

Politique de Signature du Secrétariat général de l'ACPR

**Pour les remises réglementaires du domaine Assurance
mentionnant l'application de l'instruction n° 2015-I-18
relative à la signature électronique de documents télétransmis à l'ACPR**

Date : 01/10/2016
Version 3.1
Nombre de pages : 11

Table des matières

1.	Objet du document	4
2.	Politique de signature électronique	4
2.1.	Champ d'application.....	4
2.2.	Identification	4
2.3.	Publication du document	5
2.4.	Processus de mise à jour	5
2.4.1.	Prise en compte des remarques.....	5
2.4.2.	Information des acteurs	5
2.5.	Entrée en vigueur et période de validité.....	5
3.	Acteurs.....	5
3.1	Les représentants des organismes assujettis	5
3.2.	Le Secrétariat Général de l'ACPR.....	6
3.3.	Obligations de l'organisme assujetti	6
3.3.1.	Environnement du poste de travail.....	6
3.3.2.	Choix des représentants de l'organisme assujetti.....	6
3.4.	Obligations du représentant d'un assujetti.....	6
3.4.1.	Outil de signature utilisé	6
3.4.2.	Type de certificat utilisé	6
3.4.3.	Protection du support du certificat.....	6
3.4.4.	Révocation du certificat.....	7
3.5.	Obligations du Secrétariat Général de l'ACPR.....	7
3.5.1.	Données de Vérification	7
3.5.2.	Protection des moyens	7
3.5.3.	Journalisation	7
3.5.4.	Reprise en cas d'interruption de service	7
3.5.5.	Assistance aux organismes	7
4.	Signature électronique et validation	8
4.1	Données signées.....	8
4.2.	Caractéristiques des signatures.....	8
4.2.1.	Type de signature	8
4.2.2.	Norme de signature.....	8

4.3. Algorithmes utilisables pour la signature	9
4.3.1. Algorithme de condensation	9
4.3.2. Algorithme de chiffrement	9
4.3.3. Canonicalisation	9
4.4. Conditions pour déclarer valide le fichier signé	9
4.4.1. Vérification de la signature.....	9
4.4.2. Vérification des droits du signataire en fonction de données transmises	9
5. Politique de confidentialité	10
5.1. Classification des informations.....	10
5.2. Communication des informations à des tiers.....	10
6. Dispositions juridiques	10
6.1. Données nominatives	10
7. Certificat ayant signé le présent document	11

1. Objet du document

La signature électronique apposée sur un ensemble de données permet de garantir l'intégrité des données transmises et l'authenticité de leur émetteur.

Une politique de signature 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.

Le présent document, « Politique de Signature du Secrétariat Général de l'ACPR » pour le domaine Assurance, décrit ces conditions dans le cadre des échanges électroniques entre les organismes assujettis à des remises réglementaires et le Secrétariat Général de l'ACPR (SGACPR).

Ce document est destiné :

- au SGACPR ;
- aux organismes assujettis à des remises réglementaires ;
- aux éventuels prestataires participant à ces échanges pour le compte des assujettis ou du SGACPR.

Dans la suite de ce document, les organismes assujettis à la remise de données par voie électronique selon les collectes auxquelles ils sont soumis sont désignés par le terme « organismes assujettis ».

2. Politique de signature électronique

2.1. Champ d'application

La présente politique de signature s'applique aux collectes réglementaires dont l'instruction indique l'application de l'instruction n° 2015-I-18 relative à la signature électronique de documents télétransmis à l'ACPR et transmises par les organismes mentionnés à l'article 1^{er} de la présente instruction.

Conformément à la présente instruction, ces remises font l'objet d'une signature électronique.

La signature électronique doit être apposée sur l'intégralité des données d'une remise.

Cette signature est apposée par une personne habilitée à engager l'organisme auprès du SGACPR pour l'ensemble des données transmises.

Chaque fichier remis au format XBRL fait l'objet d'une et une seule signature électronique.
Les remises bureautiques peuvent faire l'objet de plusieurs signatures électroniques.

2.2. Identification

La présente politique de signature est identifiée par l'OID (Object Identifier) : 1.2.250.1.115.200.301.1

Cette référence figure dans les données signées conformément au paragraphe 4.2.2 de ce document afin d'attester du régime sous lequel le signataire adresse sa remise.

2.3. Publication du document

La présente politique est publiée après approbation formelle du SGACPR et apposition d'une signature électronique.

La présente politique est consultable à l'adresse suivante:

http://www.banque-france.fr/igc/signature/ps/ps_1_2_250_1_115_200_301_1.pdf

2.4. Processus de mise à jour

2.4.1. Prise en compte des remarques

Toutes les remarques, ou souhaits d'évolution, sur la présente politique sont à adresser par courriel à l'adresse suivante:

sagemoa-garu@acpr.banque-france.fr

Ces remarques et souhaits d'évolution sont examinés par le SGACPR qui engage si nécessaire le processus de mise à jour de la présente politique de signature.

2.4.2. Information des acteurs

Les informations relatives à la version courante de cette politique sont disponibles sur le site du SGACPR.

La publication d'une nouvelle version de la politique de signature consiste à mettre en ligne les éléments suivants :

- la politique de signature au format PDF,
- l'identifiant de la politique de signature (OID),
- l'empreinte de la politique de signature,
- l'algorithme de hachage utilisé pour réaliser l'empreinte de la politique de signature,
- la valeur de la signature apposée sur la politique de signature,
- l'algorithme de hachage et de chiffrement utilisé pour réaliser la signature de la politique de signature,
- la date et l'heure d'entrée en vigueur de la politique de signature.

2.5. Entrée en vigueur et période de validité

Cette politique de signature entre en vigueur à compter du 01/10/2016 après sa mise en ligne sur le site Internet du SGACPR, et reste valide jusqu'à l'entrée en vigueur d'une nouvelle version.

Le délai entre publication et entrée en vigueur est mis à profit par les organismes assujettis pour prendre en compte les changements et mettre à jour, dans leurs applications de signature, la référence à la politique courante.

3. Acteurs

3.1 Les représentants des organismes assujettis

Le rôle des représentants des organismes assujettis consiste à :

- apposer leur signature électronique sur une remise ;
- s'assurer que la remise signée est transmise au SGACPR.

Pour apposer une signature électronique sur une remise, les représentants des organismes assujettis disposent d'un certificat de signature et d'un outil de signature.

La qualité d'un signataire ne figurant pas dans son certificat, seuls les représentants préalablement enregistrés auprès du SGACPR peuvent engager leur organisme pour une remise donnée en y apposant leur signature.

3.2. Le Secrétariat Général de l'ACPR

Le rôle du SGACPR consiste à :

- vérifier la validité de la signature et du certificat ayant servi à sa création ;
- vérifier l'habilitation du signataire à engager son organisme pour une remise donnée ;
- vérifier la cohérence des données transmises ;
- traiter les données figurant dans les remises.

Le SGACPR peut déléguer tout ou partie de ces tâches à des prestataires de service en s'assurant de la conformité des services rendus par ces prestataires avec la présente politique de signature.

3.3. Obligations de l'organisme assujetti

3.3.1. Environnement du poste de travail

L'opération de création de la signature doit être réalisée sur des postes de travail contrôlés et sécurisés.

L'organisme assujetti s'assure que les postes de travail de ses représentants sont protégés notamment contre l'utilisation frauduleuse de leur identité et de leur outil de signature dans le cadre des applications dont la présente politique de signature fait objet.

3.3.2. Choix des représentants de l'organisme assujetti

Parallèlement à la déclaration prévue à l'article 4 de la présente instruction, chaque organisme assujetti télétransmet les éléments identifiant les certificats des personnes autorisées à signer en son nom, ainsi que, pour chaque certificat, la liste des documents que ce certificat est autorisé à signer.

L'ensemble de ces informations sera précisé dans une note technique.

3.4. Obligations du représentant d'un assujetti

3.4.1. Outil de signature utilisé

Le représentant d'un organisme assujetti contrôle les données qu'il va signer avant d'y apposer sa signature.

3.4.2. Type de certificat utilisé

Le représentant d'un organisme assujetti utilise un certificat de signature appartenant à une famille de certificats reconnue conformément à la présente instruction.

3.4.3. Protection du support du certificat

Le représentant prend toutes les 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, dongle, token, ...) et le code PIN associé.

3.4.4. Révocation du certificat

Le représentant d'un organisme assujetti demande dans les plus brefs délais à l'organisme émetteur de son certificat la révocation de celui-ci en cas de perte, de vol, de compromission ou de simple suspicion de compromission de sa clé privée.

3.5. Obligations du Secrétariat Général de l'ACPR

3.5.1. Données de Vérification

Pour effectuer les vérifications, le service de validation utilisé par le SGACPR utilise les données transmises par les organismes assujettis concernant les habilitations de leurs représentants, ainsi que des données publiques relatives aux certificats des signataires, telles que les listes de révocations, les services OCSP ou les certificats des prestataires de services de certification électronique émetteurs.

Selon les familles de certificat, un délai variable s'applique entre le moment où est demandée la révocation d'un certificat et le moment où la liste des certificats révoqués est mise à disposition du public. Le SGACPR ne saurait être tenu responsable des conséquences d'une validation de signature effectuée pendant ce délai de latence.

3.5.2. Protection des moyens

Le SGACPR s'assure de la mise en œuvre des moyens nécessaires à la protection des équipements fournissant les services 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.

3.5.3. Journalisation

Le SGACPR 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.

Le SGACPR s'assure que les preuves de traitement relatives à la vérification des signatures électroniques sont conservées pendant 10 ans.

3.5.4. Reprise en cas d'interruption de service

Le SGACPR 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 il a la responsabilité.

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

3.5.5. Assistance aux organismes

Les organismes assujettis peuvent s'adresser par courriel aux correspondants SAGEMOA pour toute information complémentaire ou pour signaler tout dysfonctionnement à l'adresse suivante :

sagemoa-garu@acpr.banque-france.fr

4. Signature électronique et validation

4.1 Données signées

Les données signées sont composées des éléments suivants :

- l'intégralité des données (non ré encodées) constituant chaque remise telle que décrite dans son instruction ;
- les propriétés de signature telles que définies aux paragraphes 4.2.2 du présent document.

Les différentes remises signées font l'objet de fichiers séparés.

Chaque fichier n'étant signé que par un seul et unique représentant pour les fichiers, les fichiers ne contiennent que les données pour lesquelles le représentant est habilité à engager son organisme.

Si des données doivent être signées par des personnes distinctes, les données figurent dans des fichiers distincts.

4.2. Caractéristiques des signatures

Le format de signature suit les préconisations du RGI (Référentiel Général d'Interopérabilité) défini par l'ordonnance n° 2005-1516 et plus particulièrement le format de signature XAdES en version 1.1.1 ou supérieure.

4.2.1. Type de signature

Les signatures électroniques apposées par les représentants des organismes assujettis sont de type « Signature détachée (Manifest) ».

Dans le cas d'une signature détachée Manifest, une remise est constituée par un unique fichier zip. Ce fichier zip contient :

- un premier fichier qui contient l'intégralité des données (non ré encodées) constituant la remise telle que décrite dans son instruction ;
- et un deuxième fichier signature.xml qui contient la balise « Signature ». Cette balise contient elle-même :
 - dans la première balise « Object », le manifest qui référence l'intégralité des données constituant la remise ;
 - dans la deuxième balise « Object », les propriétés de signature telles que définies aux paragraphes 4.2.2 du présent document.

4.2.2. Norme de signature

Les signatures respectent la norme XAdES (ETSI TS 101 903) en version v1.1.1 ou supérieure. Le format XAdES étant un format XML, le jeu de caractères imposé est UTF-8.

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

- le certificat du signataire (SigningCertificate) ;
- la date et l'heure de signature (SigningTime) ;
- la référence au présent document (SigningPolicyIdentifier / SigPolicyIdType) :
 - OID de la présente politique de signature (SigPolicyId) ;
 - Valeur de condensé de la politique de signature calculé et algorithme de condensation utilisé (SigPolicyHash).

Une fois signé, le fichier ne fait plus l'objet d'aucun transcodage, et transite dans le système d'information de l'organisme sous la forme d'un flux binaire, avant d'emprunter les canaux habituels de transmission entre les organismes et le SGACPR.

4.3. Algorithmes utilisables pour la signature

4.3.1. Algorithme de condensation

Les algorithmes de condensation à utiliser sont SHA-256 au minimum.

4.3.2. Algorithme de chiffrement

Les algorithmes de chiffrement à utiliser sont RSA-2048 au minimum.

4.3.3. Canonicalisation

La canonicalisation ne s'applique qu'aux remises d'un format XML/XBRL. Les remises bureautiques ne sont pas concernées par cet algorithme.

- L'algorithme de mise en forme canonique exclusif (identifié par l'URI <http://www.w3.org/2001/10/xml-exc-c14n#>) est utilisé.

4.4. Conditions pour déclarer valide le fichier signé

Un fichier signé est considéré comme valide par le SGACPR 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.

4.4.1. Vérification de la signature

La vérification de la signature porte sur :

- la vérification du respect de la norme de signature ;
- la vérification de l'appartenance du certificat du signataire à une famille de certificat reconnue par le SGACPR ;
- la vérification du certificat du signataire 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 apposée sur le fichier en utilisant la clé publique du signataire contenue dans le certificat transmis ;
- la vérification de l'identifiant de la politique de signature référencée.

4.4.2. 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.

La collecte des droits relatifs aux représentants est gérée au fil de l'eau par les administrateurs du SGACPR en fonction des informations fournies par les organismes assujettis.

5. Politique de confidentialité

5.1. Classification des informations

Les informations suivantes sont considérées comme confidentielles :

- les journaux du service de validation ;
- les procédures internes du service de validation ;
- les rapports de contrôle de conformité et les plans d'action référents.

5.2. Communication des informations à des tiers

On entend par tiers, tout organisme n'étant pas dans la chaîne de traitement des informations du SGACPR. La diffusion des informations à un tiers ne peut intervenir qu'après acceptation du SGACPR.

6. Dispositions juridiques

6.1. Données nominatives

En conformité avec les dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le traitement automatisé des données nominatives réalisé à partir de la plateforme de vérification de signature de la Banque de France a fait l'objet d'une déclaration auprès du Correspondant Informatique et Libertés (CIL) de l'ACPR.

Conformément à l'article 32 de la loi n° 78-17 du 6 janvier 1978, le signataire d'une remise au SGACPR est informé que les données à caractère personnel qu'il communique sont utilisées par la plateforme de vérification de signature (SVMA) pour la gestion et le suivi des habilitations dans l'application ainsi que pour la constitution de la Preuve.

Conformément aux articles 39 et suivants de la loi n° 78-17 du 6 janvier 1978, l'utilisateur est informé qu'il dispose d'un droit d'accès, de rectification et d'opposition, pour des motifs légitimes, portant sur les données le concernant.

À ces fins, il peut adresser une demande écrite signée et accompagnée de la photocopie d'un document officiel d'identité portant la signature du titulaire (Carte Nationale d'Identité ou passeport, même périmés, carte professionnelle délivrée par l'État, carte d'identité militaire, permis de chasser, permis de conduire, carte de séjour...) à l'adresse suivante :

Autorité de Contrôle Prudentiel et de Résolution
Secrétariat Général
SAGEMOA / GARU (066-2718)
61 rue Taitbout
75436 PARIS CEDEX 09

7. Certificat ayant signé le présent document

Le certificat ayant servi à signer le présent document a été émis par l'Autorité de Certification de Signature de la Banque de France.