MAROC ASSISTANCE INTERNATIONALE

GROUPE BANQUE POPULAIRE

Politique de signature électronique et gestion de preuve

1. CONTEXTE & OBJECTIF

Créée en 1976 et devenue l'une des filiales stratégiques du Groupe Banque Populaire en 1988, Maroc Assistance Internationale (M.A.I.) occupe une position de leader sur le marché de l'assistance au Maroc.

M.A.I. accompagne les Entreprises et les Particuliers depuis près de 40 ans, avec comme objectif premier d'apporter une assistance humaine, médicale, technique et juridique à plus de 3 millions d'assurés, que ce soit dans leur vie quotidienne ou lors de leurs déplacements partout dans le monde. Disposant d'un réseau de prestataires dense et membre d'IAG (International Assistance Groupe), M.A.I a pour mission essentielle d'accompagner le client dans toutes les situations de la vie, partout dans le monde et en temps réel pour résoudre des situations de crise, 24h/24 et 7j/7.

Les nouvelles technologies de l'information et les moyens de communication se diversifient et les utilisations des systèmes d'information aussi évoluent et s'enrichissent chaque jour, dans ce contexte, la contractualisation en ligne est devenue un enjeu stratégique pour M.A.I.

M.A.I. a lancé en juillet 2013, un nouveau site web intégrant une plateforme de « vente en ligne » des produits d'assistance voyage intitulés SCHENGEN VISA et INJAD MONDE. Le processus de la vente en ligne se résumait au paiement de la prime d'assistance via une carte bancaire. En revanche, la validité du contrat et la livraison de l'attestation d'assistance voyage restait conditionnées par la signature des Conditions Particulières par le Souscripteur auprès d'une agence Banque Populaire (Organisme agréé pour la présentation des produits d'assistance).

Aujourd'hui, M.A.I intègre le processus complet de la vente en ligne afin d'éviter le déplacement du client, tout en assurant la sécurité et la fiabilité de ses données. Ainsi elle met en place un système de signature électronique global offrant à sa clientèle la possibilité de signer en ligne son contrat, pour une dématérialisation complète de tous le processus de contractualisation en ligne. C'est le bureau direct qui assurera la fourniture à distance de ces opérations d'assurance.

Cette contractualisation en ligne est conforme aux dispositions légales en vigueur, notamment :

- La loi n°53-05 relative à l'échange électronique de données juridiques ;
- La loi n°09-08 relative à la protection des données personnelles ;
- La loi n°31-08 édictant des mesures de protection des consommateurs ;
- La loi n°17-99 portant Code des Assurances ;
- La loi n°43-05 relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme ;
- La Circulaire n°DAPS/EA/12/19 du 09 Mars 2012 relative à la fourniture à distance d'opérations d'assurances.
- La Circulaire n°DAPS/EA/11/16 du 04 juillet 2011 relative à l'application par le secteur des assurances des dispositions de la loi n°43-05 relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme.

Une signature électronique (SE), étant un procédé d'identification de l'auteur d'un document électronique, doit permettre de garantir l'authentification et la vérification de l'identité du signataire, le lien avec l'acte avec lequel elle s'attache et l'intégrité de l'acte. La signature électronique doit émaner d'un procédé fiable d'identification garantissant le lien avec l'acte avec lequel elle s'attache. Elle doit en outre satisfaire aux conditions suivantes:

- Etre propre au signataire ;
- Etre créé par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- Garantir avec l'acte auquel elle se rattache un lien, tel que toute modification ultérieure soit détectable ;
- Etre produite par un dispositif de création de SE attesté par un certificat de conformité, délivré par l'autorité nationale d'agrément et de surveillance de la certification électronique (Direction Générale de la Sécurité des Systèmes d'information) ;
- Veiller à l'existence d'un Certificat Electronique contenant notamment les données de vérification de la signature électronique.

Lorsque les fonctions de signature électronique sont mises à disposition des signataires, il est important qu'ils 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, disponible pour vérification.

2. POLITIQUE DE SIGNATURE ET GESTION DE PREUVE

2.1 Champ d'application

Une politique de signature électronique et gestion de preuve est un document décrivant les conditions de recevabilité d'un fichier sur lequel sont apposées une ou plusieurs signatures électroniques dans le cadre d'échanges électroniques prédéfinis.

La présente politique de signature et gestion de preuve, s'applique à la « Dématérialisation des contrats » sur la plateforme de « vente en ligne » des produits d'assistance voyage intitulés SCHENGEN VISA et INJAD MONDE de M.A.I., visant la signature des Conditions Particulières par les clients. La contractualisation se fait en ligne sur le portail de M.A.I..

Dans le cadre de cette « Dématérialisation des contrats », les acteurs qui ont la capacité de signer électroniquement ces contrats sont : les clients de M.A.I. ayant souscrit à un produit d'assistance et payé la prime y afférente et M.A.I., en sa qualité d'assureur (personne morale).

La signature électronique permet de répondre à plusieurs contextes :

- Contexte fonctionnel :
  - La signature électronique reprend deux fonctions de la signature sur support papier (authentification et consentement) et requiert une fonction supplémentaire: la fiabilité (procédé fiable d'identification garantissant le lien entre la signature électronique et l'acte auquel elle s'attache) ;
  - La signature électronique doit permettre d'apposer la signature du Client sur le contrat, dans le délai le plus bref après son consentement. Cette signature est réalisée à partir d'un certificat Client.
- Contexte règlementaire :
  - La solution doit s'inscrire dans le contexte réglementaire et juridique de l'IGC.
- Contexte économique :
  - La mise en œuvre de la signature électronique a pour objectif de réduire les coûts d'impression en multi-exemplaire des contrats ;
  - La mise en œuvre de la signature électronique au niveau de M.A.I. s'inscrit dans le projet global de l'Infrastructure de Confiance « Chaabi - eSign » du Groupe Banques Populaires.

La présente Politique de signature et gestion de preuve est portée à la connaissance du client lors du processus de signature électronique et avant l'opération de signature électronique. De cette façon, le signataire est en capacité de prendre connaissance de ces conditions de signature au moment de la réalisation de cette action. Respectivement, cette Politique de signature et gestion de preuve est mise à disposition des destinataires de la signature électronique, pour leur permettre de prendre connaissance des conditions dans lesquelles le signataire a produit la signature électronique.

2.2 Identification

La présente politique de signature et gestion de preuve est identifiée par l'OID 1.2.504.1.1.2.1.1.5.1

Cette référence, ainsi que le numéro de version de la Politique de signature et gestion de preuve utilisée, figure dans les données signées, afin d'attester du régime sous lequel le signataire adresse ses informations.

2.3 Publication du document

Avant toute publication officielle, la politique de signature et gestion de preuve est validée par M.A.I.

La présente Politique de signature et gestion de preuve est:

- Publiée au niveau du portail web de M.A.I., et accessible par le signataire avant la signature électronique ;
- Communiquée par mail au client ;
- Publiée sur l'URL : http://www.mai.co.ma/.

Les demandes d'information ou questions concernant la présente politique se font sur « Espace Réclamation» du portail M.A.I., ou à l'adresse suivante par courrier: 25, Boulevard RACHIDI Casablanca – Maroc.

2.4 Processus de mise à jour

2.4.1 Circonstances rendant une mise à jour nécessaire

La mise à jour d'une politique de signature et gestion de preuve 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, de nouvelles dispositions légales et réglementaires, ou combler des lacunes.

La présente politique est réexaminée lors de toute modification majeure de la plateforme de contractualisation en ligne de M.A.I.

2.4.2 Prise en compte des mises à jour

Ces remarques et demandes d'amélioration sont examinées par M.A.I., qui engage si nécessaire, le processus de mise à jour de la présente politique de signature et gestion de preuve.
Une signature électronique est toujours valide, au regard de la Politique de signature et gestion de preuve qui s'appliquait au moment de la signature électronique. Toutes les versions des Politiques de Signature et gestion de preuve, et leur durée respective de validité sont donc conservées par M.A.I., et accessibles sur demande.

2.4.3 Information des acteurs

Lorsqu'une mise à jour sera planifiée, les informations relatives à cette modification seront mises en ligne sur les lieux de publication. Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du comité d'approbation pour obtenir plus d'informations. La publication d'une nouvelle version de la politique de signature et gestion de preuve consiste à archiver la version précédente et mettre en ligne dans le répertoire prévu à cet effet, les éléments suivants :

- Document au format PDF
- OID du document
- Empreinte du document
- Algorithme de hachage utilisé (condensat SHA256 pour cette version)
- Date et heure exacte d'entrée en vigueur.
- Le document archivé porte, en filigrane sur ses pages, la mention « Document obsolète ».

2.5 Entrée en vigueur de la nouvelle version et période de validité

Lorsqu'une nouvelle version de la politique de signature et gestion de preuve est mise en ligne, un message électronique est diffusé sur le portail de M.A.I. sur l'url (http://www.mai.co.ma) accessible de tous les signataires pour les informer de la nature, de la date et de l'heure du changement.

La nouvelle version de la politique de signature et gestion de preuve entre en vigueur dès sa publication sur le site identifié à la section paragraphe 2.3. La nouvelle version reste valide jusqu'à la publication de la version suivante.

3. ACTEURS & RÔLES

3.1 Les acteurs

3.1.1 Signataires disposant du profil « Client »

Les signataires sont des personnes physiques. Il s'agit nécessairement de clients connus, ayant souscrit à un contrat d'assistance en ligne (SCHENGEN VISA ou INJAD MONDE). Le Client est assujetti à un moyen d'authentification forte, One time Password (OTP) qu'il reçoit par sms sur son GSM déclaré, qui permet de l'authentifier avant d'entamer le processus de signature.

Dans le cadre de ce processus de signature, les clients signent électroniquement des Conditions Particulières dans le cadre de la contractualisation avec M.A.I., reprenant les rôles et obligations contenues dans la présente politique.

3.1.2 Signataire Personne morale

Le GROUPE BANQUE POPULAIRE dispose d'une infrastructure de gestion à clé publique, ainsi chacun de ses établissements peut disposer d'un certificat cachet qui lui permet de signer, au nom de la personne morale que représente l'établissement.

Dans le cadre de cette contractualisation en ligne, M.A.I. dispose d'un certificat cachet pour signer les contrats en son nom avant de les soumettre aux clients.

L'application signature électronique est réalisée au niveau de GROUPE BANQUE POPULAIRE qui fait héberger et exploiter les services nécessaires à l'application auprès de l'équipe IGC de GROUPE BANQUE POPULAIRE.

L'équipe IGC est chargée d'administrer et d'exploiter l'IGC, la plate-forme de signature électronique, ainsi que le serveur d'horodatage permettant d'horodater les transactions à l'issue de leur signature, puis de valider et d'archiver ces informations signées.

3.1.3 Destinataires des contrats signés électroniquement

Les destinataires des contrats signés électroniquement sont :

- D'une part, les Clients eux-mêmes qui conservent ce document, dont la signature électronique matérialise leur consentement par rapport aux clauses du contrat ;
- M.A.I. qui apporte sa signature et cachet sur le document.

3.2 Rôles et obligations du client

3.2.1 Déroulement de la signature

Dans le processus de signature, le client doit vérifier que les informations contenues sur le document à signer sont exactes avant de donner son consentement et de le signer électroniquement à l'aide de son certificat personnel de signature généré par le système pour cette transaction.

Le client doit vérifier le détail de son ordre et son prix total et de corriger d'éventuelles erreurs, et ce avant de confirmer le dit ordre pour exprimer son acceptation.

3.2.2 Environnement du poste de travail

L'opération de création de la signature doit être réalisée sur le poste de travail du client et qui lui permet de de s'authentifier et de se connecter sur le portail de M.A.I.

3.2.3 Type de certificat utilisé

Dans le cadre de cette signature, la Bi-clé et le certificat associé du client sont générés à la volée et stockés dans un support cryptographique (HSM certifié EAL4+) et supprimés automatiquement à la fin de la transaction.

3.2.4 Outil de signature utilisé

Avec un certificat généré à la volée, le processus de signature ne dépend pas du poste client. Dans ce cas, aucun outil lié aux opérations de signature n'est à installer sur l'équipement informatique du client.

3.3 Rôles et obligations de MAROC ASSISTANCE INTERNATIONALE

3.3.1 Environnement de l'application de signature

L'application de signature pour la contractualisation en ligne au niveau du portail du M.A.I. utilisée par le client est l'élément sensible du processus de signature. L'application est installée dans des Datacenter du GROUPE BANQUE POPULAIRE.

En particulier, elle met en œuvre :

- La surveillance de l'accès physique et logique au système et de le protéger contre les intrusions ;
- Une limitation d'accès et d'administration de l'application signature à un minimum de personnes de confiance, ayant les compétences requises ;
- Le suivi des recommandations du fournisseur relatives à la sécurité du système.

3.3.2 Type de certificat utilisé

M.A.I., 1er signataire du document, dispose également d'un certificat de signature de type cachet serveur qui l'engage dans la signature en sa qualité d'assureur. Ce certificat est émis par une Autorité de Certification du GROUPE BANQUE POPULAIRE.

Dans le processus de signature, les contrats signés sont horodatés, ces certificats techniques d'horodatage sont émis par une Autorité de Certification du GROUPE BANQUE POPULAIRE.

3.3.3 Données de Vérification

Pour effectuer les vérifications, M.A.I. utilise les données présentes dans le système mis en œuvre, notamment :

- Les données publiques relatives aux certificats des signataires, telles que les listes de révocations ;
- Les habilitations des signataires à signer.

Le contrat signé fait l'objet d'un horodatage permettant :

- de s'assurer de la traçabilité des informations de date et heure de signature de ces transactions ;
- de déterminer la liste de révocation à utiliser pour valider cette transaction.

3.3.4 Protection du certificat Client

Le certificat « éphémère » de signature du client est généré dans le boitier cryptographique associé au serveur de signature. Aucun support n'est remis au client.

M.A.I. en s'appuyant sur l'IGC de GROUPE BANQUE POPULAIRE, au niveau de la plateforme de signature est en charge de :

- Générer une nouvelle bi-clé (clé publique et clé privée) pour créer le certificat client ;
- Protéger cette bi-clé dans le boitier cryptographique qualifié du serveur ;
- Réaliser les opérations de signature ;
- Détruire la bi-clé à la fin de l'opération du processus de signature.

M.A.I. autorise l'utilisation de certificats personnels référencés pour la signature d'un client. Le client est enrôlé par l'autorité d'enregistrement (Maroc Assistance Internationale) à l'autorité de certification.

La bi-clé est générée par une Autorité de Certification référencée et stockée dans un support matériel « qualifié ».

Le certificat est de courte durée, utilisé uniquement dans le cadre d'une seule transaction. Les opérations de signature sont effectuées sur l'équipement du client avec le certificat personnel « déclaré ».

Le serveur de signature consulte la liste de révocation émise par l'Autorité de certification qui a émis le certificat afin de s'assurer de sa validité.

3.3.5 Révocation du certificat

Le client a la possibilité de demander la révocation du certificat électronique utilisé pour signer auprès de M.A.I.

Il est à préciser que les certificats éphémères ayant une durée de validité de quelques minutes, le cas de révocation d'un tel certificat ne pourra être qu'extrêmement ponctuel.

En tout état de cause, l'Autorité de Certification qui a émis le certificat de signature assure un service de révocation et publie la Liste des Certificats Révoqués.

3.3.6 Protection des moyens

Le GROUPE BANQUE POPULAIRE, via l'équipe PKI, s'assure de la mise en œuvre des moyens nécessaires à la protection des équipements fournissant les services de signature et de validation.

Les mesures prises concernent à la fois :

- la protection des accès physiques et logiques aux équipements aux seules personnes habilitées ;
- la disponibilité du service ;
- la surveillance et le suivi du service.

3.3.7 Journalisation

M.A.I., via l'équipe IGC, s'assure de la conservation des traces relatives :

- à la circulation des échanges au sein des réseaux et des équipements informatiques ;
- au traitement des données échangées.

M.A.I. s'assure que les preuves de traitement relatives à la vérification des signatures électroniques sont conservées pendant toute la durée règlementaire.

3.3.8 Reprise en cas d'interruption de service

M.A.I., via l'équipe IGC, s'assure de la mise en œuvre des moyens nécessaires à la reprise d'activité en cas d'interruption de service d'un des composants nécessaire aux tâches dont elle a la responsabilité.

Elle s'assure en particulier que ces moyens font l'objet de tests à intervalles réguliers.

3.3.9 Assistance aux utilisateurs

Les clients peuvent s'adresser à M.A.I. pour toute information complémentaire ou pour signaler tout dysfonctionnement au niveau de l'espace réclamation.

3.3.10 Audit technique et juridique

Le GROUPE BANQUE POPULAIRE fait réaliser sur son infrastructure de confiance :

- Un audit technique pour s'assurer que les mises en œuvre techniques correspondent bien aux exigences prévues dans les documents de politique ;
- Un audit juridique pour s'assurer que les contextes règlementaires sont conformes.

4. SIGNATURE ÉLECTRONIQUE ET VALIDATION

4.1 Caractéristiques de l'équipement du signataire

Le poste de travail sur lequel est produite la signature est un ordinateur ou équipement adapté, fonctionnant dans un environnement sous le contrôle du signataire.

Les certificats utilisés pour la signature suite à une authentification forte (OTP) sont des certificats éphémères, valables le temps de l'opération de signature.

Ce certificat est produit par une Autorité de Certification du GROUPE BANQUE POPULAIRE.

4.2 Données signées

Au moment de la signature électronique, le Client signe électroniquement le document suivant :

- Les Conditions Particulières du contrat d'assistance, conformes au modèle homologué par l'ACAPS (ex : SCHENGEN VISA et INJAD MONDE).

4.3 Opération de signature électronique

Les fonctionnalités minimales suivantes sont assurées, pour permettre au Client d'avoir connaissance et conscience de l'action qu'il est sur le point d'effectuer :

Présentation du document à signer:

Le signataire a la possibilité de visualiser les informations du document que la plateforme de contractualisation en ligne lui propose de signer.

Présentation des attributs de la signature au signataire

La fonction de signature est intégrée au Portail de M.A.I. avec lequel le client signe le document. Les Conditions Générales d'Utilisation du Service de signature sont présentées au client et précisent notamment les conditions dans lesquelles sa signature électronique sera réalisée et traitée.

Interaction avec le signataire : consentement explicite et possibilité d'arrêt du processus de signature

Le client a les moyens d'exprimer explicitement (c'est-à-dire, de manière volontaire et non ambiguë) son consentement en confirmant sa volonté de signer les conditions particulières et déclencher le processus de signature du document sélectionné.

4.4 Caractéristiques des signatures

4.4.1 Type de signature

Les signatures électroniques apposées par les clients sont des signatures PDF

4.4.2 Norme de signature

La signature mise en œuvre est basée sur la norme PaDES.

4.5 Algorithmes utilisables pour la signature

4.5.1 Algorithme de condensation

L'algorithme de condensation utilisé est SHA-256.

4.5.2 Algorithme de chiffrement

L'algorithme de chiffrement utilisé est RSA Encryption

4.6 Conditions pour déclarer valide le contrat signé

Un contrat signé est considéré comme valide par M.A.I. lorsque les conditions suivantes sont remplies :

- Vérification positive de la signature électronique du signataire ;
- Vérification positive des droits du signataire en fonction des données transmises.

4.6.1 Vérification de la signature

La vérification de la signature porte sur :

- la vérification du respect de la norme de signature ;
- la vérification que le certificat du client est émis par l'AC du GROUPE BANQUE POPULAIRE dédiée à l'émission de certificats éphémère reconnue et acceptée par le GROUPE BANQUE POPULAIRE ;
- la vérification du certificat du Client et de tous les certificats de la chaîne de certification :
- la vérification de l'appartenance du certificat cachet M.A.I. à la famille de certificat émis par une des AC du GROUPE BANQUE POPULAIRE.
- la vérification du certificat Cachet et de tous les certificats de la chaîne de certification:
  - validité temporelle ;
  - statut ;
  - signature cryptographique.
- la vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue.
- la vérification de la signature électronique du client apposée sur le document en utilisant la clé publique du Client contenue dans le certificat transmis ;
- la vérification de la signature électronique Cachet apposée sur le document en utilisant la clé publique de la personne morale M.A.I. contenue dans le certificat transmis ;
- la vérification des données d'horodatage apposées sur la signature électronique du document;
- la vérification que les certificats utilisés au moment de la signature n'étaient pas dans une Liste de Certificats Révoqués. Cela concerne les certificats des Clients et également le certificat cachet mis en œuvre pour M.A.I. Cette vérification est basée sur la constitution d'une liste blanche lors de la génération ou la révocation d'un certificat de signature ;
- la vérification de l'identifiant de la politique de signature et gestion de preuve référencée.

4.6.2 Vérification des droits du signataire en fonction de données transmises

La vérification porte sur :

- l'identification du signataire à l'aide de son certificat ;
- la vérification des droits associés à ce certificat en fonction du type de données signées.

4.7 Gestion de la preuve

Pour conserver une trace de chaque transaction de signature, M.A.I., constitue une preuve électronique signée et horodatée, qui recense les éléments associés au processus de signature effectuée :

- Document original avant signature ;
- Document signé par l'ensemble des Parties (Client et M.A.I.) ;
- Certificat de signature utilisé par le client ;
- Certificat de signature cachet utilisé par M.A.I. ;
- Certificat cachet utilisé par l'établissement du GROUPE BANQUE POPULAIRE ;
- Numéro de téléphone GSM du client ;
- OTP envoyé au GSM du client par SMS ;
- Fichier de preuve signé et horodaté.

Cette preuve peut être exploitée ultérieurement en cas de litige pour restituer exactement les informations utilisées lors de la transaction.

5. POLITIQUE DE CONFIDENTIALITÉ ET RESPECT DES DISPOSITIONS DE LA LOI 09-08 RELATIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

5.1 Classification des informations

Les informations suivantes sont considérées comme confidentielles :

- les données secrètes associées au certificat (clé privée) ;
- les journaux de l'application « Dématérialisation des contrats » ;
- les procédures internes à l'équipe IGC permettant d'assurer la disponibilité de l'application « Dématérialisation des contrats » mise à disposition dans le portail de M.A.I. ;
- les rapports d'audit sur cette application et sur les différents composants de l'infrastructure ;
- Les données personnelles du client et des membres de sa famille bénéficiaires.

6. DISPOSITIONS JURIDIQUES

6.1 Droit applicable

Le présent document est régi par la loi marocaine.

6.2 Règlement des différents

Tout différend découlant du procédé de signature doit, en premier lieu, et dans toute la mesure du possible, être réglé au moyen de négociations amiables entre les parties.

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

6.3 Propriété intellectuelle de l'infrastructure de création et de validation des signatures

Les clients ne disposent d'aucun droit de propriété intellectuelle sur les logiciels participants à la constitution et à la validation du document signé. Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent, par quelque procédé que ce soit, est strictement interdite et constitue une contrefaçon sanctionnée par le Code de la propriété intellectuelle.

6.4 Données à caractère personnel

Les données personnelles demandées par M.A.I. ont un caractère obligatoire pour obtenir la souscription du présent contrat et l'exécution de l'ensemble des services qui y sont rattachés. Elles sont utilisées exclusivement à cette fin par les services de l'assureur et les tiers autorisés.

La durée de conservation de ces données est limitée à la durée du contrat d'assurance et à la période postérieure pendant laquelle leur conservation est nécessaire pour permettre à l'assureur de respecter ses obligations en fonction des délais de prescription ou en application d'autres dispositions légales.

Par ailleurs, la communication des informations du souscripteur assuré est limitée aux communications obligatoires en fonction des obligations légales et réglementaires qui s'imposent à l'assureur et aux tiers légalement autorisés à obtenir les dites informations. L'assureur garantit le respect de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

Les données sont protégées aussi bien sur support physique qu'électronique, de sorte que leur accès soit impossible à des tiers non autorisés. L'assureur s'assure que les personnes habilitées à traiter les données personnelles connaissent leurs obligations légales en matière de protection de ces données et s'y tiennent.

Les données à caractère personnel peuvent à tout moment faire l'objet d'un droit d'accès, de modification, de rectification et d'opposition auprès du Responsable du Département Production de M.A.I., mail : tp.prod@mai.cpm.ma, Tél : 522 457706/08, Fax : 522 204670.

De manière expresse, le souscripteur assuré autorise l'assureur à utiliser ses coordonnées à des fins de prospections commerciales en vue de proposer d'autres services d'assurance. Il peut s'opposer par courrier à la réception de sollicitations commerciales.

7. DEFINITIONS

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

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

Infrastructure de gestion de Clés (IGC)
Ensemble de composantes fournissant des services de gestion de clés et de certificats au profit d'une communauté d'utilisateurs.

Liste de Certificats Révoqués (LCR)
Liste contenant les identifiants des certificats révoqués ou invalides.

PAdES
PDF Advanced Electronic Signatures : Norme émise par l'ETSI (European Telecommunications Standards Institute) permettant de produire des signatures électroniques avancées pour le format PDF.

Politique de certification (PC)
Ensemble de règles relatives à l'applicabilité d'un certificat à une communauté et / ou à une classe d'applications ayant des besoins de sécurité communs.

Politique de signature et gestion de preuve
Document qui décrit les conditions dans lesquelles sont réalisées, traitées, conservées les signatures électroniques, les conditions et contextes dans lesquels ces signatures électroniques seront ultérieurement consultables, utilisables et vérifiables.

Politique d'horodatage
Ensemble de règles relative à l'émission de jetons d'horodatages.

Référentiel Général de Sécurité (RGS)
Le Référentiel Général de Sécurité (RGS) définit un ensemble de règles de sécurité qui s'imposent aux autorités administratives dans la sécurisation de leurs systèmes d'information. Il propose également des bonnes pratiques en matière de sécurité des systèmes d'information que les autorités administratives sont libres d'appliquer.

Signataire
Personne physique utilisant son ordinateur pour signer par voie électronique un document.
OTP
One time password (mot de passe à usage unique)
ETSI
European Telecommunications Standards
OID
Object Identifier
SHA-256
Secure Hash Algorithm (algorithme de hachage)
Empreinte du document
Condensat ou haché du document obtenu avec la fonction de hachage
IGC
Infrastructure de gestion de clés
Equipe IGC
L'équipe IGC est chargée d'administrer et d'exploiter l'IGC, la plate-forme de signature, ainsi que le serveur d'horodatage permettant d'horodater les transactions à l'issue de leur signature, puis de valider et d'archiver ces informations signées.
AC
Autorité de certification