Direction Générale des Finances Publiques

Politique de Signature électronique Hélios

de la Direction Générale des Finances Publiques (DGFiP)

Pour les flux informatiques transmis par les ordonnateurs des organismes publics locaux à leur comptable conformément au Protocole d'Echange Standard (PES) de l'application Hélios pour l'exécution de leurs recettes et de leurs dépenses

Date : 9 février 2011
Version : 1
Nombre de pages : 10

TABLE DES MATIERES

1. OBJET DU DOCUMENT

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

La présente politique de signature électronique est un document décrivant les conditions de recevabilité par les services de la direction générale des finances publiques (DGFiP) d'un fichier sur lequel sont apposés une ou plusieurs signatures électroniques dans le cadre d'échanges électroniques visés à l'article D.1617-23 du code général des collectivités territoriales.

En vertu de ce dernier article, " *les ordonnateurs des organismes publics, visés à l'article D. 1617-19, lorsqu'ils choisissent de transmettre aux comptables publics, par voie ou sur support électronique, les pièces nécessaires à l'exécution de leurs dépenses ou de leurs recettes, recourent à une procédure de transmission de données et de documents électroniques, dans les conditions fixées par un arrêté du ministre en charge du budget pris après avis de la Cour des comptes, garantissant la fiabilité de l'identification de l'ordonnateur émetteur, l'intégrité des flux de données et de documents relatifs aux actes mentionnés en annexe I du présent code et aux deux alinéas suivants du présent article, la sécurité et la confidentialité des échanges ainsi que la justification des transmissions opérées.*

La signature manuscrite, ou électronique conformément aux modalités fixées par arrêté du ministre en charge du budget, du bordereau récapitulant les mandats de dépense emporte justification du service fait des dépenses concernées et attestation du caractère exécutoire des pièces justifiant les dépenses concernées.

La signature manuscrite, ou électronique conformément aux modalités fixées par arrêté du ministre en charge du budget, du bordereau récapitulant les titres de recettes emporte attestation du caractère exécutoire des pièces justifiant les recettes concernées et rend exécutoires les titres de recettes qui y sont joints conformément aux dispositions des articles L. 252 A du livre des procédures fiscales et des articles R. 2342-4 et D. 3342-11 du présent code ".

Les mesures d'application du premier alinéa de cet article sont portées par l'arrêté relatif à la dématérialisation des opérations en comptabilité publique . L'article 4 de cet arrêté précise :

" *En application de l'article D.1617-23 du code général des collectivités territoriales, la signature électronique des fichiers de données et de documents électroniques transmis au comptable est effectuée par l'ordonnateur ou son représentant au moyen :*

- Soit d'un certificat garantissant notamment son identification et appartenant à l'une des catégories de certificats visées par l'article 6 de l'arrêté du 28 août 2006 pris en application du I de l'article 48 et de l'article 56 du code des marchés publics et relatif à la dématérialisation des procédures de passation des marchés publics formalisés,

- Soit du certificat de signature " DGFiP " délivré gratuitement par la direction générale des finances publiques aux ordonnateurs des organismes publics visés à l'article premier du présent arrêté ou à leurs représentants qui lui en font la demande.

Chaque organisme mentionné à l'article premier du présent arrêté choisit de recourir à l'un ou l'autre de ces certificats ".

Le présent document, " Politique de Signature électronique de la DGFiP/Hélios ", décrit l'ensemble des règles et des dispositions définissant les exigences auxquelles chacun des acteurs impliqués dans ces échanges dématérialisés se conforme pour la transmission et la réception des flux PES, dans le sens aller (ordonnateur > comptable), pour l'exécution des recettes et des dépenses en permettant la dématérialisation des pièces comptables (mandats de dépense, titres de recette et bordereaux les récapitulant).

Ce document est destiné :

- aux collectivités territoriales, à leurs établissements publics et aux établissements publics de santé ;
- aux fournisseurs de ces organismes publics;
- aux éventuels prestataires participant à ces échanges dématérialisés pour le compte de ces organismes publics ;
- aux différents services concernés de la DGFiP.

Dans la suite de ce document :
- les organismes publics susvisés sont désignés par le terme " *collectivités* " ;
- les échanges dématérialisés susvisés sont désignés par le terme " *flux PES aller recette et dépense* ".

2. POLITIQUE DE SIGNATURE ELECTRONIQUE

2.1. Champ d'application

La présente politique de signature s'applique aux flux PES aller recette et dépense, quel que soit le mode de transmission utilisé parmi la liste de ceux autorisés par l'arrêté d'application de l'article D1617-23 du CGCT.

Conformément à cet arrêté, la dématérialisation des flux PES aller recette et dépense requiert l'apposition de la signature électronique de l'ordonnateur de la collectivité concernée ou de son représentant dûment habilité à signer les bordereaux de recette et de dépense.

La signature électronique est apposée au choix de celui-ci :

- sur l'intégralité des données transmises (signature globale et unique couvrant l'ensemble d'un fichier) ;
- sur chaque bordereau de recette et de dépense (signature de chaque pièce comptable).

Chaque élément (le fichier ou le bordereau) fait l'objet d'une unique signature électronique (pas de co-signature, ni de sur-signature).

2.2. Identification

La présente politique de signature est identifiée par l'OID (Object IDentifier) : 1.2.250.1.131.1.5.18.21.1.4.

Cette référence doit figurer dans les données signées conformément au paragraphe 4.2.2 du présent document afin d'attester du régime sous lequel le flux PES aller recette ou dépense est signé.

2.3. Publication du document

La présente politique est publiée suite à son approbation par le Directeur Général des Finances Publiques.

La présente politique et son HASH sont consultables aux adresses suivantes :

- https://portail.dgfip.finances.gouv.fr/documents/PS_Helios_DGFiP.pdf
- https://portail.dgfip.finances.gouv.fr/portail/PS_Helios_DGFiP.pl

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 notamment, l'évolution du droit en vigueur (cf. §1 supra), l'apparition de nouvelles menaces et de nouvelles mesures de sécurité, la prise en compte des observations des différents acteurs.

La présente politique est réexaminée au moins tous les 3 ans.

2.4.2. Prise en compte des remarques

Toutes les remarques, ou souhaits d'évolution, sur la présente politique sont à adresser par messagerie électronique à l'adresse suivante : pole.demat@dgfip.finances.gouv.fr

Ces remarques et souhaits d'évolution sont examinés par la DGFiP 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 à l'adresse indiquée au §2.3 de la présente politique où une rubrique documentaire référence toutes les versions successives 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),
- le hash du document publié ainsi l'algorithme de hashage utilisé.

2) archiver la version précédente après apposition de la mention " obsolète " sur chaque page.

2.5. Entrée en vigueur d'une nouvelle version et période de validité

Une nouvelle version de la politique de signature n'entre en vigueur que 15 jours ouvrés après sa mise en ligne à l'adresse prévue au §2.3, et reste valide jusqu'à l'entrée en vigueur d'une nouvelle version.

Le délai de 3 mois est mis à profit par les collectivités pour prendre en compte dans leurs applications de signature, les changements apportés par la nouvelle politique de signature.

3. ACTEURS

3.1. Le signataire de la collectivité (déterminé au §2.1 supra)

Le rôle du signataire

Le signataire a pour rôle :

- d'apposer sa signature électronique sur le flux PES aller dépense et recette,
- de transmettre les flux PES aller signés au système d'information de la DGFiP selon l'une des deux modalités définies dans l'arrêté d'application de l'article D1617-23 du CGCT. Le choix de la modalité est effectué librement par la collectivité.

Pour apposer une signature électronique sur un flux PES aller recette ou dépense, les signataires s'engagent à utiliser un outil de signature respectant la présente politique de signature. A ce titre, l'identifiant et le hash de cette politique de signature devront figurer dans la signature électronique.

Les obligations du signataire

3.1.1. Outil de signature utilisé

Le signataire doit pouvoir contrôler les données qu'il va signer avant d'y apposer sa signature.

3.1.2. Type de certificat utilisé

e signataire doit utiliser un certificat électronique ayant un usage de signature :

- soit un certificat référencé conformément à l'article 6 de l'arrêté du 28 août 2006 (NOR: ECOM0620009A) pris en application du I de l'article 48 et de l'article 56 du code des marchés publics et relatif à la dématérialisation des procédures de passation des marchés publics formalisés[1].
- soit le certificat de signature délivré à titre gratuit par la DGFiP pour la signature des flux PES aller.

[1] Le référentiel intersectoriel de sécurité et la liste des catégories de certificats de signature électronique mentionnés à l'alinéa précédent sont accessibles à l'adresse suivante : http://www.entreprises.minefi.gouv.fr/certificats/ .
Les certificats sont également accessibles à l'adresse suivante : http://www.telecom.gouv.fr/rubriques-menu/entreprises-economie-numerique/certificats-references-pris-v1/categories-familles-certificats-references-pris-v-1-506.html

Les informations relatives à la signature doivent contenir notamment le nom, le prénom, la qualité du signataire (Maire, chef du service financier…) en application de l'article D.1617-5 du CGCT.

3.1.3. Protection et usage du certificat

Le signataire 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.

Dès lors que le certificat a été accepté et remis au porteur, ce dernier est responsable de la protection de l'accès à son certificat et à la Clé Privée associée.

A ce titre, il s'engage à ne les utiliser :

- qu'en son nom propre,
- uniquement pour des opérations pour lesquelles il a obtenu les pouvoirs de la collectivité (signature électronique des bordereaux de recette et de dépense au format Protocole d'Echange Standard aller recette et dépense, attestation du caractère exécutoire),
- uniquement à des fins de signature,
- uniquement pour des opérations licites.

3.1.4. Révocation du certificat

Le signataire, utilisateur d'un certificat de signature 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.

Le signataire doit aviser le comptable public de la révocation de son certificat par un formulaire dédié à cette opération.

3.2. Les fournisseurs de solutions de signature électronique

La solution doit incorporer, dans la structure des données de signature, la présente politique de signature de la DGFiP publiée à l'adresse indiquée au §2.3 de la présente politique.

3.3. La Direction Générale des Finances Publiques

- Le rôle de la DGFiP

- vérifier la validité de la signature,
- vérifier la période de validité du certificat à la date de la signature,
- vérifier que le certificat est autorisé à signer,
- vérifier que le certificat a bien été délivré par une autorité de certification référencée ou par l'autorité de certification de la DGFiP,
- vérifier la cohérence des données transmises,
- intégrer les données dans Hélios.

- Les obligations de la DGFiP

3.3.1. Données de vérification

Pour effectuer les vérifications, la DGFiP utilise les données transmises par les collectivités concernant les habilitations de leurs représentants, ainsi que des données publiques relatives aux certificats des signataires.

3.3.2. Protection des moyens

La DGFiP s'assure de la mise en oeuvre 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.

3.3.3. Assistance au signataire des collectivités

L'assistance relative à la mise à disposition du certificat électronique de la DGFiP est assurée par l'assistance du Portail de la gestion publique de la DGFiP (voir les coordonnées en page d'accueil de ce site).

L'assistance à l'utilisation du certificat électronique est assurée par le fournisseur de l'outil de signature utilisé.

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 du PES aller recette ou dépense selon la dernière version des spécifications publiées à l'adresse indiquée au §2.3 de la présente politique .

L'empreinte de signature est calculée sur l'ensemble du flux comprenant également les pièces justificatives transmises dans le flux concerné,

- les propriétés de signature telles que définies aux paragraphes 4.2.2 du présent document.

Chaque bordereau ne peut être signé que par un seul et unique représentant. La signature peut être apposée soit au niveau du flux PES aller recette ou dépense, soit au niveau de chaque bordereau dans les conditions prévues dans l'arrêté d'application de l'article D1617-23 du CGCT.

4.2. Caractéristiques des signatures

L'information de signature respecte les spécifications XML Signature du W3C (www.W3.org) ainsi que les extensions de format de signatures spécifiées dans le standard européen XML Advanced Electronic Signature (XADES) de l'ETSI (www.etsi.org).

Les spécifications du PES aller pour la description détaillée du bloc signature sont publiées à l'adresse suivante https://adullact.net/docman/?group_id=552 (document : 100419_H1_3_ET_DOSTEC_SystemeEchangesDonneesPES ALLER_V2.rar, §4.2.2 bloc signature électronique).

Les flux PES aller dépense et recette signés reçus par Hélios doivent respecter les spécifications définies ci dessus. La signature électronique se rapporte aux données du flux PES aller concerné.

4.2.1. Type de signature

Les signatures électroniques apposées par les représentants des collectivités doivent être de type enveloppées.

4.2.2. Norme de signature

Les signatures doivent respecter la norme XAdES-EPES (Explicit Policy based Electronic Signature), ETSI TS 101 903 version v1.2.2.

Conformément à la norme XadES, les propriétés signées (SignedProperties / SignedSignatureProperties) doivent contenir les éléments suivants :

- le certificat du signataire (SigningCertificate)
- le rôle ou qualité du signataire au sein de la collectivité (SignerRole)
- la date et l'heure de signature (SigningTime) au format UTC
- 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)

4.3. Algorithmes utilisables pour la signature

4.3.1 Algorithme de condensation

Cet algorithme est fixé à :
<ds:DigestMethodAlgorithm = "http://www.w3.org/2000/09/xmldsig#sha1"/)

4.3.2. Algorithme de signature

L'algorithme de signature est fixé à :
<ds :SignatureMethod Algorithme = " http://wwww.w3.org/2000/09/xmldsig#rsa-sha1 "/>

4.3.3. Algorithme de canonicalisation

L'algorithme de mise sous forme canonique appliqué à l'élément ds:SignedInfo est fixé à :
<ds:CanonicalizationMethod Algorithm = "http://www.org/2001/10/xml-exc-c14n#"/>

4.4. Conditions pour déclarer valide le fichier signé

Un fichier signé est considéré comme valide par la DGFiP après vérification technique de la signature électronique du signataire.

La vérification de la signature porte sur :

- la vérification du respect de la norme de signature (conformité par rapport aux spécifications du PES aller),
- la vérification de l'appartenance du certificat du signataire à une famille de certificat reconnue par la DGFiP,
- la vérification du certificat du signataire et de tous les certificats de la chaîne de certification :
    - validité temporelle,
    - usage (droit de signature du certificat),
    - signature cryptographique,
- la vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue,
- la vérification de l'identifiant de la présente politique de signature.

5. DISPOSITIONS JURIDIQUES

5.1. Données nominatives

Le porteur dispose d'un droit d'accès, de modification, de rectification et de suppression des données le concernant qu'il peut exercer par courrier du représentant de la DGFiP.

5.2. Droit applicable – Résolution des litiges

Les présentes conditions générales sont soumises au droit français.

Tout litige relatif à la validité, l'interprétation ou l'exécution des présentes conditions générales sera soumis à la juridiction du ressort de l'Autorité de Certification.