énumérées ci-dessus ne sont accessibles qu'aux personnes habilitées par GPM Assurances et ayant besoin d'en connaître.

8. Dispositions juridiques

8.1. Loi applicable

Le procédé de signature est soumis à la législation et la réglementation française en vigueur.

8.2. Réclamation - Médiation

Toute information complémentaire ou réponse à une réclamation concernant l'application de l'Acte dématérialisé auquel l'Adhérent a souscrit est fournie par le Département des Services Adhérents de GPM Assurances au siège social selon les modalités relatives à toute réclamation ou médiation décrites dans les conditions contractuelles applicables à l'Adhérent.

8.3. Attribution de compétence

Tout différend né de l'interprétation ou de l'exécution de la Politique de signature relèvera de la compétence expresse du Tribunal du ressort de la Cour d'appel de Paris, nonobstant pluralité de défendeurs ou appel en garantie, y compris pour les procédures d'urgence ou les procédures conservatoires, en référé ou par requête.

8.4. Propriété intellectuelle

Ni les Adhérents, ni les Conseillers GPM Assurances ne disposent des droits de propriété intellectuelle sur les éléments composant le service de signature, dont GPM Assurances est titulaire.

8.5. Droit de renonciation ou de rétractation

L'Adhérent dispose d'un droit de rétractation ou de renonciation. Ce droit de rétractation doit être exercé obligatoirement par lettre recommandée avec demande d'avis de réception selon les modalités relatives au droit de renonciation ou de rétractation décrites aux conditions contractuelles applicables à l'Adhérent.