

Ce document vous est offert par
la Banque Carrefour de la sécurité sociale.

Il peut être diffusé librement, à condition de
mentionner la source et l'URL

**Banque Carrefour
de la
Sécurité Sociale**

Chaussée Saint-Pierre 375
B-1040 BRUXELLES

Tél: +32 2 741 83 11
Fax: +32 2 741 83 00

AVIS N° 03/07 DU 17 JUIN 2003 RELATIF A UNE DEMANDE DU FONDS D'ASSURANCE SOCIALE VEV AFIN D'OBTENIR L'AGREATION MINISTERIELLE POUR UN SYSTEME D'ARCHIVAGE ELECTRONIQUE EN APPLICATION DE L'ARRÊTÉ ROYAL DU 28 NOVEMBRE 1995 RELATIF A LA VALEUR PROBANTE, EN MATIÈRE DE SÉCURITÉ SOCIALE DES TRAVAILLEURS INDEPENDANTS, DES INFORMATIONS ÉCHANGÉES, COMMUNIQUÉES, ENREGISTRÉES, CONSERVÉES OU REPRODUITES PAR LES SERVICES MINISTÉRIELS ET LES PARASTATAUX DU MINISTÈRE DES CLASSES MOYENNES

Vu l'Arrêté royal du 28 novembre 1995 relatif à la valeur probante, en matière de sécurité sociale des travailleurs indépendants, des informations échangées, communiquées, enregistrées, conservées ou reproduites par les services ministériels et les parastataux du Ministère des Classes Moyennes.

Vu la demande du VEV du 10 février 2003;

Vu le rapport d'auditorat de la Banque-carrefour du 12 juin 2003;

Vu le rapport de Monsieur Foulek Ringelheim.

1. INTRODUCTION

En date du 17 février 2003, le Fonds d'assurance sociale VEV introduisait une demande auprès du Comité de surveillance afin d'obtenir l'agrément ministériel d'une procédure dans le cadre de l'application de l'arrêté royal du 28 novembre 1995 relatif à la force probante en matière de sécurité sociale des travailleurs indépendants.

2. CONTEXTE GÉNÉRAL

Il y a lieu de vérifier si la procédure de reconnaissance satisfait aux conditions techniques décrites à l'article 3 de l'arrêté royal du 28 novembre 1995.

La demande transmise par l'organisation VEV repose sur le projet d'utiliser les formulaires électroniques fournis par le service CERTIPOST.

Dans l'énoncé de la demande de VEV on peut lire :

'La mise en ligne de formulaires à remplir permet d'éviter au maximum des erreurs (lors de l'introduction et du traitement) étant donné que les utilisateurs de PostBox remplissent ces formulaires à l'écran et les transmettent ensuite directement. La Caisse d'Assurances Sociales reçoit chaque formulaire complété à travers un e-mail contenant trois annexes : le formulaire rempli sous format PDF, les données remplies sous format XML et un PostMark qui garantit l'identité de l'expéditeur, la date et l'heure de l'envoi et l'intégrité du message. Le traitement ultérieur peut être réalisé de façon automatique par

l'introduction du fichier XML dans le back-office de la Caisse d'Assurances Sociales.'
On se situe donc dans un contexte d'échange de courrier électronique auquel est associé un émetteur, un récepteur et une autorité de certification chargée d'assurer la notion universelle : **'le cachet de la Poste faisant foi'**.

L'examen du Comité s'est concentré sur l'utilisation de la solution CERTIPOST. L'analyse d'un tel processus doit particulièrement veiller à vérifier la confidentialité, la fiabilité, la disponibilité et la non-répudiation des informations échangées.

3. DÉMARCHE SUIVIE

Considérant que les informations transmises lors du dépôt de la demande étaient insuffisantes pour développer un rapport d'auditorat le plus complet possible, le service de sécurité de la Banque Carrefour a pris contact avec les responsables techniques de CERTIPOST à fin d'obtenir des informations complémentaires sur les aspects techniques et de sécurité de leur solution.

En prolongement des informations reçues des collaborateurs de l'organisation CERTIPOST, le service de sécurité de la Banque Carrefour a également souhaité obtenir de VEV des réponses à différentes questions liées à l'utilisation de diverses fonctionnalités présentes dans la solution

Suite aux réponses fournies, le service de sécurité a invité les représentants de Certipost, en présence de Madame Minnaert conseillère en sécurité de l'INASTI, à une réunion technique à la Banque Carrefour à fin d'éclaircir davantage différents aspects indispensables à la bonne compréhension du processus audité.

Conscient de l'importance de présenter un dossier complet auprès du Comité de surveillance de la Banque Carrefour, les représentants de Certipost ont transmis, en date du 6 juin, au service de sécurité de la Banque Carrefour un dossier technique complet de la solution audité.

4. CERTIPOST

Le groupe de La Poste a créé en 2000 une filiale dédiée aux nouveaux moyens de communication électroniques sous le nom BPG e-Services. Cette filiale développe de nouveaux canaux de communication électroniques basés sur les technologies de l'Internet.

En tant qu'entreprises de communication, La Poste et Belgacom ont décidés d'adopter une approche commune en matière d'optimisation et de sécurisation des communications électroniques. En décembre 2002, le Conseil de la Concurrence a approuvé la création d'une joint-venture de La Poste et Belgacom.

Belgacom apporte à CERTIPOST les activités de Belgacom E-Trust, tandis que La Poste y regroupe les activités de sa filiale e-Services. Cette association porte le nom de CERTIPOST.

Belgacom E-Trust, est une Autorité de Certification, un instrument de création et de gestion de certificats digitaux. Ces certificats sont utilisés pour sécuriser des applications Internet telles que le web browsing, le secure messaging, le contrôle de l'accès à des informations confidentielles ou la sécurisation de transactions commerciales.

La Poste apporte la plate-forme « PostBox » regroupant entre autres, le guichet électronique sécurisé pour les communes et notaires, et la gestion électronique du courrier administratif (factures, fiches de paie, renouvellement de contrats,...).

La société Aditel, reprise par La Poste e-Services en septembre 2002, est intégrée dans la nouvelle société.

5. REMARQUES CONCERNANT L'APPLICATION DE L'ARTICLE 3 DE L'ARRÊTÉ ROYAL DU 28 NOVEMBRE 1995

5.1. La proposition décrit la procédure avec précision.

Suite aux différents contacts, réunions, recherches et questions posées les services de la Banque carrefour ont pu constituer un dossier de référence permettant d'auditer de manière précise la solution mise en place.

Suite aux réponses à nos différentes questions, il s'avère que l'organisation VEV n'envisage d'utiliser la solution CERTIPOST que dans le contexte du courrier électronique classique par opposition au courrier électronique recommandé qui n'entre pas dans la demande adressée au Comité de surveillance.

En annexe du présent rapport figure une copie du dossier papier transmis par Certipost qui décrit avec précision l'ensemble des composantes et les procédures qui sont d'application dans l'utilisation de leur solution en générale. L'obtention de ce dossier a été liée à un engagement par le service de sécurité de la Banque Carrefour de respecter la confidentialité des informations transmises et de ne les utiliser que dans le cadre de cet auditorat.

5.2. La technologie utilisée garantit une reproduction fidèle, durable et complète des informations

L'audit porte exclusivement sur les aspects liés à l'utilisation de la solution CERTIPOST. Elle n'a pas pour finalité d'évaluer le processus mis en place en amont et en aval de la solution envisagée.

La technologie utilisée par la solution CERTIPOST repose sur l'utilisation de standards utilisés aujourd'hui dans le cadre du développement des systèmes d'information. On se situe dans l'utilisation d'un service INTERNET basé sur un processus sécurisé au travers de la technologie SSL (Secure Socket Layer). Ce protocole permettant la transmission sécurisée de formulaires sur le Web, notamment lors des transactions commerciales en ligne. Ce service INTERNET est basé sur l'utilisation d'un Browser standard (Application logicielle résidant sur un serveur Internet, à laquelle on accède par l'intermédiaire d'un navigateur Web et qui s'exécute à l'intérieur de la fenêtre du navigateur. Internet Explorer 5 et + / Internet Explorer 6 et + sont à ce jour qualifiés par la solution CERTIPOST).

Le Comité a été attentif au processus d'enregistrement de l'utilisateur qui se compose de trois étapes distinctes et obligatoires à savoir :

- ❖ Etape 1 : une inscription en ligne,
- ❖ Etape 2 : une identification physique dans un bureau accrédité par Certipost (Les utilisateurs de CERTIPOST doivent passer par une inscription en face à face, comportant la signature d'un contrat sur papier. Le bureau d'enregistrement accrédité contrôle l'identité de l'utilisateur au moyen d'un document légal, comme la carte d'identité).
- ❖ Etape 3 : une première connexion à Certipost

A ces trois étapes sont associés la transmission d'une lettre de confirmation de l'enregistrement, l'attribution d'un code PIN de type bancaire et d'un mot de passe provisoire à modifier obligatoirement lors de la première connexion à son compte.

Pour toute question relative à une Certipost spécifique, le Centre de Services Certipost doit pouvoir identifier de manière certaine l'utilisateur. A cet effet, ce dernier doit pouvoir fournir la réponse à la question secrète qu'il a choisie lors de son inscription.

D'autre part dans le cas de perte de son mot de passe l'utilisateur doit suivre une procédure qui l'oblige à se rendre dans un bureau d'enregistrement accrédité par CERTIPOST.

5.3. Les informations sont enregistrées systématiquement et sans lacunes

On se situe dans un contexte d'échanges électroniques au travers d'une solution basée sur l'utilisation d'un cachet électronique de la poste qui garantit la date et l'heure de réception du courrier certifié sur la plate-forme CERTIPOST.

Cette technique du PostMark a fait l'objet d'une documentation précise de la part de l'organisation Certipost.

Il s'agit d'une marque ajoutée à tout message transmis dans le cadre de l'environnement Certipost qui empêche toute modification du message. Le cachet électronique ajoute une signature numérique à tout message Certipost pour :

- ❖ certifier la date et l'heure auxquelles le serveur Certipost reçoit le message électronique;
- ❖ garantir l'identité de l'émetteur, à savoir son nom et son adresse tels qu'ils ont été enregistrés par le bureau d'enregistrement accrédité;
- ❖ garantir l'intégrité du message lors de sa réception par le serveur Certipost.

5.4. Les informations traitées sont conservées avec soin, classées systématiquement et protégées contre toute altération

Chaque annexe associée au compte email, est analysée automatiquement avant de la télécharger. Si cette annexe est infectée par un virus, un processus d'alerte est mis en place et le message infecté n'est pas transmis. Tout processus d'échanges électroniques est

conditionné par le rôle responsable de chaque acteur dans l'exécution de son échange d'information. L'organisation VEV doit dès lors veiller à disposer d'une infrastructure à jour dans la lutte contre toutes les attaques possibles dans un tel mode de communication. L'infrastructure du réseau CERTIPOST est protégée par des murs pare-feu (firewall) et des systèmes de détection d'intrusion, de manière à empêcher d'accéder sans autorisation à des données CERTIPOST. Des mécanismes et procédures de sécurité physique garantissent un contrôle du serveur CERTIPOST.

Un des objectifs recherché par VEV est d'utiliser la fonctionnalité du formulaire électronique intelligent qui correspond à la version informatique d'un formulaire papier. Ces formulaires électroniques peuvent être remplis plus rapidement grâce à la programmation qui leur est associée.

Chaque organisation peut développer ses propres formulaires à condition d'utiliser certains outils spécifiques et répondre à certaines caractéristiques techniques afin que les formulaires soient compatibles avec la plate-forme CERTIPOST.

Tout formulaire papier utilisé par l'organisation VEV dans le cadre de ses échanges d'informations en matière de sécurité sociale des travailleurs indépendants est préalablement validé par l'INASTI. Il importe de ne pas déroger à cette règle dans le cadre de l'utilisation du formulaire électronique et de considérer que tout formulaire développé par l'organisation VEV au sein de l'infrastructure CERTIPOST doit être approuvée par l'organisation tutelle avant son utilisation.

5.5. Conservation des indications suivantes relatives au traitement des informations : l'identité du responsable du traitement ainsi que de celui qui a exécuté celui-ci, la nature et l'objet des informations auxquelles le traitement se rapporte, la date et le lieu de l'opération, les perturbations éventuelles qui sont constatées lors du traitement

On se situe dans un contexte d'échanges électroniques basés sur l'utilisation d'un cachet électronique de la poste qui garantit:

- ❖ L'identité de l'expéditeur grâce à la procédure d'enregistrement qui exige une vérification physique de son identité
- ❖ L'intégrité du courrier certifié est garantie par l'apposition d'une signature électronique assurant que les messages ne peuvent être altérés pendant l'envoi
- ❖ La date et l'heure de réception du courrier certifié sur la plate-forme CERTIPOST

Dans le respect de la directive européenne sur le commerce électronique 2000/31/EC le processus "d'opt-in" (liste d'inclusion à laquelle l'adresse de l'internaute nouvellement inscrit, est ajoutée seulement après l'envoi à cette adresse d'un courrier électronique de confirmation auquel celui-ci répond en cliquant sur un lien pour confirmer son adhésion initiale) est utilisé pour garantir qu'aucune communication ne sera envoyée sans le consentement express de l'utilisateur CERTIPOST.

Il a pu être vérifié que le 'POSTMARK' (cachet de la poste faisant foi) de validation de l'échange de courrier n'est attribué qu'après l'exécution des différentes étapes du processus et est le seul garant de la complétude du processus exécuté.

6. CONCLUSION

Le dossier introduit par le VEV remplit les conditions visées par l'article 3 de l'arrêté royal du 28 novembre 1995 déterminant les conditions et les modalités relatives à la valeur probante en matière de sécurité sociale des travailleurs indépendants, des informations échangées, communiquées, enregistrées, conservées ou reproduites par les services ministériels et les parastataux du Ministère des Classes Moyennes.

Il est à noter que le service «sécurité» de la Banque-carrefour de la sécurité sociale a collaboré avec les services de l'institution de tutelle, l'INASTI, à la constitution du dossier. Les représentants de VEV ainsi que ceux de l'institution de tutelle ont donc été entendus comme le prévoit l'article 4 de l'arrêté royal précité et ils ont été mis en mesure de s'expliquer de manière complète.

Par ces motifs,

le Comité de surveillance

émet un avis favorable.

F. Ringelheim
Président