Annexe 1

Politique de Signature du Secrétariat général de l'ACPR

Pour les remises réglementaires du domaine Bancaire
mentionnant l'application de l'instruction n° 2015-I-19
relative à la signature électronique de documents télétransmis à l'ACPR

Date : 05/11/2018
Version 4.0
Nombre de pages : 11

Table des matières

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 bancaire », décrit ces conditions dans le cadre des échanges électroniques entre les établissements assujettis à des remises règlementaires et le Secrétariat Général de l'ACPR (SGACPR).

Ce document est destiné :

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

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

2. Politique de signature électronique

2.1. Champ d'application

La présente politique de signature s'applique aux collectes règlementaires des établissements visés par l'ensemble des instructions de l'ACPR dans lesquelles il est fait référence à la signature électronique.

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

Cette signature est apposée par une personne assurant la direction effective de l'entreprise ou ayant des compétences et une position lui permettant d'engager l'établissement auprès du SGACPR sur la qualité et la fiabilité des informations transmises.

Chaque fichier remis au format XBRL fait l'objet d'une seule signature électronique, par les personnes mentionnées à l'article 4 de l'instruction.
Les remises bureautiques peuvent faire l'objet de plusieurs signatures électroniques : dans le cas où les fichiers sont transmis séparément via plusieurs documents bureautiques, chaque document doit être individuellement signé.

2.2. Identification

La présente politique de signature est identifiée par l'OID (Object IDentifier) : 1.2.250.1.115.200.300.4

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_300_4.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 et aux versions antérieures sont disponibles sur le site de la Banque de France.

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 nouvelle version de la politique de signature entre en vigueur à compter du 05/11/2018 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 la date de publication et la date d'entrée en vigueur de la nouvelle version de la politique de signature permet aux établissements assujettis de tenir compte des changements opérés et de mettre à jour, dans leurs applications de signature, la référence à la politique courante.

3. Acteurs

3.1 Les représentants des établissements assujettis

Le rôle des représentants des établissements 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 établissements 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 établissement 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 établissement 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'établissement 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'établissement 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 état.

3.3.2. Choix des représentants de l'établissement assujetti

Parallèlement à la déclaration prévue à l'article 4 de la présente instruction, chaque établissement 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 établissement assujetti

3.4.1. Vérification des données à signer

Le représentant d'un établissement 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 établissement 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 établissement 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 auquel a recours le SGACPR utilise les données transmises par les établissements assujettis concernant les habilitations de leurs représentants, ainsi que les 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 la 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 établissements

Les établissements 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, les fichiers ne contiennent que les données pour lesquelles le représentant est habilité à engager son établissement.

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 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives 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 sur les remises effectuées au format XBRL par les représentants des établissements assujettis sont de type :

- Signature enveloppante[1] ou détachée (Manifest) pour les fichiers dont la volumétrie est en deçà du seuil de 10 Mo.
- Signature détachée (Manifest) pour les fichiers dont la volumétrie dépasse le seuil de 10 Mo.

Dans le cas d'une signature enveloppante, une remise est constituée par un unique fichier XML contenant la balise « Signature ». Cette balise contient elle-même :

- dans la première balise « Object », l'intégralité des données (non ré encodées) constituant la remise telle que décrite dans son instruction ;
- dans la deuxième balise « Object », les propriétés de signature telles que définies aux paragraphes 4.2.2 du présent document.

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.

Les remises effectuées au format bureautique sont signées électroniquement selon le mode détaché.

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 (SignaturePolicyId / SignaturePolicyIdType) :

[1] La signature enveloppante signe le document complet, à ne pas confondre avec la signature enveloppée qui ne concerne qu'une partie du document.

- 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'établissement sous la forme d'un flux binaire, avant d'emprunter les canaux habituels de transmission entre les établissements 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

Un bloc XML peut avoir plusieurs représentations. Par exemple, les espaces ne sont pas significatifs s'ils sont présents dans un élément. <MonElement> et <MonElement > sont identiques du point de vue logique. Néanmoins l'empreinte générée sera différente dans les deux cas. La forme canonique va permettre que des XML identiques au niveau logique produisent la même empreinte.

Les mises en forme canonique à utiliser sont :

<table>
<tr><td rowspan="3">Remises au format XML/XBRL</td><td rowspan="2">Avec une signature enveloppante</td><td>• L'algorithme de mise en forme canonique XML exclusive (identifié par l'URI https://www.w3.org/TR/xml-exc-c14n/) est préconisé.</td></tr>
<tr><td>• L'algorithme de mise en forme canonique inclusive V1.1 (http://www.w3.org/TR/xml-c14n11/) peut également être utilisé.</td></tr>
<tr><td>Avec une signature détachée Manifest</td><td>• L'algorithme de mise en forme canonique exclusif (identifié par l'URI http://www.w3.org/2001/10/xml-exc-c14n#) est utilisé.</td></tr>
<tr><td>Remises bureautiques</td><td>Avec une signature détachée Manifest</td><td>• Pas de mise en forme canonique.</td></tr>
</table>

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 établissements 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

Les « tiers » s'entendent comme 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.

Dans ce cadre, 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)
4, place de Budapest
CS 92459
75 436 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.

SAGE MOA-2 718-GI

Signature numérique de SAGEMOA-2718 -GI
Date : 2018.09.14 14:52:19 +02'00'