Politique de Signature
du Secrétariat général de la Commission bancaire

Pour les remises de type COREP/FINREP/SURFI et BAFI

Date	**:**	30/06/2009
Version	**:**	2. 0
Nombre de pages	**:**	14

TABLE DES MATIERES

1. Objet du document 4

2. Politique de signature électronique 5

2.1. Champ d'application 5

2.1.1. Cas des remises COREP, FINREP et SURFI 5

2.1.2. Cas des remises BAFI 5

2.2. Identification 5

2.3. Publication du document 5

2.4. Processus de mise à jour 6

2.4.1. Circonstances rendant une mise à jour nécessaire 6

2.4.2. Prise en compte des remarques 6

2.4.3. Information des acteurs 6

2.5. Entrée en vigueur et période de validité 6

3. Acteurs 7

3.1. Les représentants des établissements assujettis 7

3.2. Le Secrétariat Général de la Commission Bancaire 7

3.3. Obligations de l'établissement assujetti 7

3.3.1. Environnement du poste de travail 7

3.3.2. Choix des représentants de l'établissement assujetti 7

3.4. Obligations du représentant d'un établissement assujetti 8

3.4.1. Outil de signature utilisé 8

3.4.2. Type de certificat utilisé 8

3.4.3. Protection du support du certificat 8

3.4.4. Révocation du certificat 8

3.5. Obligations du Secrétariat Général de la Commission Bancaire 8

3.5.1. Données de Vérification 8

3.5.2. Protection des moyens 8

3.5.3. Journalisation 9

3.5.4. Reprise en cas d'interruption de service 9

3.5.5. Assistance aux établissements 9

4. Signature électronique et validation 10

4.1. Données signées 10

4.2. Caractéristiques des signatures 10

4.2.1. Type de signature 10

4.2.2. Norme de signature 10

4.3. Algorithmes utilisables pour la signature 11

4.3.1. Algorithme de condensation 11

4.3.2. Algorithme de chiffrement **11**
4.3.3. Canonicalisation **11**
4.4. Conditions pour déclarer valide le fichier signé 11
4.4.1. Vérification de la signature **11**
4.4.2. Vérification des droits du signataire en fonction de données transmises **11**
5. Politique de confidentialité **12**
5.1. Classification des informations 12
5.2. Communication des informations à des tiers 12
6. Dispositions juridiques **13**
6.1. Données nominatives 13
7. Certificat ayant signé le présent document **14**

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 la Commission Bancaire », décrit ces conditions dans le cadre des échanges électronique entre les établissements assujettis aux remises BAFI et COREP/FINREP/SURFI et le Secrétariat Général de la Commission Bancaire (SGCB).

Ce document est destiné :

- au SGCB ;
- aux établissements assujettis aux remises BAFI et COREP/FINREP/SURFI ;
- aux éventuels prestataires participant à ces échanges pour le compte des assujettis ou du SGCB.

Dans la suite de ce document, les établissements assujettis aux remises BAFI et COREP/FINREP/SURFI sont désignés par le terme « établissement assujettis ».

2. Politique de signature électronique

2.1. Champ d'application

La présente politique de signature s'applique aux remises mentionnées aux paragraphes 2.1.1 et 2.1.2 transmises par les établissements assujettis au SGCB.

Conformément à l'instruction de la Commission Bancaire n° 2007-01, ces remises doivent faire l'objet d'une signature électronique.

2.1.1. Cas des remises COREP, FINREP et SURFI

Ces remises font l'objet d'une signature apposée sur l'intégralité des données transmises.

Cette signature doit être apposée par une personne habilitée à engager son établissement auprès du SGCB pour l'ensemble de données transmises.

Chaque fichier fait l'objet d'une et une seule signature électronique.

2.1.2. Cas des remises BAFI

Les remises objet de la présente politique de signature sont les suivantes :

- les remises réglementaires des états BAFI.

Ces remises font l'objet d'une signature apposée sur l'intégralité des données transmises.

Cette signature doit être apposée par une personne habilitée à engager son établissement auprès du SGCB pour l'ensemble de données transmises.

Chaque fichier fait l'objet d'une et une seule signature électronique.

2.2. Identification

La présente politique de signature est identifiée par l'OID (Object IDentifier) : 1.2.250.1.115.200.300.2

Cette référence doit figurer 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 SGCB 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_2.pdf

2.4. Processus de mise à jour

2.4.1. Circonstances rendant une mise à jour nécessaire

La mise à jour de la présente politique de signature peut avoir pour origines, l'évolution du droit, l'apparition de nouvelles menaces et de nouvelles mesures de sécurité, les observations des différents acteurs, etc.

La présente politique est réexaminée a minima tous les 2 ans.

2.4.2. 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:

sigd.gi@banque-france.fr

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

2.4.3. Information des acteurs

Les informations relatives à la version courante de cette politique et aux versions antérieures sont disponibles sur le site du SGCB où une rubrique documentaire référence toutes les versions précédentes de ce document.

La publication d'une nouvelle version de la politique de signature consiste à

1) 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) archiver la version précédente après apposition de la mention « obsolète » sur chaque page.

2.5. Entrée en vigueur et période de validité

Cette nouvelle version de la politique de signature entre en vigueur le 10 juin 2010 après sa mise en ligne sur le site Internet du SGCB, 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 établissements 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 établissements assujettis

Le rôle des représentants des établissements assujettis est de :

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

Pour apposer une signature électronique sur une remise, les représentants des établissements assujettis doivent disposer 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 SGCB peuvent engager leur établissement pour une remise donnée en y apposant leur signature.

3.2. Le Secrétariat Général de la Commission Bancaire

Le rôle du SGCB est de :

- 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 SGCB 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 le poste de travail du signataire.

L'établissement assujetti doit s'assurer 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'établissement assujetti

Parallèlement à la déclaration sur papier prévue à l'article 3 de l'instruction n° 2007-01, 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. Outil de signature utilisé

Le représentant d'un établissement assujetti doit contrôler 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 doit utiliser un certificat de signature appartenant à une famille de certificats reconnue conformément à l'instruction de la Commission Bancaire n° 2007-01.

3.4.3. Protection du support du certificat

Le représentant doit prendre 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 doit demander 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 la Commission Bancaire

3.5.1. Données de Vérification

Pour effectuer les vérifications, le service de validation utilisé par le SGCB utilise les données transmises par les établissements assujettis concernant les habilitations de leurs représentants, ainsi que des données publiques relatives aux certificats des signataires, telles que les listes de révocations 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 SGCB 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 SGCB 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 SGCB 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 SGCB 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 SGCB 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 SIGD pour toute information complémentaire ou pour signaler tout dysfonctionnement à l'adresse suivante :

sigd.gi@banque-france.fr

4. Signature électronique et validation

4.1. Données signées

Au sein d'un fichier signé, les données signées sont composées des éléments suivants :

- l'intégralité des données constituant la remise BAFI (encodées en base 64) ou COREP/FINREP/SURFI (non réencodées) ;
- les propriétés de signature telles que définies aux paragraphes 4.2.2 du présent document.

Ces deux éléments doivent figurer dans des balises « Object » distinctes, la première balise « Object » contenant les données relatives aux remises.

Les remises signées BAFI et COREP/FINREP/SURFI doivent faire l'objet de fichiers séparés.

Chaque fichier ne devant être signé que par un seul et unique représentant, les fichiers ne doivent contenir 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 doivent donc figurer 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 1.0.

4.2.1. Type de signature

Les signatures électroniques apposées par les représentants des établissements assujettis doivent être de type enveloppantes.

4.2.2. Norme de signature

Les signatures doivent respecter 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) doivent contenir 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 doit plus faire l'objet d'aucun transcodage, et doit transiter 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 SGCB.

4.3. Algorithmes utilisables pour la signature

4.3.1. Algorithme de condensation

Les algorithmes de condensation à utiliser sont SHA-1 ou SHA-256. SHA-256 est à privilégier.

4.3.2. Algorithme de chiffrement

Les algorithmes de chiffrement à utiliser sont RSA-1024 ou RSA-2048. RSA-2048 est à privilégier.

4.3.3. Canonicalisation

- L'algorithme de forme canonique REC-xml-c14n identifié par l'URI http://www.w3.org/TR/2001/REC-xml-c14n-20010315 doit être utilisé comme algorithme de canonicalisation pour les données signées contenues dans la première des balises object (ds : Transform) du paragraphe 4.1 ;
- L'algorithme de forme canonique exclusive xml-exc-c14n identifié par l'URI http://www.w3.org/2001/10/xml-exc-c14n# est préconisé comme algorithme de canonicalisation pour tous les autres usages.

4.4. Conditions pour déclarer valide le fichier signé

Un fichier signé est considéré comme valide par le SGCB 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 SGCB ;
- 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 SGCB 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

On entend par tiers, tout organisme n'étant pas dans la chaîne de traitement des informations du SGCB.

La diffusion des informations à un tiers ne peut intervenir qu'après acceptation du SGCB.

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 plate forme 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 Commission bancaire.

Conformément à l'article 32 de la loi n° 78-17 du 6 janvier 1978, le signataire d'une remise au SGCB est informé que les données à caractère personnel qu'il communique sont utilisées par la plate forme 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 :

Commission Bancaire
Secrétariat Général
SIGD
115 rue Réaumur
BP 6522
75065 PARIS Cedex 02

7. Certificat ayant signé le présent document

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