

PARIS, le 29/07/2002

DIRECTION DES SYSTEMES
D'INFORMATION DU RECOUVREMENT
DISIR

LETTRE CIRCULAIRE N° 2002-173

OBJET : Procédure « e-mail sécurisé » pour la transmission des déclarations et paiements EDI.

Pour garantir l'authentification et l'identification des déclarations et paiements EDI, transmis par e-mail, il apparaît aujourd'hui nécessaire de faire évoluer la procédure actuelle, et de mettre en place une nouvelle procédure, dite « e-mail sécurisé ».

Cette procédure est applicable à toute nouvelle adhésion à la DUCS EDI. Les entreprises déjà adhérentes à la DUCS EDI, disposeront d'un délai pour faire évoluer leur procédure de transmission.

Après plus de trois années d'exploitation, la procédure de transmission, via e-mail, des télédéclarations et téléversements EDI, enregistre aujourd'hui 15 900 comptes.

L'augmentation sans cesse croissante des flux de déclarations et paiements transmis via Internet (plus de 30 % en un an), a conduit l'ACOSS à renforcer les conditions de sécurité dans lesquelles s'effectue cette transmission, dans l'intérêt des déclarants et des Organismes.

Une procédure technique dite « e-mail sécurisé » a été mise au point par le CERTI de LILLE, pôle de compétence des téléprocédures dans la Branche Recouvrement.

Par ailleurs, des travaux sont en cours avec la Mission DUCS dans le but d'intégrer et d'harmoniser ces dispositions, dans le Cahier des Normes et Recommandations de la DUCS EDI.

Il est demandé aux URSSAF de veiller à la mise en œuvre de cette procédure pour les transmissions par messagerie Internet des déclarations et paiements qui leur sont destinés, selon les modalités décrites au paragraphe IV – Modalités de déploiement.

Cette lettre circulaire a pour objectif de présenter aux URSSAF la procédure définie en précisant :

- le contexte et le champ d'application,
- le mode opératoire prévu pour sa mise en œuvre,
- les modalités de son déploiement.

Elle fait suite aux formations effectuées aux URSSAF d'appui téléprocédures en Octobre 2001 au CIRSO de TOULOUSE et en Mars 2002 à l'ACOSS.

I - CONTEXTE

Les solutions de sécurisation basées sur la certification électronique, s'inspirent des travaux menés par le Ministère de l'Economie, des Finances et de l'Industrie (MINEFI), dans le cadre du lancement de l'offre « Télé-tva ».

Le MINEFI a basé la stratégie de dématérialisation de ses offres, sur la certification électronique, en rendant obligatoire, la téléprocédure « Télé-tva » ainsi que l'utilisation d'un certificat électronique, pour toutes les entreprises payant plus de 15 millions d'euros de TVA par an.

Pour cela, le MINEFI a mis en place une politique dite « de référencement ».

Cette politique définit les critères de sécurité que doit respecter tout organisme ou instance souhaitant devenir « autorité de certification », et être ainsi référencé par le MINEFI, de façon à pouvoir distribuer des certificats auprès des entreprises.

Aujourd'hui plusieurs autorités de certification (essentiellement des organismes bancaires), sont référencées par le MINEFI et distribuent des certificats auprès des entreprises adhérentes à « Télé-tva ».

Le Recouvrement s'est inscrit dans ces travaux en permettant aux entreprises disposant d'un tel certificat, de l'utiliser également pour certaines de ses téléprocédures, dans le cadre de transmissions de fichiers.

Des tests techniques avec chacune des autorités de certification ont validé la capacité pour nos serveurs de messagerie Internet, à recevoir des fichiers cryptés et signés à l'aide du certificat électronique qu'elle délivre.

Si, sur le plan de la sécurité des données transmises, ces certificats offrent de bonnes garanties permettant notamment l'authentification de l'émetteur, ils ne peuvent comme c'est le cas dans la procédure « Télé-tva », garantir la sécurité juridique de l'échange. Cette sécurité juridique ou garantie de non-répudiation, peut constituer une prochaine étape, qui sera atteinte avec l'adoption et la publication de la politique de référencement de la branche.

Des travaux visant à établir cette politique ont en effet été engagés par le GIP-MDS à la demande de l'ACOSS et devraient aboutir avant la fin 2003.

Compte-tenu des enjeux pour la branche et des risques inhérents aux transmissions par Internet, l'ACOSS a souhaité mettre en œuvre une première solution technique de sécurisation sans attendre l'achèvement de ces travaux.

II – CHAMP D'APPLICATION

Dans un premier temps, seules les téléprocédures EDI sont en mesure d'accepter les certificats d'entreprises obtenus auprès des autorités de certifications référencées par le MINEFI.

A - Téléprocédures visées

Ces téléprocédures EDI reposent sur les formats de fichiers suivants :

- DUCS EDI au format Copaym ou Coplat,
- BRC Magnétique, utilisés principalement par les VLU.

A terme, il est prévu d'élargir ce dispositif de sécurisation aux services DUE-EDI, et aux services de déclarations et paiements, accessibles via www.urssaf.fr, sous la rubrique « calculer,déclarer et payer par Internet ».

Pour les téléprocédures interactives, l'utilisation du mot de passe associé au siret de l'adhérent, offre aujourd'hui, de bonnes garanties d'identification et d'authentification.

Toutefois, il convient de rappeler aux adhérents qu'ils doivent régulièrement modifier ce mot de passe, afin de limiter tout risque d'usurpation de ce dernier.

B - Adhérents concernés

La procédure « e-mail sécurisé » s'applique et couvre l'ensemble des adhérents potentiels de la DUCS EDI, et des utilisateurs du BRC magnétique.

Les adhérents à la DUCS EDI, actuellement recensés et pouvant avoir recours à un certificat électronique pour la transmission des déclarations et des paiements sont :

- l'entreprise transmettant directement ses fichiers ;
- le tiers rédacteur (expert comptable ou société de services, autres...) ;
- le relais ou portail de communication : (jedeclarare.com, coala).

Le certificat, est alors délivré à l'adhérent à la DUCS EDI, ou à l'utilisateur du BRC magnétique, émetteur des déclarations et paiements vers l'URSSAF : entreprise, tiers-rédacteur, relais de communication, portail...

III - MODE OPERATOIRE

Le mode opératoire se décline en quatre étapes :

- 1 - Acquisition par l'entreprise d'un certificat électronique,
- 2 - Installation par l'entreprise du certificat,
- 3 - Mise à jour par l'URSSAF des données d'adhésion dans GESUR,
- 4 - Configuration du gestionnaire de messagerie par l'entreprise pour la transmission des déclarations et des paiements.

3.1 Acquisition par l'entreprise d'un certificat électronique

L'entreprise qui produit un fichier de télédéclaration et de télérèglement au format DUCS EDI, ou BRC magnétique, et souhaite le transmettre à l'URSSAF par « e-mail sécurisé » doit tout d'abord acquérir ou obtenir un certificat électronique d'identité pour chaque personne habilitée par l'entreprise à effectuer les transmissions via e-mail.

A - Certificat de type « MINEFI »

L'acquisition d'un certificat électronique peut se faire auprès d'une des autorités de certification référencées par le MINEFI, et dont la liste est publiée à partir de la page d'accueil des services Teledep, (<https://www.declaration.urssaf.fr>), sous la rubrique « e-mail sécurisé En savoir plus ». (2^{ème} point)

A l'heure actuelle, ces autorités de certification sont essentiellement des banques, établissements financiers, ou chambres de commerce à couverture nationale, et disposant d'un réseau d'agences locales pour distribuer auprès des entreprises les certificats électroniques.

L'entreprise s'adresse alors à l'agence ou l'organisme le plus proche de son siège.

Ce certificat payant, dont le prix est estimé en moyenne, autour de 50 euros, selon les fournisseurs, a une portée universelle (fisc, banques, URSSAF).

B - Alternative au certificat électronique payant

Dans l'hypothèse où l'entreprise, préalablement informée par l'URSSAF des risques liés à la non-authentification du message, ne peut ou ne souhaite pas avoir recours aux services d'une autorité de certification, l'URSSAF peut lui proposer une alternative.

Il revient alors au déclarant de décider de l'une ou l'autre des deux solutions suivantes :

- certificat « recouvrement »,
- transmission via le logiciel « Efi-Micro ».

B1 - Certificat « recouvrement »

L'URSSAF pourra mettre gratuitement à disposition de l'entreprise un certificat électronique « recouvrement », valable uniquement pour les déclarations et paiements URSSAF, pour une durée de un an, renouvelable.

Pour délivrer ce certificat à l'entreprise, l'URSSAF devra accomplir les mises à jour suivantes au niveau de l'application Gesur :

- Dans un premier temps, l'URSSAF enregistre sur Gesur, le nom et les habilitations de l'utilisateur,
- l'URSSAF positionne ensuite une autorisation à faire des « edi sécurisé »,
- La prise en compte de cette autorisation entraîne la création d'un mot de passe, que l'URSSAF communique au déclarant.

Ce mot de passe permettra à l'entreprise d'obtenir et d'installer le certificat électronique « recouvrement ».

B2 - Transmission via le logiciel EFI – MICRO

L'autre solution de sécurisation pouvant être proposée à l'entreprise consiste à remplacer la transmission par messagerie Internet par un autre mode de transmission, en utilisant le logiciel EFI-MICRO.

Cette alternative de nature différente de la certification électronique, apporte toutes les garanties en matière d'authentification de l'émetteur.

Cette solution ne remet pas en cause les principes de fonctionnement de la DUCS EDI, puisqu'elle conduit simplement à intervenir sur le mode de transmission à l'URSSAF sans modifier le contenu ni la structure du fichier.

L'URSSAF proposera ainsi le logiciel EFI-MICRO dont la dernière version a été diffusée en Mars 2002 et assure la compatibilité avec les formats DUCS EDI et BRC magnétique.

Cette dernière solution implique que l'entreprise installe sur un poste de travail le logiciel fourni par l'URSSAF.

Avec ce logiciel, l'entreprise pourra importer de sa paie, le fichier DUCS EDI ou BRC magnétique, et utiliser la fonction de transmission pour l'adresser par une connexion directe au serveur Teledép du Recouvrement, sans transiter via Internet.

3.2 - Installation par l'entreprise du certificat

A - Certificat MINEFI

Lorsque l'entreprise a acquis son certificat auprès d'une autorité de certification, elle effectue les procédures d'installation et de paramétrage de messagerie selon les modalités techniques prévues par chacune des autorités de certification, et avec son assistance technique.

B - Certificat « recouvrement »

Pour installer le certificat recouvrement, l'entreprise munie du mot de passe (délivré par l'URSSAF, lors de l'enregistrement de l'autorisation à faire des edi sécurisés), et de son siret accède à la page suivante : <https://www.declaration.urssaf.fr/certif> .

Cette page contient l'ensemble des instructions permettant à l'entreprise d'installer, par téléchargement, le certificat recouvrement, dans le logiciel de messagerie.

Il appartient à l'URSSAF, le cas échéant, d'assurer l'assistance technique relative à cette opération. Les URSSAF d'appui téléprocédures ayant reçu les formations portant sur ce point, sont susceptibles d'être sollicitées, par les URSSAF.

3.3 - Mise à jour par l'URSSAF des données d'adhésion dans GESUR

D'une manière générale, les modalités d'adhésion de l'entreprise sont inchangées et s'appuient sur le bulletin d'adhésion qu'elle retourne à l'URSSAF en y joignant éventuellement une autorisation pour le télérèglement.

Sur ce bulletin d'adhésion, l'entreprise désigne le ou les utilisateurs qui pratiqueront effectivement la télédéclaration et qui doivent être en possession d'un certificat électronique d'identité.

L'URSSAF enregistre alors dans Gesur le nom des utilisateurs tels qu'ils figurent sur le bulletin. Cet enregistrement effectué, les utilisateurs sont alors habilités à transmettre des e-mails comportant en pièces jointes les fichiers de déclarations et de paiement.

Concernant les portails de communication, il convient de préciser que les utilisateurs de portail n'ont pas à obtenir de certificat électronique, puisque le portail assure la sécurisation de l'échange avec son propre certificat électronique.

Lors de l'adhésion, l'utilisateur du portail indiquera à l'URSSAF, qu'il transmet ses fichiers via un portail de communication, en le mentionnant, sur le bordereau.

Des travaux sont en cours avec la Mission DUCS afin de prendre en compte ces évolutions sur le bordereau d'adhésion à la DUCS – EDI. Des précisions seront apportées prochainement sur ces travaux ainsi que sur la procédure d'adhésion applicable aux portails.

3.4 - Configuration du gestionnaire de messagerie par l'entreprise pour la transmission

A - Configurations du gestionnaire de messagerie

Pour les deux types de certificat (MINEFI et recouvrement), les configurations nécessaires à l'utilisation de la procédure « e-mail sécurisé », sont décrites sur la page suivante :

<https://www.declaration.urssaf.fr>, sous la rubrique « e-mail sécurisé »
En savoir plus « (3^{ème} point) ».

L'entreprise devra également rendre actives, les options de chiffrement et de signature au niveau de son gestionnaire de messagerie Internet.

Pour les entreprises adhérentes à la DUCS EDI, ces options sont applicables uniquement aux transmissions destinées au Recouvrement. Ces options de messagerie ne doivent pas, pour l'instant, être activées pour les envois vers l'Assedic et la Caisse retraite complémentaire.

Des précisions complémentaires seront communiquées sur ce sujet selon les instructions que fournira la Mission DUCS.

B - Transmission des fichiers

Pour les transmissions sécurisées, le Recouvrement a mis en place 2 nouvelles boîtes aux lettres, (Envois en réel, envois en test) pour chaque format de fichier utilisé.

	Envois réels	Tests
Format Copaym	copaym.s@declaration.urssaf.fr	testcopaym.s@declaration.urssaf.fr
Format Coplat	Coplat.s@declaration.urssaf.fr	testcoplat.s@declaration.urssaf.fr
Format BRC magnétique	brc.s@declaration.urssaf.fr	testbrc.s@declaration.urssaf.fr

C - Traitement des fichiers

Les fichiers reçus, sont traités par Teledép qui vérifie les signatures et les habilitations des émetteurs en fonction des informations entrées par le Gesur. Les déclarations et les paiements sont enregistrés dans la base de donnée de l'URSSAF, et un accusé de réception est délivré au cotisant.

Ces déclarations et paiements sont traités au même titre que ceux émanant d'autres téléprocédures, c'est à dire qu'ils restent modifiables par le cotisant jusqu'à la date limite et seront alors extraits pour être transmis au SNV2, aux banques. L'URSSAF peut suivre le traitement de chaque e-mail grâce au Gesur EDI.

IV – MODALITES DE DEPLOIEMENT

Pour faciliter le déploiement de cette procédure, l'ACOSS a décidé de mettre en œuvre des actions d'accompagnement auprès des URSSAF et des CERTI.

A - Mise en œuvre d'un plan d'accompagnement au niveau national

Un plan d'actions comprenant :

- des formations techniques et fonctionnelles auprès des URSSAF et des CERTI,
- l'élaboration de guides d'information et d'utilisation,
- l'élaboration d'outils de communication

est en cours de définition par un groupe de travail composé de représentants de l'ACOSS, du CERTI de LILLE, et des URSSAF.

Les URSSAF seront tenues informées très prochainement par leur URSSAF d'appui, des modalités de mise en œuvre de ce plan d'actions.

B - Cas des entreprises déjà adhérentes à la DUCS EDI

Les cotisants ou tiers-déclarants déjà adhérents à la DUCS EDI via Internet devront avoir mis en œuvre un des modes de sécurisation proposés par cette procédure au plus tard au 01-03-2003. Le dispositif étant déjà opérationnel, les URSSAF peuvent contacter ces entreprises afin de les inciter à utiliser la procédure « e-mail sécurisé », dès réception de la présente lettre circulaire.

C - Cas des nouvelles adhésions

La procédure « e-mail sécurisé » s'applique à toute nouvelle adhésion d'une entreprise ou d'un tiers déclarant souhaitant transmettre ses déclarations par messagerie Internet.

D - Expérimentations avec les autorités de Certification

Dans le cadre de la mise en œuvre de la solution de sécurisation des EDI via Internet, le Recouvrement a organisé, au niveau national, différentes rencontres avec les autorités de certification, référencées par le MINEFI, afin d'envisager une montée en charge des télédéclarations et des télépaiements via messagerie Internet.

Ces rencontres ont été l'occasion de définir un premier niveau de déploiement de cette nouvelle procédure de transmission via Internet.

→ Communication sur la compatibilité du certificat avec l'URSSAF.

En accord avec l'ACOSS, la communication faite auprès des entreprises par les autorités de certification, mentionnera la compatibilité du certificat de cette autorité, avec les téléprocédures du Recouvrement (EDI).

Cette démarche devrait renvoyer vers l'URSSAF les entreprises ayant acquis un certificat et souhaitant adhérer à la procédure DUCS EDI ou BRC magnétique, selon la situation de l'entreprise.

→ URSSAF d'appui téléprocédures.

Les premières expérimentations et démarrages concerneront les URSSAF d'appui Téléprocédures. La liste de ces URSSAF d'appui a été transmise aux différentes autorités de certification, de façon à engager des rencontres sur le plan local.

Dans ce cadre, les URSSAF, via les correspondants Teledép pourraient être sollicitées par les agences bancaires assurant la distribution de certification, afin de définir les modalités de démarrage de la procédure «e-mail sécurisée ».

Les URSSAF sont invitées à faire remonter à l'ACOSS – DISIR (Malika ZIANE), toute difficulté liée à la mise en œuvre de cette procédure.