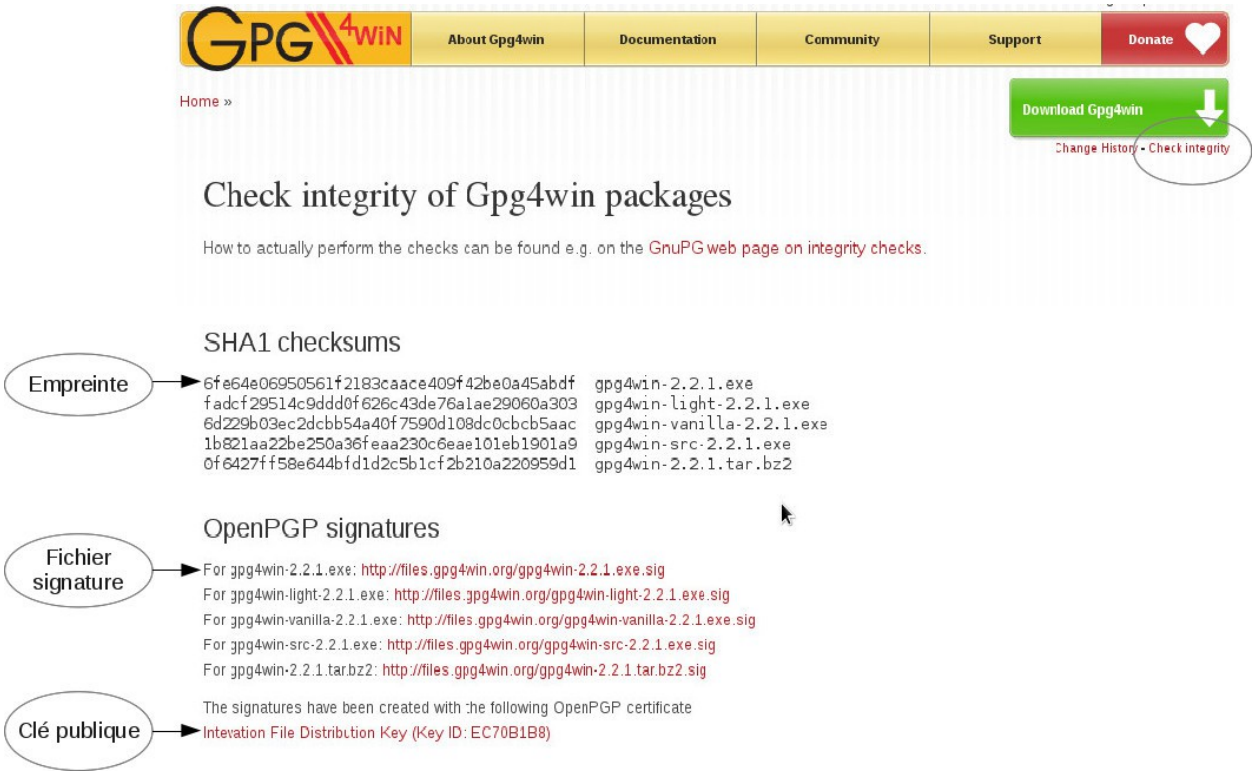
Annexe 5 Vérification de l'intégrité d'un fichier téléchargé

Les sites de téléchargement proposent fréquemment un fichier de signature (empreinte) permettant de vérifier l'intégrité du fichier téléchargé. Les distributions du code source de GnuPG, par exemple, sont signées de telle manière que les utilisateurs puissent vérifier qu'elles n'ont pas été modifiées depuis qu'elles ont été empaquetées. Dans la première partie de l'activité, vous avez téléchargé le logiciel Gpg4win version 2.2.1 ainsi qu'un fichier de signature. Ce dernier a été généré à l'aide de la clé privée de signature du site Gpg4win.



La clef publique de Gpg4win correspondant à la clef privée qui a servi à signer le fichier de signature permet de vérifier la signature et l'intégrité de la distribution téléchargée

1. Utilisation d'une fonction de hachage

- Exécuter la commande : sha1sum.exe gpg4win-2.2.1.exe
- Vérifier l'empreinte calculée à l'empreinte affichée sur le site.

La fonction de hachage permet de vérifier l'intégrité de la distribution téléchargée par comparaison des empreintes. Cette vérification est relative, l'empreinte affichée sur le site peut être contrefaite au même titre que les fichiers téléchargés.

2. Utilisation du fichier de signature détachée

- Importer la clé publique de signature du site Gpg4win à partir d'un serveur de clé :

- soit en ligne de commande : gpg --keyserver pgp.mit.edu --recv-keys 0xEC70B1B8 (noter qu'une empreinte de clé commence par 0x),
- soit à l'aide du menu OpenPGP d'Enigmail.

Au moment de son importation, la clé est vérifiée, sa base de confiance est indiquée (nombre de signatures notamment).
Vérifier le fichier de signature détachée à l'aide de la commande : gpg --verify gpg4win-2.2.1.exe.sig

Le fichier de signature téléchargé sur le site a bien été réalisé à l'aide de la clef "Intevation File Distribution Key distribution-key@intevation.de" récupérée sur le serveur de clef.

L'identifiant de la clef est identique à celui précisé sur le site.

Pour autant, nous ne pouvons pas être absolument surs de l'identité du propriétaire, s'il ne fait pas partie de notre toile de confiance.

La vérification de la signature détachée permet de garantir l'intégrité de la distribution téléchargée relativement à la confiance accordée à la clef publique utilisée.