

Le service d'échange de fichiers (SEF)

L'Insee a construit une offre de service d'échanges de fichiers en TCP/IP avec ses partenaires.

Les flux considérés sont des flux « métier » c'est-à-dire que les informations qui transitent sont, soit émises par des applications Insee, soit à destination des applications Insee. Il s'agit donc d'un système d'échange de fichiers asynchrones inter-applications.

Ce service d'échange repose sur :

- une chaîne unique d'échange de fichiers avec les partenaires externes,
- une automatisation des interactions avec les applications internes,
- une automatisation des traitements de transformations techniques et d'acheminement des données.

Les échanges réseau peuvent se faire via un réseau inter ou intra-ministériel pour les organismes autorisés, soit via Internet pour les entreprises ou autres organismes. Deux protocoles de communication sont disponibles : SFTP ou CFT (Pesit E). Pour les nouvelles demandes le protocole SFTP est à privilégier. En SFTP : L'insee peut être client ou serveur.

En CFT, l'émetteur est client du site vers qui il envoie un fichier. Dans ce cadre, chacun est client quand il envoie un fichier, et serveur lorsqu'il en reçoit un.

Les fichiers à transmettre sont déposés par le partenaire ou par l'Insee sur un serveur situé sur la passerelle Internet de l'Insee. Un serveur de l'Insee, récupère les fichiers déposés par le partenaire ou met à disposition du partenaire les fichiers produits par les applications Insee.

La sécurité est assurée par :

- Authentification mutuelle forte et chiffrement des transferts :
- chiffrement des connexions par TLS 1,2 (Pesit) ou SSH (SFTP)
- authentification mutuelle par certificats (Pesit) ou login + Mot de passe + clé SSH (SFTP)

La nature des données et leur niveau de confidentialité imposent la nécessité de chiffrer également les données. Ce chiffrement sera pris en compte par l'équipe métier en lien avec la Division Sécurité et Maîtrise des Risques (DSMR) à la Direction du Système d'Information (DSI) de l'Insee,

- Chiffrement des données :
 - l'algorithme utilisé est le RSA
 - la taille est de 3072 bits pour les clés applicatives et de 4096 pour les clés maîtres
 - la durée des clés applicatives est de 3 ans
 - La durée de la clé maître est de 10 ans

La compression des fichiers est fortement encouragée. Elle est faite au format zip ou gzip.

Selon les besoins, il peut être mis en place des avis de mise à disposition d'un fichier : selon la cible (interne /externe), ces avis peuvent être de différente nature (message ; accusé réception, etc.)

Résumé :

- Un échange se fera toujours avec une sécurisation du transfert (SSLV3 ou TLSv1.2). Ceci nécessite de la part du partenaire l'achat d'un certificat commercial.

L'Insee ne fait pas de référencement. Avant le passage en production, la Division Sécurité et Maîtrise des Risques (DSMR) à la Direction du Système d'Information (DSI) de l'Insee examine la politique de sécurité de l'autorité de certification choisie par le partenaire afin de vérifier qu'elle peut être considérée de confiance.

- Tout échange de données confidentielles doit s'accompagner du chiffrement des données. Voir ci-dessous le § politique de gestion des clés.

Dès lors qu'un des échanges nécessite le chiffrement des données, le chiffrement des données sera effectué pour tous les échanges, y compris ceux sur supports physiques.

Politique de gestion de clés

Si le chiffrement des données doit être mis en place, un document appelé « politique de gestion des clés » dont l'Insee fournira le canevas sera signé après accord sur son contenu par les deux parties.

L'échange de clé-maître est fait face à face par le Responsable Sécurité du Système d'Information de l'Insee et son homologue chez le partenaire.

La politique de gestion des clés signée à l'occasion d'un transfert donné sera valable pour les autres transferts qui seraient mis en place ultérieurement (moyennant la création des clés applicatives adéquates). C'est pourquoi, même si le besoin n'est pas immédiat, nous demandons que partenaire et Insee génèrent une clé-maître.

Recommandations

Afin de faciliter les transmissions de fichiers, il est recommandé :

- D'effectuer la compression des fichiers. La compression des fichiers est dans certains cas incontournable. Elle est faite au format zip ou gzip.
- De limiter la durée des transferts à une heure maximum afin de minimiser les risques d'interruption.
- D'étudier, en cas de volumétrie importante (la limite maximale est à 3 Go par fichier compressé), la possibilité de faire des envois plus fréquents et de volumétrie moindre ou opter pour un transfert sur support physique respectant les règles de sécurité préconisées pour la protection des données.

Protocole de tests

La mise en place du service d'échange de fichiers nécessite le déroulement d'un protocole de test et le passage en production se fait après validation par les deux parties du fonctionnement de bout en bout de l'échange.

Cette mise en place passe par :

- La définition des paramètres du transfert et des besoins des applications clientes
- Le déroulement des tests visant à vérifier progressivement
 - la capacité de s'échanger des données - contexte réseau,
 - la capacité à faire des transferts chiffrés,
 - la capacité à faire des transferts de données chiffrées,
 - la compression /décompression,
 - le chiffrement / déchiffrement.