Politique de Signature électronique
INTEROP - HOMOLOGATION

Date : 25/01/2019
Version 1.1
Nombre de pages : 10

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 INTEROP », décrit ces conditions dans le cadre des échanges électroniques entre les clients et la Banque de France.

Ce document est destiné :

- À INTEROP (Application et ses gestionnaires Banque de France)
- Aux établissements de crédits et aux clients institutionnels
- Aux transporteurs de fonds mandatés par les établissements de crédits ou clients institutionnels, avec délégation de signature

Dans la suite de ce document, ces établissements seront désignés par le terme « client ». De même, les commandes ou annulations de commande envoyées par voie électronique sont désignés par le terme « commande ».

2. Politique de signature électronique

2.1. Champ d'application

La présente politique de signature s'applique à l'application INTEROP.

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

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

La commande doit être signée par une ou deux personne(s), disposant des droits INTEROP lui permettant d'engager son établissement pour l'ensemble des données transmises.

Chaque fichier remis au format XML fait l'objet d'une ou deux signature(s) électronique(s) et ne concerne qu'une commande.

2.2. Identification

La présente politique de signature est identifiée par l'OID (Object *SignPolicyID*) : **1.2.250.1.115.200.303.1**

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 commande.

2.3. Publication du document

La présente politique est publiée après approbation formelle d'INTEROP et apposition d'une signature électronique issue de la Banque de France.

La présente politique est consultable à l'adresse suivante:

http://www.banque-france.fr/igc/signature/ps/draft_ps_1_2_250_1_115_200_303_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:

INTEROP_assistance@banque-france.fr

Ces remarques et souhaits d'évolution sont examinés par INTEROP 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 INTEROP.

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 après communication officielle de la Banque de France et au plus tard le 01/01/2019, 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 clients 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 clients

Le rôle des représentants des clients, habilités à signer, consiste à :

- apposer la signature électronique du client sur une commande et par là-même autoriser les mouvements au compte du client.
- s'assurer de la mise en œuvre des moyens pour la transmission de la commande auprès de la Banque de France via INTEROP.

Pour apposer une signature électronique sur une commande, les représentants des clients disposent d'un certificat de signature et d'un outil de signature.

- Le certificat de signature doit être enregistré au préalable dans INTEROP
- L'outil de signature, distinct du certificat, est au choix du client.

3.2. Le Responsable d'INTEROP

Le rôle du Responsable d'INTEROP consiste à :

- vérifier la validité de la signature et du certificat utilisé pour signer ;
- vérifier l'habilitation du signataire à engager son établissement pour une commande ;

Le Responsable d'INTEROP 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 du client

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.

Le client 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 du client

Les modalités de choix des représentants du client sont décrites dans les *Conditions Générales d'Utilisation d'INTEROP*. La déclaration du représentant pour signer est réalisée à travers les formulaires transmis par INTEROP Assistance.

3.3.3. Outil de signature utilisé

Le choix de l'outil de signature utilisé par le client est libre dès lors que celui-ci respecte l'implémentation de la présente politique de signature, et notamment la norme de signature XAdES (ETSI TS 101 903) en version v1.3.2 et plus particulièrement les éléments indiqués dans le paragraphe *4.2.2. Norme de signature* ci-dessous.

3.3.4. Type de certificat utilisé

Le représentant d'un client utilise un certificat appartenant à une famille de certificats reconnue :

- Certificats conformes aux normes RGS ** ou RGS *** (Référentiel Général de Sécurité v2.0) ;
- Certificats conformes à la norme QCP-n-QSCD définie par le règlement « eIDAS » (règlement n°910/2014/UE) ;
- Certificats émis par l'Autorité de Certification de la Banque de France.

À partir de 2021, seuls les certificats de Signature Qualifiée (KeyUsage Non-Repudiation) seront autorisés pour signer. Par conséquent, 2 certificats seront nécessaires :

- un certificat d'authentification pour se connecter à Interop (Cf : CGU Interop, §*VI.2 Droits d'accès sur les données et les services*)
- un certificat de Signature Qualifié pour signer les commandes

3.3.5. Protection du support du certificat

Le client prend toutes les mesures nécessaires pour protéger l'accès à son certificat et aux données secrètes associées, notamment le support (carte à puce, dongle, token, …) et le code PIN associé.

3.3.6. Révocation du certificat

En cas de perte, de vol, de compromission ou de simple suspicion de compromission de sa clé privée, le client demande dans les plus brefs délais la révocation de son certificat par l'organisme émetteur et informe INTEROP de la révocation.

3.4. Obligations d'INTEROP

3.4.1. Données de Vérification

Pour effectuer les vérifications, le service de validation de la signature utilisé par INTEROP utilise les données transmises par les clients 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. INTEROP ne saurait être tenu responsable des conséquences d'une validation de signature effectuée pendant ce délai de latence.

3.4.2. Protection des moyens

INTEROP s'assure de la mise en œuvre des moyens nécessaires à la protection des équipements fournissant les services de validation de signature.

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.

3.4.3. Journalisation

INTEROP 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.

INTEROP s'assure que les fichiers de commande signés sont conservés et exploitables pendant 10 ans.

3.4.4. Reprise en cas d'interruption de service

INTEROP 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.

3.4.5. Assistance aux clients

Les clients peuvent s'adresser par courriel à INTEROP pour toute information complémentaire ou pour signaler tout dysfonctionnement à l'adresse suivante :

INTEROP_assistance@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 commande;
- les propriétés de signature telles que définies au paragraphe *4.2.2. Norme de signature* du présent document.

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

Chaque commande étant signée par un ou deux représentant(s), la commande ne contient que les données pour lesquelles le représentant est habilité à engager son établissement.

4.2. Caractéristiques des signatures

Le format de signature suit les préconisations du RGI v2.0 (Référentiel Général d'Interopérabilité) défini par l'Arrêté n° 0095 du 22 avril 2016 et plus particulièrement le format de signature XADES en version 1.3.2 ou supérieure.

4.2.1. Type de signature

Les signatures électroniques apposées par les représentants des clients sont de type « Signature Enveloppante».
Le document signé contient l'ensemble des éléments permettant de valider l'intégrité des données transmises (données, certificats, éléments de contrôles).

4.2.2. Norme de signature

Les signatures respectent la norme XAdES (ETSI TS 101 903) en version v1.3.2 ou supérieure.
Le format XAdES étant un format XML, le jeu de caractères imposé est UTF-8.

Conformément à la norme XAdES, les balises « 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 (*SignaturePolicyIdentifier / SignaturePolicyIdentifierType*) :
  - OID de la présente politique de signature (*SigPolicyId*) ;
  - Valeur de condensé de la politique de signature calculé et algorithme de condensation utilisé (*SigPolicyHash*).

Les paramètres nécessaires à la contre-signature sont dans les balises « propriétés non signées » (*UnsignedProperties / UnsignedSignatureProperties)* de la signature à laquelle elle s'applique.
La contre-signature est définie dans une balise (CounterSignature/CounterSignatureType) et fait référence, selon la norme XAdES, à la signature enveloppante.

- l'identification de contre signature (*CounterSignature*)
- le certificat de contre signature en référence (*Signature*)

La norme XAdES est disponible sur le site W3C : http://www.w3.org/TR/XAdES/

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 le client et INTEROP.

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 exempe, 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.

Pour une signature enveloppante, l'algorithme de mise en forme canonique exclusif est utilisé :
https://www.w3.org/TR/xml-exc-c14n/

4.4. Conditions pour déclarer valide le fichier signé

Un fichier signé est considéré comme valide par INTEROP lorsque les conditions suivantes sont remplies :

- vérification positive de la signature électronique du ou des signataire(s) ;
- vérification positive des habilitations du signataire ;
- vérification du niveau de signature.

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 INTEROP ;
- 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 ;

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.

La collecte des droits relatifs aux représentants est gérée au fil de l'eau par les administrateurs d'INTEROP en fonction des informations fournies par les clients.

5. Politique de confidentialité

5.1. Classification des informations

Les informations suivantes sont considérées comme confidentielles :

- les journaux du service de validation de la signature ;
- les procédures internes du service de validation de la signature ;
- 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 d'INTEROP.
La diffusion des informations à un tiers ne peut intervenir qu'après acceptation d'INTEROP.

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 la Banque de France.

Conformément aux articles 14 et suivants du RGPD, le signataire d'une commande à INTEROP 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 14 et suivants du RGPD, 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 :

Banque de France
Délégué à la Protection des Données
31 rue Croix-des-Petits Champs
75049 PARIS CEDEX 01

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.

SIF-MOA-INTEROP

Signature numérique de SIF-MOA-INTEROP
Date : 2019.02.22 09:38:37 +01'00'