Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

DIRECTION GÉNÉRALE DES FINANCES PUBLIQUES
SERVICE DES COLLECTIVITES LOCALES
Sous-direction du conseil fiscal, financier et économique
BUREAU CL-2C – Maîtrise d'ouvrage du secteur public local
7 porte de Neuilly – Maille nord 3
93192 NOISY LE GRAND Cedex

Affaire suivie par Anne POULVELARIE
anne.poulvelarie@dgfip.finances.gouv.fr
☎ 01 58 84 75 84
Référence : DGFiP Bureau CL2C/2016/01/783

Noisy-le-Grand, le 6 janvier 2016

Monsieur,

Dans le cadre de l'exécution budgétaire et comptable des collectivités territoriales et des établissements publics locaux et en particulier de la transmission des fichiers au format du Protocole d'Echange Standard (PES) d'Hélios, vous avez sollicité l'homologation d'un dispositif de télétransmission conformément aux termes du cahier des charges annexé à l'arrêté du 27 juin 2007 du ministre du budget, des comptes publics et de la fonction publique, modifié par l'arrêté du 3 août 2011, portant application de l'article D 1617-23 du code général des collectivités territoriales relatif à la dématérialisation des opérations en comptabilité publique (NOR : BCFR0750735A).

Sur la base du rapport établi par le centre d'évaluation de la sécurité des technologies de l'information (CESTI) que vous avez sollicité et des tests fonctionnels réalisés avec la plate-forme Hélios, j'ai le plaisir de vous informer que le dispositif de transmission dénommé **«S²LOW »** est conforme aux exigences du cahier des charges annexé à l'arrêté du 27 juin 2007 du ministre du budget, des comptes publics et de la fonction publique, modifié par l'arrêté du 3 août 2011, portant application de l'article D 1617-23 du code général des collectivités territoriales.

Cette homologation, délivrée pour une période de cinq années, est prononcée au profit des éléments suivants : **dispositif de télétransmission S²LOW de l'ADULLACT, utilisant la solution TéDéTis**

Dans ce prolongement, et conformément aux dispositions de l'arrêté ministériel précité, je vous invite, en tant que responsable de la mise en œuvre opérationnelle et de l'exploitation du dispositif **«S²LOW »**, à signer la convention de raccordement jointe en double exemplaire au présent courrier, et à me retourner un exemplaire.

Je vous remercie de l'intérêt que vous avez porté à la modernisation de l'exécution budgétaire et comptable dans le secteur public local et je souhaite que le dispositif **«S²LOW »**, puisse contribuer pleinement à la transmission des flux PES d'Hélios des collectivités et établissements publics locaux.

Monsieur Pascal KUCZYNSKI
Directeur Technique ADULLACT
836 rue du Mas de Verchant
Bât le Tucano
34000 MONTPELLIER

L'Administrateur Civil,
Chef du Bureau CL2 C

Etienne ERASIMUS

MINISTÈRE DES FINANCES
ET DES COMPTES PUBLICS

Convention de raccordement

entre l'opérateur d'un dispositif de télétransmission homologué et le ministère des finances et des comptes publics

En application des dispositions de l'arrêté du ministre du budget, des comptes publics et de la fonction publiques aux collectivités territoriales du 27 juin 2007 portant approbation d'un cahier des charges de télétransmission avec Hélios et fixant une procédure d'homologation, l'opérateur du dispositif de télétransmission homologué **S²LOW de l'ADULLACT**, **utilisant la solution TéDéTis** s'engage, par la présente convention, à respecter les clauses qui suivent :

1. L'opérateur vérifie que dans chaque fichier transmis respecte les règles de transfert de fichier décrites en annexe de ce document.

2. L'opérateur doit assurer, au sein de son infrastructure, la protection en confidentialité des secrets d'identification et d'authentification au serveur du ministère des finances :
   - L'identifiant et le mot de passe ;
   - L'adresse IP fixe, dédiée au dispositif unique et utilisées par les machines depuis lesquelles ledit dispositif dépose les fichiers ;
   - La protection de la clé privée associée au certificat d'authentification du dispositif.

Toute divulgation ou suspicion d'atteinte à la confidentialité de ces éléments est de nature à favoriser l'usurpation d'identité du dispositif. L'opérateur, par son organisation et les mécanismes de sécurité mis en œuvre dans son système, devra être en mesure de détecter ces évènements. En cas de survenance, il en informera immédiatement les équipes techniques du ministère des finances.

Le mot de passe attribué au dispositif pour le raccordement au système mis en place par du ministère des finances doit être changé régulièrement, à l'initiative du ministère. Si l'opérateur souhaite changer l'adresse IP depuis laquelle son dispositif se connecte, il doit en faire la demande aux équipes techniques du ministère avec un délai préalable de 15 jours.

3. L'opérateur (fournisseur de dispositif de télétransmission et exploitant de ce dispositif) doit tenir compte des recommandations de la norme ISO/IEC 177999 (BS-7799) concernant la préservation de :
   - La confidentialité ;
   - L'intégrité des informations ;
   - La disponibilité du dispositif.

L'application des recommandations de ladite norme doit se traduire dans :

- L'application de la documentation de mise en œuvre et d'exploitation du dispositif ;
- La politique de sécurité ;
- Le signalement de la gestion des incidents et leur consignation dans les journaux.

4. L'opérateur devra veiller à ce que l'authentification des collectivités repose sur l'utilisation de certificats ; ces certificats devront être conforme au Référentiel Général de Sécurité (RGS) prévu par l'ordonnance n° 2005-1516 du 8 décembre 2005, dès publication officielle du RGS. Il devra être capable d'accepter, notamment, les certificats référencés par l'arrêté du 15 juin 2012 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. La liste de ces certificats est consultable à l'adresse électronique suivante sur internet : http://www.lsti-certification.fr/index.php/signature-electronique.html
5. L'opérateur devra contrôler la validité du certificat d'authentification utilisé par une collectivité au regard de la liste de révocation mise à disposition par l'Autorité de Certification.

6. L'opérateur doit être en mesure de fournir, à la demande de la DGFIP, la liste (telle que définie dans le paragraphe 3.4.2 du cahier des charges de télétransmission avec Hélios) des documents transmis sur une période donnée. Cette liste fera l'objet d'un archivage sur une période minimale de 8 ans.

7. Les services techniques de la DGFIP doivent pouvoir, en tant que de besoin, prendre contact avec les responsables de l'exploitation du dispositif de télétransmission, afin de mettre en œuvre ponctuellement des mesures de limitation des flux (limitations du volume de données transmis, en nombre de mega-octets par heure) émis vers la plate-forme du ministère. La prise en compte de ces limitations par l'opérateur doit être faite dans les quatre heures suivant la demande (en heures ouvrables).

8. L'opérateur du dispositif de télétransmission doit être en mesure de gérer les éventuels incidents de fonctionnement survenant dans sa sphère en garantissant aux utilisateurs de son système une assistance. Il doit traiter et faire son affaire des demandes desdits utilisateurs et ne peut les renvoyer vers le ministère.

   Les sollicitations réciproques entre les équipes techniques du ministère et l'opérateur se feront par voie de messagerie. L'opérateur fournit aux équipes techniques du ministère, une fois la présente convention signée, une adresse de messagerie :

   - Qui sera la seule adresse d'expéditeur autorisée quand l'opérateur sollicitera les équipes techniques du ministère ;
   - Qui sera l'adresse qu'utilisera le ministère pour solliciter l'opérateur.

   L'opérateur s'engage à ne pas solliciter les équipes du ministère dans d'autres conditions, et à exploiter les messages envoyés par le ministère à l'adresse susmentionnée.

   L'opérateur ne peut solliciter les équipes techniques du ministère que :

- en cas de problème de transmission de fichier entre le dispositif et la plate-forme de traitement des flux PES d'Hélios. Préalablement à la sollicitation du ministère, l'opérateur s'engage à effectuer les opérations de diagnostic nécessaires permettant de s'assurer que le problème vient de la plate-forme Hélios, et permettant de transmettre les éléments d'information nécessaires au diagnostic de l'incident par le ministère. Le ministère répond alors dans les 4 heures en jours ouvrés ;
- en cas d'indisponibilité des serveurs du ministère ;
- en cas de problème ou de sollicitation liée à la sécurité des échanges (changements de mots de passe, etc.) ;
- dans tous autres cas explicitement prévus par le cahier des charges d'homologation ou dans le présent document.

Le ministère des finances pourra utiliser l'adresse de messagerie précitée de l'opérateur pour lui communiquer des avis de maintenance, des informations générales sur la télétransmission des flux, des demandes de régulation de flux, des demandes liées à la mise en œuvre des obligations du cahier des charges et de la présente convention.

L'opérateur s'engage à ne pas diffuser les coordonnées du service technique du ministère.

L'opérateur s'engage à fournir aux collectivités des conditions d'intervention prévoyant des garanties de temps d'intervention (GTI) de l'ordre de 4 à 6 heures, et des garanties de temps de rétablissement (GTR) n'excédant pas 8 heures pour le matériel les jours ouvrables.

9. L'opérateur doit garantir la maintenance technique de son dispositif et assurer une adaptation aux évolutions du cahier des charges de la télétransmission.

10. Le dispositif de transmission ne doit pas conduire à exploiter des données à caractère personnel détenues dans le cadre de la transmission. Si, le dispositif utilise des données, collectées dans le cadre de la transmission des données et documents électroniques, pour des usages ou des traitements ayant un objet autre que la seule transmission, et si ces données incluent des données nominatives personnelles, ces usages et traitements doivent faire l'objet d'une déclaration spécifique auprès de la CNIL conformément aux dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cette obligation est rappelée dans la convention de raccordement signée par l'opérateur de transmission

11. L'opérateur s'engage à effectuer les mises à jour nécessaires aux outils de protection contre les intrusions et les codes malveillants dont le dispositif doit être doté.

12. Interruptions programmées du service.

L'opérateur s'engage à adapter sa capacité de stockage afin de pouvoir stocker des actes transmis par les collectivités, sans pouvoir les transmettre à la plate-forme du ministère, pendant 2 jours ouvrés. Quel que soit l'état de disponibilité du service d'échange d'Hélios, les fonctionnalités du dispositif de transmission doivent rester accessibles à la collectivité territoriale ou à l'établissement public local.

13. L'opérateur s'engage à respecter les mesures et protocoles décrits dans la documentation de mise en œuvre et d'exploitation du dispositif qu'il doit présenter afin de garantir la mise en œuvre intégrale dudit dispositif sans altération.

14. Si l'opérateur ne respecte pas ses engagements, le ministère peut suspendre temporairement ou définitivement le raccordement de son dispositif, et rapporter la présente convention.

Le dispositif de télétransmission **S²LOW de l'ADULLACT, utilisant la solution TéDéTis** ayant souscrit aux engagements ci-dessus mentionnés, il est convenu de raccorder ledit dispositif à l'application Hélios du Ministère des finances à compter de janvier 2016

Le

Le 6 janvier 2016

Monsieur Pascal KUCZYNSKI
Directeur Technique
ADULLACT

Etienne ERASIMUS
Administrateur Civil
Chef du Bureau CL2C

ANNEXES

Annexe 1 : règles de transfert des fichiers

1.2. Introduction

Les données comptables au format PES v2 sont transmises de la plate-forme du TdT vers Hélios via CFT ou FTP.

Quatre types de flux sont échangés :

Du TdT vers Hélios :

- PES_Aller : Flux contenant les informations comptables de l'ordonnateur.

D'Hélios vers le TdT :

- PES_Acquit : Flux renvoyer à l'ordonnateur après la prise en compte d'un flux PES_Aller,
- PES_NonAcquit : Flux renvoyer à l'ordonnateur en cas de rejet d'un flux PES_Aller,
- PES_Retour : Flux contenant des informations comptables en réponse à un flux PES_Aller.

Remarque : La documentation du PES v2 est disponible à l'adresse suivante :

http://adullact.net/docman/index.php?group_id=552&selected_doc_group_id=1063&language_id=1

1.3. Routage des fichiers depuis la plate-forme du TdT vers Hélios

Les fichiers contenant flux PES_Aller doivent respecter la règle de nommage suivante :

PESALR2_*idColl*_*date*_*numOrdre*.xml avec :

- *idColl* : numéro siret de la collectivité,
- *date* : date d'envoi sous la forme AAMMJJ,
- *numOrdr* : numéro d'ordre d'envoi sur 3 positions.

Quelque soit le protocole utilisé le routage d'un fichier contenant un flux PES_Aller vers Hélios nécessite l'initialisation du paramètre CFTPARM sous la forme suivante :

```
Dans le cas d'un TDT CFT

CodeFich#CodColl#IdPost#CodBud
```

Avec :

- CodeFich : PESALR2,
- CodCol : code collectivité,
- IdPost : Identifiant du poste comptable,
- CodBud : code budget.

Le caractère « # » est le séparateur qui permet à Hélios de repérer les champs.
Les informations CodColl, IdPost et CodBud peuvent être obtenues en utilisant une expression xPath sur le flux PES_Aller :

- CodCol : /PES_Aller/EnTetePes/CodCol,
- IdPost : /PES_Aller/EnTetePes/IdPost
- CodBud : /PES_Aller/EnTetePes/CodBud

Chaque flux PES_Aller contient une balise <NomFic> (xPath : /PES_Aller/Parametres/NomFic) dont le contenu doit être unique pour une collectivité car il permet de faire le lien entre le PES_Aller et le flux PES_Acquit ou PES_NonAcquit en fonction du cas.

Dans le cas d'un TDT FTP

Seul le nom du fichier doit être passé en CFTPARM

1.4. Routage des fichiers depuis Hélios vers la plate-forme du TdT

La plate-forme du TdT doit être configurée pour recevoir d'Hélios des flux PES_*Acquit, PES_NonAcquit* et *PES_Retour* qui doivent être ensuite transférées aux collectivités. Il existe deux méthodes de routage selon la nature du flux.

1.4.1. *_PES_Acquit et PES_NonAcquit*

Lorsque le fichier PES_Acquit transmis par Hélios est récupéré par le TdT, ce dernier procède à l'extraction du paramètre ***NomFic*** en utilisant le xpath suivant :

- //Envelope/Parametres/NomFic

La correspondance doit être établie entre le ***NomFic*** du flux PES_Aller et le ***NomFic*** du flux PES_Acquit ou PES_NonAcquit selon le cas. à partir de ce **nomFic** de telle sorte que le PES_Acquit puisse être routé vers l'émetteur initial du PES_Aller.

1.4.2. PES_Retour

- **Définition des PES_Retour**

Le flux PES_Retour est un fichier transmis d'Hélios vers l'ordonnateur. Les données véhiculées sont relatives à un budget/collectivité unique. Un flux PES_Retour peut combiner des données issues de différents domaines (Dépense, Recette, Rôle, Budget, Etat de l'actif, Marche, Etat du passif). Ce flux permet au comptable de transmettre des informations à la collectivité qu'il administre (états de versement, demande d'émission de mandat, etc.). S'il peut parfois être associé à un flux PES_Aller fonctionnellement, il n'est jamais lié techniquement à un flux PES_Aller. Il n'y a donc aucune correspondance possible entre un flux PES_Aller et un flux PES_Retour.

- **Mise à disposition de la collectivité**

Un flux PES_Retour n'est destiné qu'à une unique collectivité. La collectivité destinatrice peut être déterminée à l'aide du paramètre IdColl.

L'IdColl se trouve :

- Dans le PES_Retour : Enveloppe\EnTetePES\IdColl.

1.4.3. Contrôles à effectuer sur les flux en provenance d'Hélios

- **Contrôle du destinataire**

Si le destinataire du flux PES_Retour n'est pas connu ou n'est pas abonné au service du TdT, il faut envoyer un mail de notification d'erreur aux agents du poste comptable à l'initiative du *PES_Retour*. Cet émetteur est défini par le paramètre *IdPost* qui se trouve :

- Dans le *PES_Retour* : Enveloppe\EnTetePES\IdPost

- **Les messages d'erreur adressés seront les suivants**

Abonné non inscrit
« La collectivité <nom de la collectivité> n'est pas abonnée à l'application *Comptabilité Publique* du TdT, elle n'est donc pas autorisée à recevoir le *PES_Retour* <NomFic> envoyé le <date d'envoi> »

Annexe 2 : Paramètres des protocoles de transferts : FTP et PESIT

Une fois la convention de raccordement signée, la DGFIP fournira au TdT les informations suivantes :

- Identifiant et mot de passe CFT de la collectivité,
- Les codes destinataires CFT d'Hélios (transmis en temps voulu par les équipes compétentes)

  Remarque : chaque collectivité est gérée par un Poste Comptable. Chaque Poste Comptable est associée à un site Hélios particulier.
- L'identifiant CFT des flux Hélios (IDF)
- Pour le PESV2 : GHELPES2.

L'envoi par FTP est décrit dans le document ANX-AX-07-8050-R001-Parametre-FTP.doc

Annexe 3 : Formulaire de déclaration d'Interconnexion Hélios/Partenaire

Cf. fichier ANX-AX-07-8049-R002-Lan2Lan-Partenaires.doc

Annexe 4 : Complément à l'exigence 2.13 du cahier des charges

Rappel de l'exigence 2.13 :
Pour les transmissions d'information en provenance des organismes publics locaux, le dispositif comprend des mécanismes garantissant la confidentialité et l'intégrité des données de la collectivité ou de l'établissement au cours de la transmission.

A titre de recommandation et conformément au Référentiel Général d'Interopérabilité, les protocoles suivants peuvent être utilisés : TLS 1.0 et SSL 3.0, IPSEC.

Mise en œuvre de HTTP et FTP sur SSL :

- RFC2246 : TLS Transport Layer Security : TLS v1.0,
- SSL Protocol version 3 (spécification Netscape),
- RFC2818 : HTTP over TLS.

Les tailles des clés utilisées seront de 128 bits minimum.

Suite de chiffrement SSL V3.0 :

- SSL RSA RC4 128 bits MD5,
- SSL RSA RC4 128 bits SHA,
- SSL RSA 3DES (EDE CBC) SHA.

Suite de chiffrement TLS v1.0 :

- TLS RSA RC4 128 bits MD5
- TLS RSA RC4 128 bits SHA
- TLS RSA 3DES 168 bits (EDE CBC) SHA
- TLS RSA AES 128 bits (CBC) SHA
- TLS RSA AES 256 bits (CBC) SHA

Mise en œuvre d' IPSEC :

IPSEC SA :

- 3DES-MD5
- 3DES-SHA1

IKE :

- 3DES-MD5
- 3DES-SHA1