Politique de signature électronique

OID : numéro (en cours d'acquisition)

Version 1.0

Société de conseil en assurance et finance

298 Boulevard Mohammed V, 20000 Casablanca Maroc.

FAX : 05 22 47 11 51

TEL : 05 22 47 47 26

MAIL : contact@voyageassur.ma

Évolutions du document

Date	Action	Auteur
07/10/2015	Initialisation du document V1.0	SafeDEMAT

Sommaire

1. INTRODUCTION

1.1. Présentation de l'offre

Dans une optique de sécurisation et de dématérialisation des services offerts à sa clientèle, la société de conseil en assurance et finance a mis en œuvre une offre de souscription en ligne d'assurances. Ces services ont était bâtit grâce à la solution eContract de SafeDEMAT qui comprend les services de confiance suivants : Un service de création de certificat, un service de signature, un service de traçabilité et un service d'horodatage.

La signature électronique vise à attester du consentement du ou des signataire(s) sur le contenu du document signé. En l'occurrence les conditions particulières du contrat d'assurance/assistance.

1.2. Objet du document

Le présent document constitue la **Politique de Signature** du service VOYAGEASSUR.

Une politique de signature est un document décrivant les règles à suivre pour créer des signatures électroniques dans le cadre d'échanges électroniques prédéfinis, d'en le but d'en assurer la fiabilité, l'intégrité des données transmises et l'authenticité de leur émetteur.

Elle est composée d'un ensemble de règles et de dispositions définissant les exigences auxquelles chacun des acteurs impliqués se conforme et qui régit la création des signatures électroniques.

Le présent document, décrit ces conditions dans le cadre des échanges électroniques entre les clientes (souscripteurs) et VOYAGEASSUR.

Il expose le contexte dans lequel les usagers de VOYAGEASSUR prennent des engagements sur le contenu des contrats souscrits à l'aide de signatures électroniques, ainsi que le mode de réalisation et de vérification de ces signatures.

Ce document décrit notamment les conditions auxquelles les certificats, les signatures électroniques et les contremarques de temps seront considérés comme fiables par les services de signatures précédemment cités, ainsi que les obligations et responsabilités de chacun des intervenants.

La présente Politique de signature fait partie intégrante des termes des Conditions d'utilisation des services offerts par la plate-forme VOYAGEASSUR.

La signature électronique apposée sur un ensemble de données permet de garantir :

- l'identité du signataire,
- l'intégrité du document signé,
- le lien entre le document signé et la signature.

La signature électronique traduit ainsi la manifestation du consentement du signataire quant au contenu des données signées.

Lorsque des fonctions de signature électronique sont mises à disposition d'une population ou d'une entité, il est important que celle-ci ait 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 d'une « politique de signature » (P.S.) 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.

1.3. Définitions et acronymes

1.3.1. Définitions

Application utilisatrice - Processus automatique (« applicatif ») ayant suivi le processus de souscription au service de l'Autorité de Validation de Signature

Authentification - Vérification de l'identité d'une personne ou d'une application. L'authentification est l'un des services rendus par une IGC grâce à l'utilisation conjointe d'un certificat et de la clé privée associée : un porteur peut s'authentifier par exemple pour accéder à la plate-forme d'une application

Autorité d'Archivage (AA) - Autorité responsable de l'archivage et la conservation dans le temps de données au format électronique afin d'en assurer la pérennité en matière d'enregistrement, de stockage et de restitution, selon les modalités définies dans une Politique d'Archivage.

Autorité de Certification (AC) - Autorité responsable de l'émission et la gestion des certificats électroniques. Elle correspond à l'entité organisationnelle et technique qui reçoit les demandes de certificats, génère les certificats et les signe avec sa clé privée, selon les modalités définies dans une Politique de Certification.

Autorité d'Horodatage (AH) - Autorité responsable de la gestion de l'environnement d'horodatage et de la production des jetons d'horodatage sur les données qui lui sont présentées afin d'attester de l'existence de ces données à la date de la contremarque de temps, selon les modalités définies dans une Politique d'Horodatage.

Autorité de Signature (AS) - Autorité en charge de la signature électronique des documents qui lui sont présentées. Elle vérifie notamment la validité du certificat utilisé pour la signature et génère la signature numérique selon les modalités définies dans une Politique de Signature. La composante technique de l'Autorité de Signature est nommée Plate-forme de Signature (PFS).

Bi-clés - Couple de clés cryptographiques, composé d'une clé privée (devant être conservée secrète) et d'une clé publique (largement diffusée par le biais du certificat électronique). Ce couple de clés permet, par le biais de divers mécanismes, de rendre des services de sécurité comme la non-répudiation, l'authentification, la confidentialité et l'intégrité.

Certificat électronique - Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement

ou indirectement (pseudonyme), et mentionné dans le certificat. Il est géré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé.

Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Chaîne de confiance (chemin de certification) - Ensemble ordonné des certificats nécessaires pour vérifier la filiation d'un certificat donné.

Compromission - Une clé privée est dite compromise lorsqu'elle est potentiellement utilisable ou a été utilisée par une personne autre que celle habilitée à la mettre en œuvre.

Contremarque de temps - Données qui lient une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant que la donnée existait à cet instant là.

Infrastructure de Gestion de Clés (IGC) - Ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique.

Liste d'Autorités Révoquées (LAR ou ARL) - Liste des certificats d'Autorités ayant fait l'objet d'une révocation.

Liste de Certificats Révoqués (LCR ou CRL) - Liste de numéros de certificats ayant fait l'objet d'une révocation.

Object IDentifier (OID) - Identifiant alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.

Plate-forme de Signature - Ensemble des composants matériels et logiciels qui servent à assurer le fonctionnement de l'Autorité de Signature.

Politique de Certification (PC) - Ensemble de règles définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses

prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Politique d'Horodatage (PH) - Ensemble de règles définissant les exigences auxquelles une AH se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'une contremarque de temps à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PH peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les abonnés et les utilisateurs de contremarques de temps.

Politique de Signature (PS) - Ensemble de règles définissant les exigences auxquelles une AS se conforme dans la mise en place et la fourniture de ses prestations et qui régit la signature de document et/ou d'un élément de preuve à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PS peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les abonnés et les utilisateurs des services de signature.

Porteur (de certificat) - Personne physique titulaire d'un certificat. On peut distinguer le porteur de certificat (certificate holder) du propriétaire du certificat (certificate owner) : le porteur utilisera le certificat en qualité de représentant du propriétaire du certificat.

Prestataire de services de certification électronique (PSCE) - Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles).

Données d'Activation : données connues du Porteur de Certificat uniquement lui permettant de mettre en oeuvre sa clef privée.

Génération d'un Certificat : action réalisée par une Autorité de Certification et qui consiste à signer le gabarit d'un Certificat édité par une Autorité d'Enregistrement.

Identité : ensemble des informations définissant un individu (nom, prénom(s)…) ou une entité (dénomination sociale, SIRET…).

Opérateur de Certification (OC) : entité chargée d'exploiter techniquement l'ICP pour le compte de l'Autorité de Certification.

Produit de sécurité - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en oeuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée ou immatérielle (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Propriétaire (de certificat) - Personne, morale ou physique, qui a souscrit un certificat électronique auprès d'une Autorité de Certification

Révocation (d'un certificat) - Opération de mise en opposition effectuée à la demande du porteur ou de toute autre personne autorisée, qui entraîne la suppression des garanties apportées par l'Autorité de Certification sur un certificat donné avant la fin de sa période de validité. Les conditions de mise en oeuvre de la révocation sont définies dans la Politique de Certification de l'Autorité de Certification concernée.

Signature numérique - Cryptogramme issu du chiffrement d'une empreinte de données à la société de conseil en assurance et finance d'une clé privée, cette empreinte étant obtenue par application d'une fonction de « hachage » (algorithme de codage irréversible) sur lesdites données. Le terme signature numérique désigne indifféremment le cryptogramme et le mécanisme permettant de l'obtenir. Une signature numérique peut accompagner les données qui ont été signées et en

garantir l'intégrité et l'engagement du titulaire de certificat. Le mécanisme de signature numérique peut également être utilisé pour authentifier dynamiquement un titulaire de certificat.

Titulaire de certificat - Sujet qui s'est vu délivrer un certificat par une Autorité de Certification. Lorsque le titulaire est une personne physique, cette dernière est appelée « porteur ».

Vérification de validité (d'un certificat) - Opération de contrôle du statut d'un certificat (ou d'une chaîne de certification). Un certificat référencé peut être dans l'un des trois états suivants : valide, expiré ou révoqué.

1.3.2. Acronymes

Les acronymes utilisés dans le présent document sont les suivants :

Sigle	Description
AC	Autorité de Certification
AH	Autorité d'Horodatage
AS	Autorité de Signature
CN	Common Name
CRL	Certificate Revocation List, ou LCR
DN	Distinguished Name
FQDN	Fully Qualified Domain Name
LCR	Certificate Revocation List Liste de certificats révoqués
OID	Object Identifier
PS	Politique de Signature
TSP	Time Stamp Protocol.
PDF	Portable Document Format
IGC	Dans le contexte de ce document, synonyme français de l'anglais PKI qui signifie « Public Key Infrastructure ».

2. POLITIQUE DE SIGNATURE ELECTRONIQUE

2.1. Identification du document

La présente Politique de signature est identifiée par l'OID (Object IDentifier) suivant : numéro en cours d'acquisition.

2.2. Domaine d'application

Les signatures électroniques réalisées par les services de signature électronique de eContract ne portent que sur des documents générés ou échangés via le service VOYAGEASSUR.

la société de conseil en assurance et finance ne saurait endosser aucune responsabilité relativement à des documents non générés, non signés ou non conservés dans le cadre des services dématérialisés de VOYAGEASSUR.

la société de conseil en assurance et finance ne saurait endosser aucune responsabilité dans les cas où un ou des documents provenant du service VOYAGEASSUR seraient employés à titre de preuve dans un contexte différent.

2.3. Publication du document

Dans le processus de signature, l'application de signature rappelle la politique en vigueur au signataire, préalablement à son engagement (ou une référence à celle-ci).

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

http://www.VOYAGEASSUR.com/ps.pdf (à mettre à jour avec le bon emplacement)

2.4. Processus de mise à jour du document

La Politique de signature est maintenue à jour par la société de conseil en assurance et finance

2.4.1. Circonstances rendant une mise à jour nécessaire

La mise à jour de la présente Politique de signature peut avoir pour origine :

- l'évolution du droit,
- le besoin de s'adapter aux évolutions technologiques,
- la mise à jour de la liste des certificats concernés par la présente politique de signature,
- les observations des différents acteurs.

La périodicité minimale de révision de la présente politique de signature est fixée à 2 ans

2.4.2. Prise en compte des remarques

Toutes les remarques concernant la présente Politique de signature sont à adresser par courriel à l'adresse : contact@voyageassur.ma

Ces remarques seront examinées par la société de conseil en assurance et finance qui engagera, si nécessaire, le processus de révision de la présente Politique de signature.

3. SERVICE DE SIGNATURE INTEGRE A LA PLATFORME ECONTRACT

Ce chapitre de la politique de signature entre dans les détails techniques de sa création et de sa vérification.

3.1. Certificats de signature utilisés

Les usagers du service VOYAGEASSUR appelés à réaliser des signatures électroniques au sein du service, son équipés à la volé, d'un certificat de signature électronique éphémère, généré pour chaque transaction et créée à la base des données d'activation recueillies à travers le formulaire de souscription ainsi qu'un SMS d'identification unique OTP. Ce certificat expire en 4 heures et est protégé par

un passe phrase aléatoire généré par le serveur et non accessible aux administrateurs systèmes. Ce qui garantie une protection optimale de la clé privée associée au certificat de signature.

A noter que ces certificats sont générés à partir d'une IGC intégrer dans la plateforme eContract pour le compte de la société de conseil en assurance et finance (VOYAGEASSUR).

3.2. Pré-requis à l'acte de signature

Le navigateur de l'utilisateur doit être configuré correctement et doit être récent.

Le poste de l'utilisateur doit disposer du plug-in Adobe® Reader® dans la version minimale 9.

3.3. Déroulement fonctionnel de l'acte de signature

Au sein du service VOYAGEASSUR, l'acte de signature est clairement mis en exergue de plusieurs manières :

- Un texte explicite est présenté au signataire pour lui expliciter la portée de l'acte qu'il s'apprête à réaliser ;
- Le document que l'utilisateur s'apprête à signer lui est présenté : il a la possibilité de le visualiser entièrement à travers son poste de travail ;
- L'utilisateur à la possibilité de renoncer et de refuser de signer ;
- L'utilisateur doit activer un bouton intitulé « signer » opérationnel après avoir accepté toutes les messages de consentement.

Les documents signés sont exclusivement au format **PDF.**

Une fois le bouton « signer » activé par l'utilisateur, les opérations suivantes se déroulent :

- Un certificat éphémère est généré à l'occasion de la transaction en cours
- La signature électronique est générée;
- la signature est complétée par un jeton d'horodatage

- le document signé est traité et conservé dans le cadre du service VOYAGEASSUR.

3.4. Processus de signature

Le processus décrit, assure l'information correcte du signataire sur la portée de son action :

1. Présentation du document à signer : Le signataire a la possibilité de visualiser les informations qu'il s'apprête à signer.

2. Présentation des attributs de la signature au signataire : Les « attributs » de la signature font partie des données signées et, à ce titre, sont présentées au signataire pour lui permettre d'avoir connaissance des conditions dans lesquelles sa signature électronique sera réalisée et traitée. Ces attributs contiennent:

- Une référence non ambiguë de la politique présente de signature (en pratique, un OID) – éventuellement.
- Le certificat à utiliser pour signer
- Date et heure de signature
- type d'engagement

3. Consentement explicite et possibilité d'arrêt du processus de signature : Le signataire a les moyens d'exprimer explicitement (c'est-à-dire, de manière volontaire et non ambiguë) son consentement pour sélectionner un document et déclencher le processus de signature. Ce consentement porte aussi sur l'acceptation de la politique de signature applicable.

Ce consentement se manifeste par une case à cocher permettant de déverrouiller le bouton déclenchant la signature.

3.5. Contrôle de révocation

Le certificat de signature généré par la plateforme au nom de l'usager à l'occasion d'une transaction, a une durée limité ne dépassant pas 4 heures. Aucune fonctionnalités de révocation n'est prévue et le certificat n'est pas utiliser ailleurs que

la transaction pour laquelle elle a était générée d'autant plus qu'il est protégé par un passe-phrase que uniquement le serveur génère et gère.

3.6. Horodatage de la signature

Les signatures électroniques générées sont horodatées par le service d'horodatage BarideSign de de Barid Al Maghrib conformément à la Politique d'Horodatage ayant l'OID : **1.2.504.1.1.1.1.1.3.1.2.1**

Cet horodatage est conforme au standard RFC 3161 et accessible sur : https://psce.baridesign.ma/AC_Horodatage/indexs/indexEntity.php?name=TSP Service&action=timestamp

3.7. Format des signatures électroniques

3.7.1. Stockage des signatures

Les signatures électroniques sont incluses dans les documents signés conformément au format PDF (CMS). Elles sont donc enveloppées (PDF).

Les jetons d'horodatage qui y sont inclus sont conformes à la RFC 3161 de l'IETF.

3.7.2. Garantie du lien entre la signature et le document

Le protocole standard de signature SHA256-RSA garantit techniquement un lien entre la signature électronique et le document sur lequel il porte. Toute modification ultérieure du document sera détectable par l'opération de vérification de signature

3.7.3. Mode de vérification des signatures électroniques

Les signatures électroniques réalisées au sein des services dématérialisés de eContract peuvent être vérifiées en utilisant les fonctions natives de l'outil Adobe ® Reader ®, disponible gratuitement sur Internet.

Elles peuvent également être vérifiées par tout autre outil implémentant les normes SHA256-RSA, TSP et CMS.

Seule pré-requis étant l'acceptation du certificat racine de la plateforme eContract dans le magasin de certificat de confiance du poste de vérification et dans Acrobat.