

Installation du kit de connexion



CESAM

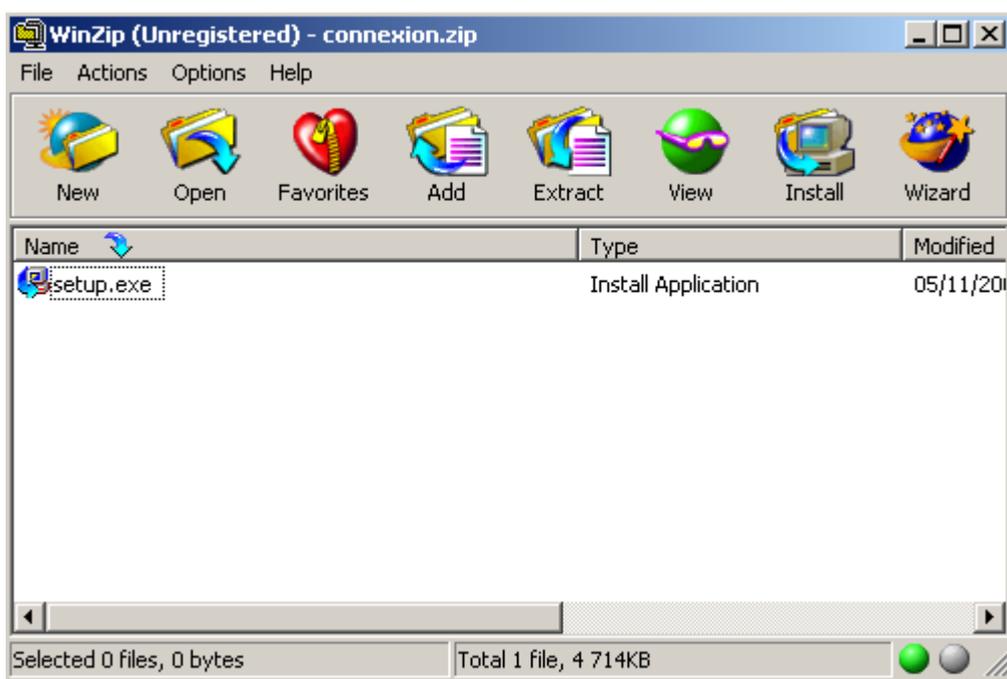
Télécharger par FTP le kit de connexion (connexion.zip) sur le site www.optiflux.fr rubrique Obtenir un identifiant.

1 – Installation Kit de Connexion :

Vous devez avoir Winzip (logiciel gratuit) pour lire connexion.zip

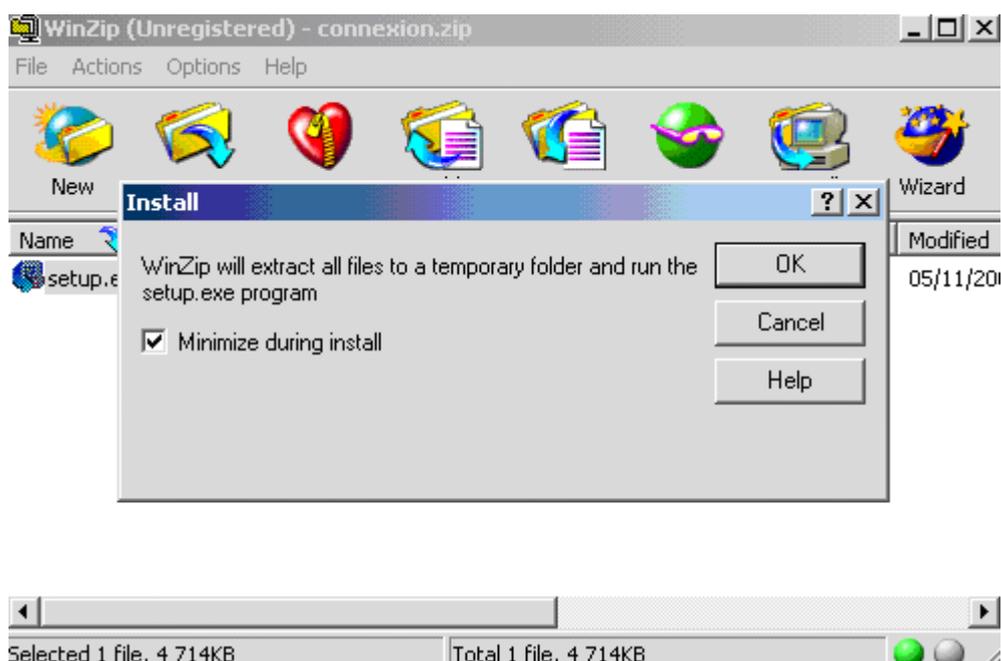
Cliquez sur connexion.zip.

S'affiche alors la fenêtre suivante :

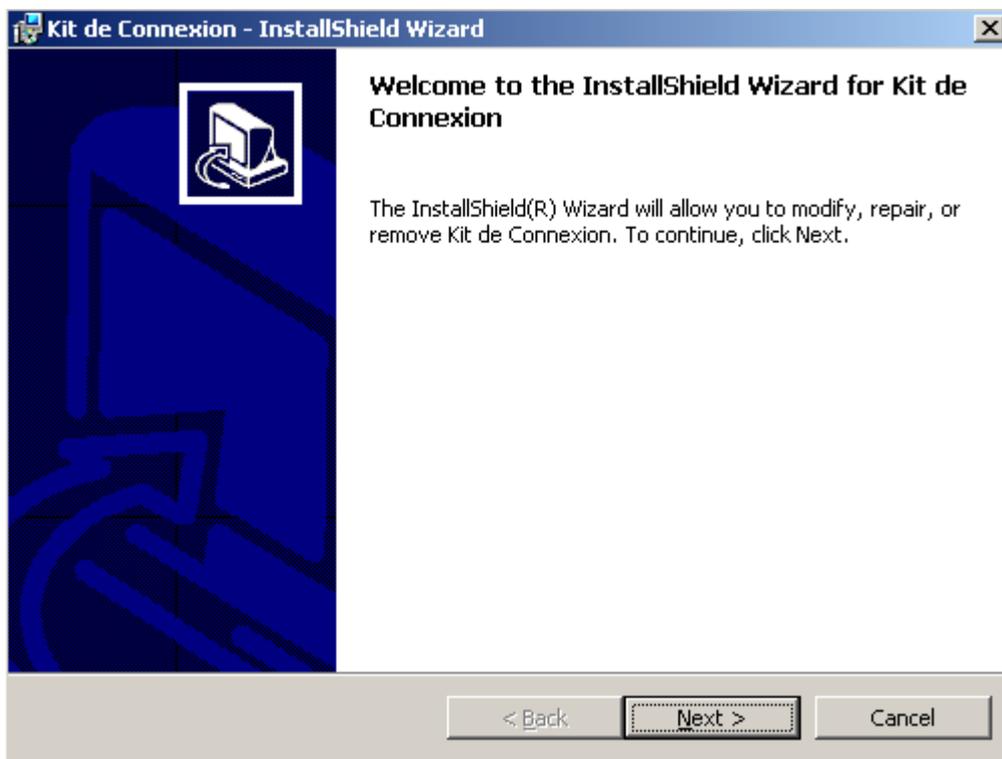


Lancer setup.exe

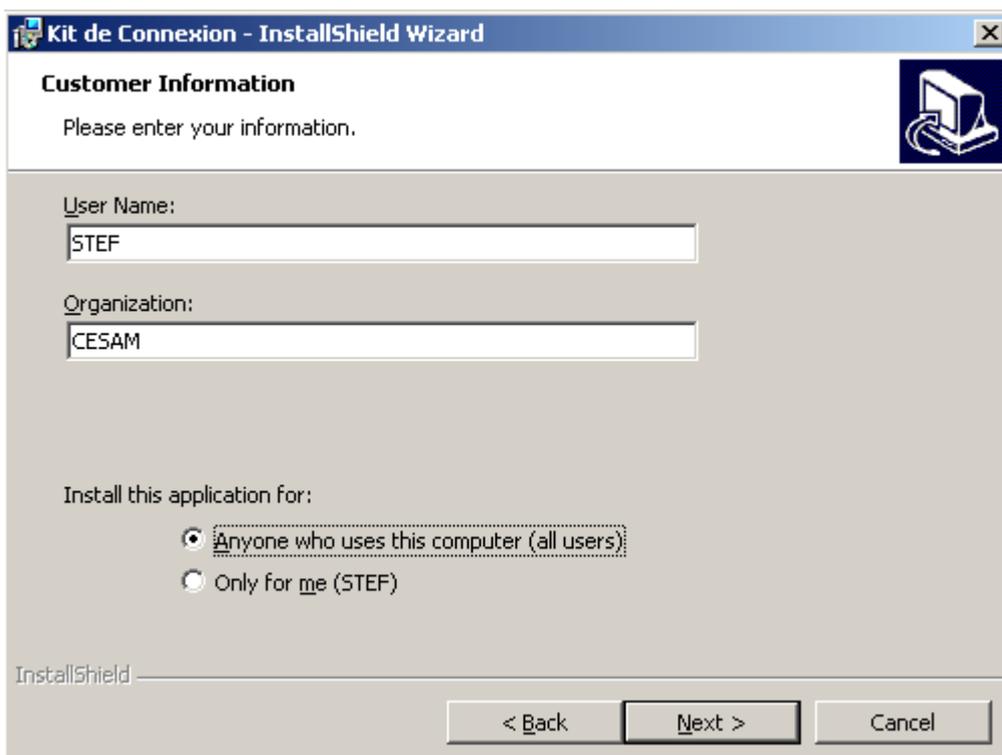
S'affiche alors la fenêtre suivante :



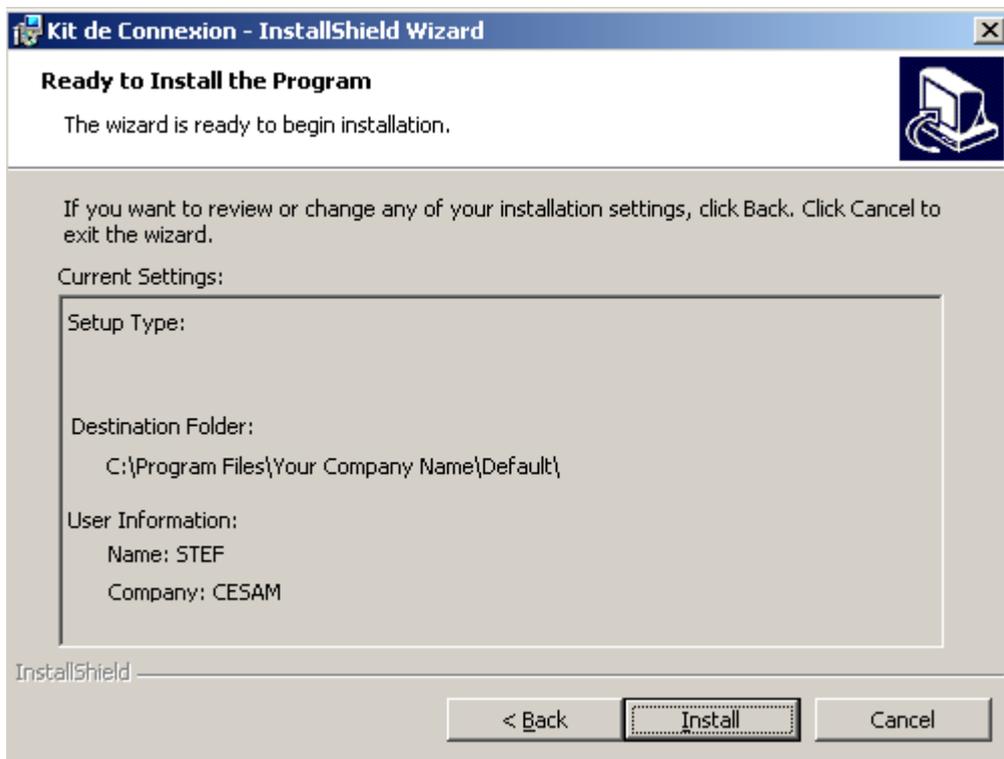
Cliquer sur ok



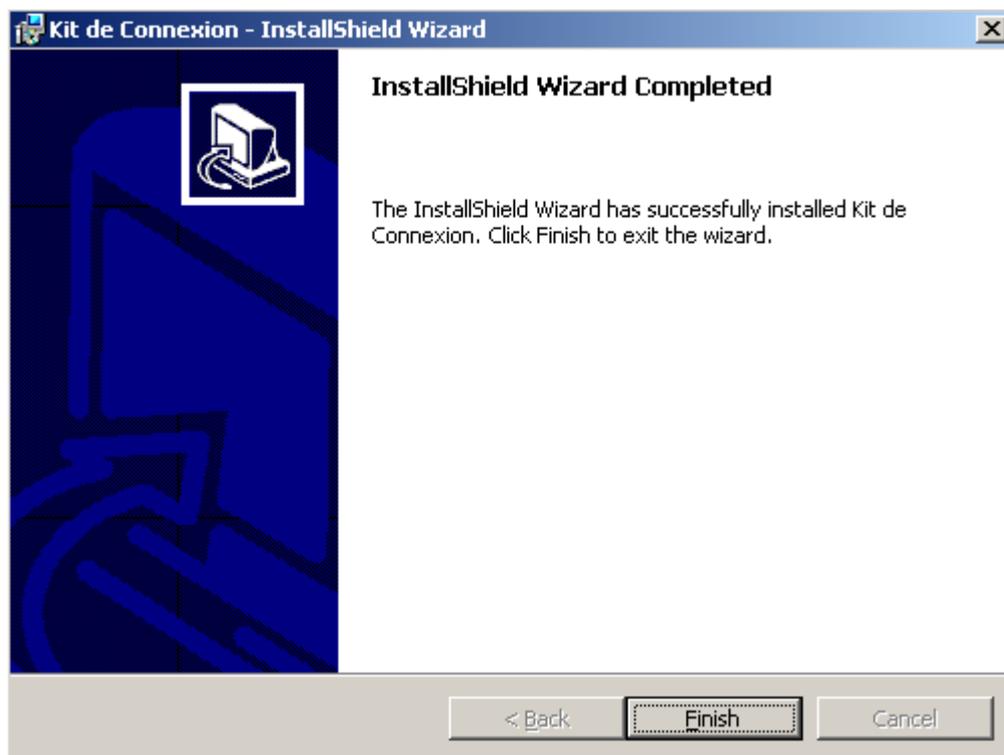
Cliquer sur le bouton Next



Saisissez un nom d'utilisateur et le nom de la société.
Cliquer sur le bouton Next.



Cliquer sur le bouton Install



Cliquer sur le bouton Finish

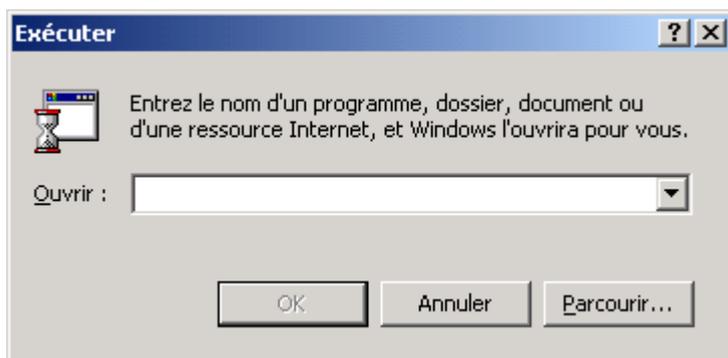
2 - Paramétrage du kit de connexion.

Le paramétrage du logiciel consiste à créer une clé de cryptage. Cette clé de cryptage va vous permettre de crypter et décrypter les fichiers.

Si vous êtes sous Windows, allez dans le menu « Démarrer », et sélectionnez l'option « Exécuter ».



S'affiche ensuite la fenêtre suivante :

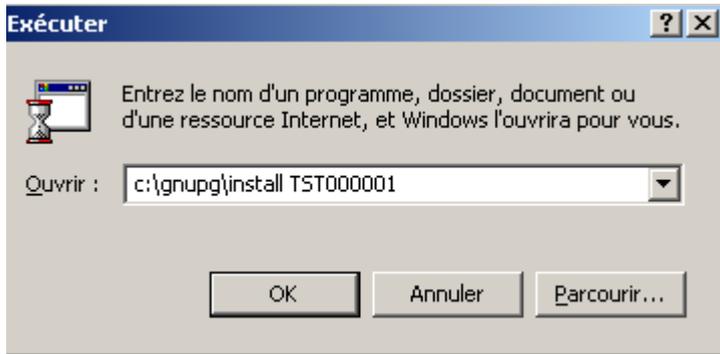


Dans le champ Ouvrir, tapez la commande suivante :

C:\gnupg\install *votre_identifiant_bdi*

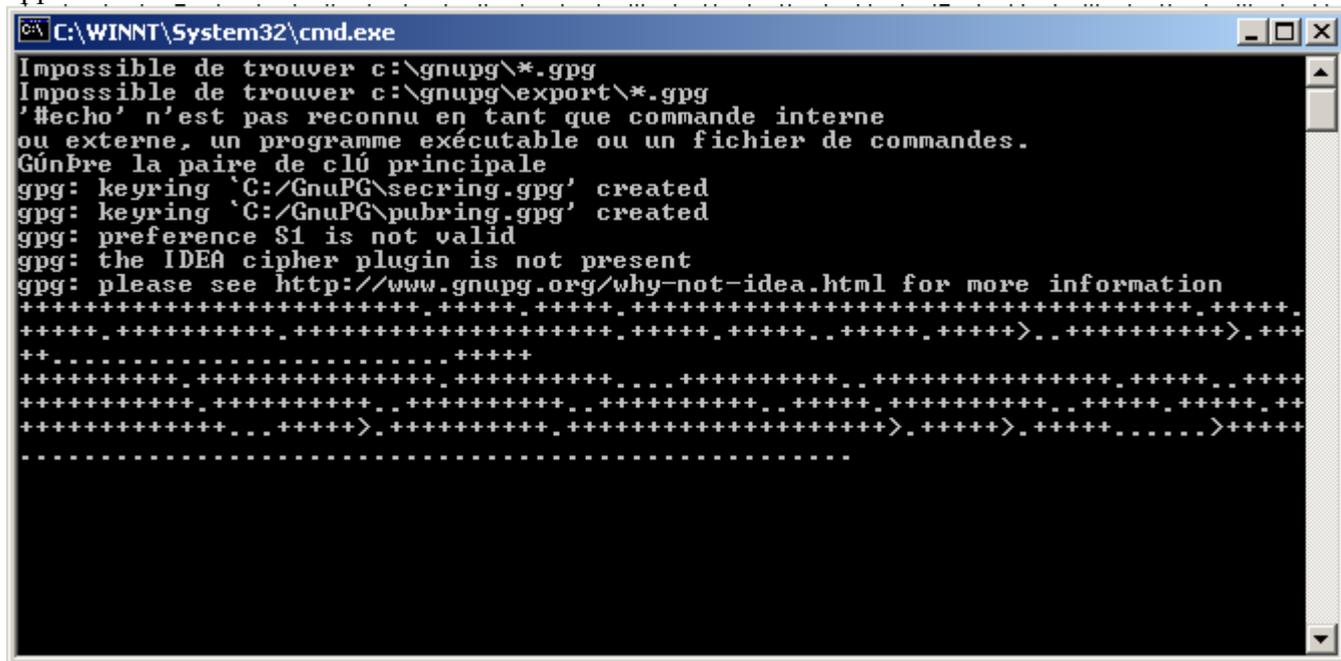
NOTE : Si vous souhaitez générer une clé en remplacement de toutes les clés existantes, au lieu de la commande install, tapez la commande c:\gnupg\installnew *votre_identifiant_bdi*

TST000001 correspond à votre identifiant BDI , spécifié par le CESAM en contactant le service informatique.



Validez par la touche Entrée ou cliquez sur OK

Le programme va donc générer vos clés et configurer le logiciel. Lors de la génération de la clé, voici ce qui doit apparaître à l'écran



Cela peut prendre quelques minutes.

Au bout de quelques instants l'application vous pose différentes questions :

```
C:\WINNT\System32\cmd.exe
gpg: key 8FBB8F62: public key "BDI000001 <BDI000001>" imported
gpg: Total number processed: 1
gpg: imported: 1

gpg: checking the trustdb
gpg: checking at depth 0 signed=0 ot(-/q/n/m/f/u)=0/0/0/0/0/1
pub 1024D/8FBB8F62 created: 2003-10-21 expires: never trust: -/-
sub 1024g/D81EFP55 created: 2003-10-21 expires: never
(1). BDI000001 <BDI000001>

pub 1024D/8FBB8F62 created: 2003-10-21 expires: never trust: -/-
Primary key fingerprint: 5A91 84FD 0D0A 2450 3675 3CE3 ECCD 296C 8FBB 8F62
BDI000001 <BDI000001>

How carefully have you verified the key you are about to sign actually belongs
to the person named above? If you don't know what to answer, enter "0".

(0) I will not answer. (default)
(1) I have not checked at all.
(2) I have done casual checking.
(3) I have done very careful checking.

Your selection?
```

Appuyez sur la touche « Entrée »

```
C:\WINNT\System32\cmd.exe
gpg: checking the trustdb
gpg: checking at depth 0 signed=0 ot(-/q/n/m/f/u)=0/0/0/0/0/1
pub 1024D/8FBB8F62 created: 2003-10-21 expires: never trust: -/-
sub 1024g/D81EFP55 created: 2003-10-21 expires: never
(1). BDI000001 <BDI000001>

pub 1024D/8FBB8F62 created: 2003-10-21 expires: never trust: -/-
Primary key fingerprint: 5A91 84FD 0D0A 2450 3675 3CE3 ECCD 296C 8FBB 8F62
BDI000001 <BDI000001>

How carefully have you verified the key you are about to sign actually belongs
to the person named above? If you don't know what to answer, enter "0".

(0) I will not answer. (default)
(1) I have not checked at all.
(2) I have done casual checking.
(3) I have done very careful checking.

Your selection?
Are you really sure that you want to sign this key
with your key: "TST000001 <TST000001>"
Really sign? y
```

Répondez y, appuyez sur la touche « Entrée »

Une fois le paramétrage fini, la fenêtre doit se fermer.

L'application de cryptage est maintenant installée.

SI VOUS SOUHAITEZ LE LOGICIEL DE CRYPTAGE SUR PLUSIEURS POSTES UTILISTEURS, VOUS COPIEZ LE REPERTOIRE C:\GNUPG SUR TOUS LES POSTES, CAR SI VOUS RELANCEZ L'INSTALLATION AVEC LE MEME IDENTIFIANT, LA CLE GENEREE N'EST PAS LA MEME.

SI VOUS SOUHAITEZ INSTALLER PLUSIEURS CLES DE CRYPTAGE SUR LE MEME POSTE, RELANCEZ LA COMMANDE INSTALL POUR CHAQUE CLE A GENERER.

3 - Export des clés publiques

A ce niveau là de la configuration du logiciel, vous êtes en mesure de crypter des fichiers à destination du serveur BDI du CESAM, mais celui-ci ne vous a pas encore déclaré, donc il ne distribuera pas le fichier envoyé. Il faut pour cela que vous envoyez au CESAM le fichier situé dans le répertoire c:\gnupg\export de votre disque dur.

Copiez ce fichier sur disquette ou email (sdasilva@cesam.fr).

Envoyez le formulaire d'inscription BDI signé soit par FAX (01.58.56.96.39), ou à l'adresse suivante :

CESAM

Service Informatique

8 rue d'Artois

75008 Paris

Le fichier sera intégré au serveur BDI dès sa réception.

A ce moment, votre mot de passe sera communiqué par email. Il s'agit de l'adresse email indiquée sur le formulaire.

Pendant la phase de test, vous prenez contact avec le service informatique au 01.58.56.96.34 ou 35, vous enverrez la clé par email.

Utilisation de scripts ftp pour gérer ses envois sans utiliser le kit Optiflux.

A partir d'un environnement UNIX ou DOS, il est possible de créer des scripts de cryptage/décryptage et des scripts de transfert de fichiers depuis et vers le serveur BDI. Ces scripts peuvent être appelés directement depuis la ligne de commande.

Voici deux exemples de scripts qui vous permettront d'automatiser vos envois et réceptions de fichier vers la BDI

1 – Cryptage et Envoi de fichier

Ce script crypte le fichier passé en paramètre lors de l'appel du script et l'envoie au serveur BDI :

- Dans le cas où une seule clé a été générée sur la machine :

```
GPG --encrypt --sign --recipient BDI000001 %1  
ftp -i -v -s:ftpsend.txt
```

Dans ce cas, l'appel du script se fait en passant en paramètre :

- Le nom du fichier à crypter

- Dans le cas où plusieurs clés de cryptage ont été générées sur la machine ;

```
GPG --default-key %1 --encrypt --sign --recipient BDI000001 %2  
ftp -i -v -s:ftpsend.txt
```

Dans ce cas, l'appel du script se fait en passant en paramètre :

- La clé utilisée pour la signature (le login du compte utilisé)
- Le nom du fichier à crypter

La première commande (GPG) se charge de crypter et signer le fichier à destination de la BDI.

La seconde commande (FTP) lance le transfert FTP en faisant appel à un fichier ftpsend.txt décrit ci-dessous. Ce fichier contient toutes les commandes de connexion FTP

Ftpsend.txt :

```
Open ftp.optiflux.fr  
login  
motdepasse  
binary  
cd emission  
mput *.gpg  
close  
bye
```

Remplacez *login* et *motdepasse* par votre identifiant et votre mot-de-passe.

2 – Réception et decryptage de fichiers

Ce script récupère tous les fichiers du répertoire réception de l'utilisateur sur le serveur BDI et les décrypte

```
ftp -i -v -s:ftprcve.txt  
GPG --decrypt-files *.gpg
```

La première commande lance le transfert FTP en faisant appel à un fichier `ftprcve.txt` décrit ci-dessous. Ce fichier contient toutes les commandes de connexion FTP

La seconde se charge de décrypter les fichiers reçus.

`Ftprcve.txt` :

```
Open ftp.optiflux.fr
login
motdepasse
binary
cd reception
mget *.gpg
close
bye
```

Remplacez *login* et *motdepasse* par votre identifiant et votre mot-de-passe.

Ces scripts vous sont fournis en tant qu'exemple. Vous pouvez tout à fait les adapter à vos besoins.