Politique de Signature

Espace personnel MACSF

Version 3

Référence du document	Date d'application
PSIGN_MACSF_03	14 mars 2017

SOMMAIRE

1 DEFINITIONS ET ACRONYMES

Actes : désigne les opérations ou actions disponibles et réalisées en ligne telles que prévues dans les Conditions Générales et avec Signature électronique.

Archiveur : désigne l'hébergeur des Fichiers de preuve placé sous la responsabilité du Prestataire de Service d'Archivage Electronique.

Autorité de Certification (ou **AC**) **:** désigne l'une des composantes de l'Infrastructure de confiance générant et émettant des Certificats sur demande des Autorités d'enregistrement, et ce en application des règles et des pratiques déterminées par elle dans sa Politique de Certification.

Autorité d'Enregistrement (ou **AE**) : désigne l'une des composantes de l'Infrastructure de confiance, pour enregistrer les demandes des Utilisateurs, les valider ou les rejeter.

Autorité de Gestion de Preuve (ou **AGP**) : désigne l'une des composantes de l'Infrastructure de confiance, qui a en charge la création du Fichier de preuve permettant d'attester de la réalisation de l'Acte sensible par l'Utilisateur.

Autorité de Restitution de Preuve (ou **ARP**) : désigne l'une des composantes de l'Infrastructure de confiance, qui a en charge la restitution des preuves permettant d'attester de la réalisation de l'Acte par l'Utilisateur.

Certificat électronique ou **Certificat** : désigne un fichier électronique attestant du lien entre une identité et la Clé publique de la personne titulaire du Certificat.

Clé publique : désigne une clé mathématique rendue publique et qui est utilisée pour vérifier la signature numérique d'une donnée reçue.

Code de sécurité : code temporaire à usage unique adressé à l'Utilisateur par SMS sur son téléphone mobile personnel.

Code secret : code temporaire délivré à l'issue du processus d'identification par SMS ou courrier postal ou courrier électronique à l'Utilisateur permettant l'accès à l'Espace personnel. Selon les cas, l'Utilisateur devra se connecter à l'Espace personnel et suivre les instructions qui lui seront données jusqu'à la modification de son code secret. Ce code secret est strictement personnel et non cessible. L'Utilisateur reconnait s'imposer comme règle de sécurité de modifier son code secret fréquemment.

Conditions Générales : désigne les Conditions générales d'utilisation de l'Espace personnel et/ou les conditions générales de souscription en ligne et/ou tout document décrivant le processus de souscription en ligne d'un contrat et/ou les conditions acceptées dans le cadre de la réalisation de l'Acte.

Espace personnel : désigne le portail internet sécurisé et accessible gratuitement par les Utilisateurs (hors frais d'accès et d'utilisation du réseau Internet) à l'adresse www.macsf.fr.

Fichier de preuve : dans le cadre de la Signature Électronique, désigne l'ensemble des données électroniques lié à un acte réussi, conservé par le Groupe MACSF ou un Tiers de confiance conformément aux exigences légales et permettant ainsi d'assurer la preuve d'un Acte.

Groupe MACSF : signifie toute entité juridique entrant directement dans le périmètre de combinaison de MACSF SGAM (Société de Groupe d'Assurance Mutuelle, dont le siège social est Cours du triangle, 10, rue de Valmy, 92800 Puteaux, SIREN n° 488 324 617), tel que défini par les articles L345-2 et R345-1-2 du Code des assurances ainsi que toute entité juridique contrôlée, directement ou indirectement, par les entités entrant directement dans ledit périmètre de combinaison, à la date de rédaction de la présente PSIGN ou à quelque moment que ce soit après ladite date.

Horodatage : désigne l'ensemble des prestations nécessaires à la génération des contremarques de temps et à la gestion des unités d'horodatage.

Identifiant : désigne le numéro à sept chiffres de l'Utilisateur, qui lui est communiqué par le Groupe MACSF lors de la souscription d'un contrat auprès d'une entité du Groupe MACSF.

Infrastructure de confiance : désigne un ensemble de services consistant en la mise en œuvre des fonctions qui contribuent à la sécurisation des informations échangées par voie électronique.

DOCUSIGN : est le tiers de confiance**.** DOCUSIGN France est une Société anonyme au capital de 2 085 600,40 euros, immatriculée au Registre du Commerce et des sociétés de Nanterre sous le numéro 812 611 150, dont le siège social est situé 175 rue Jean Jacques Rousseau 92138 92131 Issy-les-Moulineaux Cedex et dont le nom commercial est DOCUSIGN.

MACSF assurances : Société d'Assurances Mutuelle, entreprise régie par le Code des assurances, SIREN N° 775 665 631, dont le siège social est situé Cours du triangle, 10, Rue de Valmy, 92800 PUTEAUX.

Politique de Certification : désigne l'ensemble des règles énoncées et publiées par l'AC décrivant les caractéristiques générales des Certificats qu'elle délivre. Ce document décrit les obligations et responsabilités de l'AC, de l'AE, des porteurs de Certificat (ou Utilisateurs) et de toutes les composantes intervenant dans l'ensemble du cycle de vie d'un Certificat. Elle est accessible à l'adresse : http://www.docusign.com

Prestataire de Service d'Archivage Electronique (PSAE) : le PSAE a en charge la conservation des Fichiers de preuve et met à la disposition du Client un coffre-fort électronique pour l'archivage des Fichiers de preuve, garantissant ainsi leur pérennité et leur intégrité pendant la durée d'archivage.

Service Protect&Sign® : désigne le service de DOCUSIGN mis à disposition de ses clients et constitué notamment de l'Application Protect&Sign® dont l'objet pour le Groupe MACSF est de lui permettre, à partir de l'Espace personnel, de proposer à ses Utilisateurs un service de signature de document sous forme électronique à partir d'une Signature électronique associée à un Certificat à usage unique d'une durée limitée émis pour chaque Acte et de constituer pour archivage électronique un Fichier de preuves relatif à l'Acte conclu en ligne.

Signature électronique : en application de l'article 1317 du Code civil, la signature électronique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.

Système d'Information MACSF (SI MACSF) : désigne le Système d'Information du Groupe MACSF dont la responsabilité est confiée à MACSF assurances.

Tiers de confiance : désigne DOCUSIGN, agissant en qualité d'Autorité de Certification, d'Autorité de Gestion de Preuve et de Prestataire de Service d'Archivage Electronique.

Utilisateur : désigne tout prospect ou tout assuré, adhérent, sociétaire ou client des entités appartenant au Groupe MACSF ayant accepté les Conditions générales et ayant souscrit un contrat, un produit ou un service avec l'une de ces entités.

2 INTRODUCTION

2.1 Présentation et périmètre

Le Groupe MACSF met à disposition des Utilisateurs un Espace personnel afin de réaliser des Actes tels que prévus dans les Conditions Générales.

En effet, certaines actions ou opérations nécessitent d'être signées électroniquement par l'Utilisateur.

Le présent document décrit :

- les mesures et les contraintes mises en place afin que ces opérations de Signature électronique soient réalisées sur le site macsf.fr
- les conditions d'accès, de vérification et de restitution des documents signés.

Ce document est destiné aux :

- Utilisateurs amenés à signer des Actes sur l'Espace personnel
- destinataires des Actes signés qui ont, ou auront, besoin de connaître les conditions de réalisations des Actes signés.

Il est complété par les documents listés au 2.4 ci-dessous.

Il ne s'applique pas aux opérations ou actions réalisées sans Signature électronique.

2.2 Identification et publication de la Politique de Signature des Actes sur l'Espace personnel

Le présent document est une Politique de Signature des Actes sur l'Espace personnel (ci-après « PSIGN »). La PSIGN a été portée à la connaissance de l'Utilisateur dans le cadre du processus de Signature électronique et avant l'opération de Signature électronique.

La validité de la Signature électronique est appréciée au regard de la PSIGN en vigueur au moment de la Signature électronique.

La PSIGN en vigueur est identifiée avec son numéro de version et sa date de mise à jour.

Elle est accessible sur le site macsf.fr à l'adresse : https://www.espacemembre.macsf.fr/securite

Les questions ou demandes concernant la PSIGN sont à communiquer au Responsable de la Sécurité du Système d'Information du Groupe MACSF (ci-après le « RSSI ») par :

- Courrier
  Sécurité des Systèmes d'Information
  10 cours du Triangle de l'Arche
  92919 La Défense Cedex
- Courriel
  securite@macsf.fr

Toutes les versions de la PSIGN sont également disponibles sur demande à l'adresse ci-dessus.

Le Groupe MACSF utilise les solutions de Signature électronique et d'enregistrements informatiques mises à disposition par MACSF assurances.

2.3 Gestion de la PSIGN

L'entité en charge de la gestion de la PSIGN est la Sécurité du Système d'Information du Groupe MACSF, représentée par le RSSI. A ce titre, elle est garante du processus de mise à jour de la PSIGN.

2.4 Documents complémentaires

La PSIGN est notamment complétée par les documents suivants :

- Conditions Générales
- Politique de signature et de gestion de preuves du Service Protect&Sign® disponible sur le site www.docusign.com
- Politique de certification DOCUSIGN disponible sur le site www.docusign.com

3 SIGNATURE ELECTRONIQUE DES ACTES

3.1 Périmètre

Le Groupe MACSF met en ligne sur l'Espace personnel des services permettant à l'Utilisateur de réaliser des Actes.

Certains Actes nécessitent un processus de Signature électronique pour être réalisés. Le périmètre de ces Actes pourra être revu régulièrement sans que la PSIGN n'évolue systématiquement.

3.2 Rôles et responsabilités

Les droits et obligations de l'Utilisateur et du Groupe MACSF sont décrits dans les Conditions Générales.

3.2.1 L'Utilisateur

Pour réaliser des Actes sur l'Espace personnel, les Utilisateurs doivent au préalable accepter les Conditions Générales.

L'objectif des Conditions Générales est de définir les conditions d'accès à l'Espace personnel. Elles décrivent notamment pour l'Utilisateur :

- les moyens nécessaires à l'utilisation de l'Espace personnel
- les conditions d'accès à l'Espace personnel
- la convention de preuve
- les obligations et les responsabilités.

Dans certains cas, l'accès à l'Espace personnel nécessite une identification / authentification de l'Utilisateur par l'Autorité d'Enregistrement. L'Utilisateur a la responsabilité de la sécurité des moyens d'authentification que sont :

(i) son Code secret,
(ii) son Code de sécurité et
(iii) son téléphone mobile sur lequel il reçoit son Code de sécurité.

L'authentification nécessaire à la réalisation des Actes est basée sur des informations fournies par l'Utilisateur.

3.2.2 MACSF assurances

MACSF assurances, en sa qualité d'Autorité d'Enregistrement, a en charge l'identification et l'authentification de l'Utilisateur.

Son rôle est d'établir que l'Utilisateur, lorsqu'il réalise un Acte, justifie de l'identité utilisée. Pour cela, il respecte les procédures définies dans le cadre de ses procédures d'enregistrement.

MACSF assurances délègue en partie l'enregistrement des nouveaux Utilisateurs aux entités du Groupe MACSF.

MASCF assurances est garante de la sécurisation des Actes sur l'Espace personnel dans le cadre du processus de signature en ligne ; MACSF assurances :

- Collecte auprès de l'Utilisateur les données de l'Acte souhaité
- Constitue le(s) fichier(s) pdf contenant les données de l'Acte
- Transmet le(s) fichier(s) à signer contenant les données de l'Acte au Tiers de confiance et des données à intégrer dans le Fichier de preuve
- Transmet, quand il est nécessaire, le Code de sécurité à l'Utilisateur par SMS.

3.2.3 Tiers de confiance

DOCUSIGN est Tiers de confiance. DOCUSIGN est Autorité de Certification, Autorité de Gestion de Preuve et Prestataire de Service d'Archivage Electronique.

Les Certificats utilisés pour signer les documents pdf sont délivrés par le Tiers de confiance et ont une durée de vie limitée.

Ils sont délivrés au nom de l'Utilisateur qui réalise l'Acte et ne sont utilisés qu'une seule fois.

L'Autorité de Certification délivre également des Certificats pour authentifier MACSF assurances auprès du Tiers de confiance et sécuriser leurs échanges.

DOCUSIGN a en charge la création des Fichiers de preuve.

Ce Fichier de preuve sera utilisé en cas de litige afin de démontrer l'existence de l'Acte et l'intégrité des données qui le constituent.

DOCUSIGN met en oeuvre les applications logicielles nécessaires à la génération du Fichier de preuve et est en charge de l'hébergement de l'applicatif de signature pour signer les Actes.

Les engagements de DOCUSIGN sont notamment formalisés au travers de la politique de signature et de gestion de preuve du Service Protect&Sign® définie à l'article 2.4 ci-dessus.

DOCUSIGN a en charge la conservation des Fichiers de preuve et met à la disposition de MACSF assurances un coffre-fort électronique pour l'archivage de ceux-ci, garantissant ainsi leur pérennité et leur intégrité pendant la durée d'archivage.

Il conserve les Fichiers de preuve conformément aux dispositions relatives à l'archivage décrites à l'article 3.6.

DOCUSIGN utilise l'archiveur CDC Arkhinéo pour l'hébergement et la restitution des Fichiers de preuve.

3.3 Enregistrement des Utilisateurs

L'enregistrement définitif des Utilisateurs est subordonné à l'accord d'une des entités du groupe MACSF, conformément à ses règles d'acceptation.

L'acceptation des Conditions Générales par l'Utilisateur est un prérequis à l'utilisation de la Signature électronique d'un Acte.

3.4 Signature électronique de l'Acte

3.4.1 Pré-requis de l'équipement de l'Utilisateur

Les pré-requis nécessaires à l'utilisation de l'Espace personnel sont listés dans les Conditions Générales.

3.4.2 Données à valider par l'Utilisateur

L'Utilisateur valide les éléments présents dans le fichier pdf ou sur l'écran de synthèse. Ces éléments sont variables en fonction de l'Acte mais sont au minimum :

- l'Acte concerné
- le type d'Acte
- le contenu de l'Acte.

3.4.3 Opération de validation de l'Acte : le consentement

Cette opération permet d'obtenir le consentement de l'Utilisateur sur la réalisation de l'Acte et se compose a minima des étapes suivantes :

- L'Utilisateur saisit les données de l'Acte souhaité.
- Les données saisies sont présentées à l'Utilisateur. Il peut modifier sa demande si la demande présentée ne lui convient pas.
- S'il est demandé, il saisit le Code de sécurité transmis par SMS sur son numéro de téléphone mobile référencé dans le Système d'Information MACSF.
- Il accepte les conditions de réalisation de l'Acte en cochant une ou plusieurs cases
- Il clique sur un bouton de type « Signer ».
- Le document pdf est signé au nom de l'Utilisateur chez le Tiers de confiance.

Ces différentes étapes permettent d'assurer que l'Utilisateur a exprimé son consentement de manière volontaire et non ambiguë. Il dispose des moyens lui permettant d'arrêter le processus de validation.

3.4.4 Procédé de signature électronique

Le document pdf produit est signé électroniquement avec le Certificat généré à la volée par le Tiers de confiance. Ce Certificat est au nom de l'Utilisateur. Il est délivré dans les conditions décrites dans la Politique de Certification.

3.4.5 Information de l'Utilisateur suite à la réalisation d'un Acte

Après la réalisation de l'Acte, l'Utilisateur peut retrouver les données de celui-ci dans, au minimum, son Espace personnel.

3.5 Gestion de la preuve

Pour conserver une trace de l'Acte réalisé, MACSF constitue un Fichier de preuve électronique signé et horodaté qui contient les données associées à l'Acte réalisé.

Ce Fichier de preuve est constitué et archivé immédiatement après la signature de l'Acte.

Sur ce Fichier de preuve, une contremarque de temps est apposée.

Le Fichier est signé au nom de MACSF assurances.

3.6 Archivage du Fichier de preuve

3.6.1 Objectifs

Le présent chapitre constitue la politique d'archivage des traces des Actes réalisés par les Utilisateurs sur leur Espace personnel (ci-après « la Politique d'archivage »).

La Politique d'archivage décrit les règles applicables à la constitution et à la mise en archive des éléments liés aux Actes, afin que l'archivage puisse être défini comme fiable. Ces éléments archivés sont ceux nécessaires à l'établissement des preuves et peuvent être restitués en cas de litige avec un Utilisateur.

Les objectifs recherchés sont de disposer d'archives :

- dont la source est identifiée/authentifiée,
- intègres,
- disponibles et lisibles durant toute la durée de conservation définie,
- dont les opérations sur celles-ci sont tracées.

Cette Politique d'archivage reprend, en partie, les conditions contractualisées avec le Tiers de confiance.

3.6.2 Cycle de vie de l'archive

Dans le cadre d'un Acte réalisé par un Utilisateur sur son Espace personnel, les éléments mis en archive sont les Fichiers de preuve constitués par le Tiers de confiance.

Les Fichiers de preuve sont transmis au Prestataire de Service d'Archivage Electronique par l'Autorité de Gestion de Preuve.

Les Fichiers de preuve archivés sont stockés dans un coffre-fort électronique adapté.

Dès réception du Fichier de preuve à archiver, celui-ci est aussitôt validé comme étant émis ou reçu, puis horodaté et signé numériquement afin de garantir son intégrité et son inviolabilité.

Le Fichier de preuve à archiver est ainsi encapsulé avec ces informations puis dirigé vers un équipement d'archivage définitif.

Ces actions sont réalisées sous la responsabilité du PSAE.

3.6.3 Architecture du service d'archivage électronique

Le système interne d'horodatage est assuré via un dispositif GPS qui permet d'assurer une heure juste de type GMT.

Un calcul interne d'empreinte est réalisé sur l'ensemble du Fichier de preuve reçu.

Une archive ne peut pas être supprimée d'un coffre existant.

La sécurité et la continuité du service sont assurées et selon les conditions prévues dans le contrat conclu avec le Prestataire de Service d'Archivage Electronique.

Le service de consultation des Fichiers de preuve est notamment secouru sur un site distant du site de production.

3.6.4 Restitution de la preuve

MACSF assurances est l'Autorité de Restitution de Preuves.

Cette ARP est la seule habilitée à accéder aux éléments archivés et ceci afin de constituer les éléments de preuve nécessaires en cas de litige.

Les flux entre l'ARP et le PSAE sont sécurisés/chiffrés avec le protocole TLS.

4 DISPOSITIONS JURIDIQUES

4.1 Droit applicable et juridictions compétentes

La PSIGN est soumise au droit français. En cas de litige relatif à l'application de la PSIGN, les tribunaux français seront seuls compétents.

4.2 Données personnelles – Loi « Informatique et libertés »

L'Utilisateur accepte le traitement informatisé des informations recueillies dans le cadre de la Signature des Actes et de son accès à l'Espace personnel.

Les informations nominatives ainsi recueillies sont obligatoires pour le traitement de la demande de l'Utilisateur dans le cadre de la PSIGN. Elles sont destinées, de même que celles qui seront recueillies ultérieurement, à chaque entité du Groupe MACSF auprès de laquelle l'Utilisateur a souscrit un contrat, un produit ou un service. A défaut d'opposition de la part de l'Utilisateur pour des motifs légitimes, chacune de ces entités du Groupe MACSF est autorisé, de convention expresse, à les conserver en mémoire informatique, à les utiliser, ainsi qu'à les communiquer aux même fins aux entités du Groupe MACSF, voire à des tiers ou à des sous-traitants pour des besoins de gestion.

L'Utilisateur peut s'opposer, sans frais, à ce que les données le concernant soient utilisées à des fins de prospection, notamment commerciale.

Les droits d'accès, de rectification et d'opposition peuvent être exercés par courrier auprès de MACSF – Direction Juridique - 10 Cours du Triangle de l'Arche - TSA 40100 - 92919 La Défense Cedex.

Le Groupe MACSF conserve l'historique des connexions de l'Utilisateur à l'Espace personnel dans les délais et conditions prévues par la loi, sans que ces délais ne soient inférieurs à ceux applicables aux contrats souscrits par l'Utilisateur. A ce titre, l'Utilisateur déclare accepter la possibilité pour le Groupe MACSF d'utiliser la technique des cookies ou toute autre technique assimilée ou similaire permettant de tracer la navigation de l'Utilisateur.

5 POLITIQUE DU RISQUE DE SECURITE DE L'INFORMATION

De manière plus générale, les Actes sur l'Espace personnel sont réalisés dans le respect de la politique du Risque de Sécurité de l'Information MACSF.

La politique du Risque de Sécurité de l'Information MACSF constitue le cadre de référence en matière de sécurité de l'information du Groupe MACSF. Elle précise les enjeux et les exigences de sécurité et exprime les principes de gouvernance qui s'appliquent. Elle permet de garantir :

- La disponibilité des informations et des moyens de les traiter.
- L'intégrité des informations et des moyens de les traiter.
- La confidentialité des informations gérées.
- L'auditabilité des moyens de traitement de l'information.

Le RSSI est le garant de la sécurité et de la continuité du Système d'Information MACSF.

La présente PSIGN fait donc partie intégrante du dispositif de contrôle des risques liés à la sécurité de l'information.