LABO6 – Protéger ses mots de passe

1 GESTIONNAIRE DE MOTS DE PASSE – KEEPASS

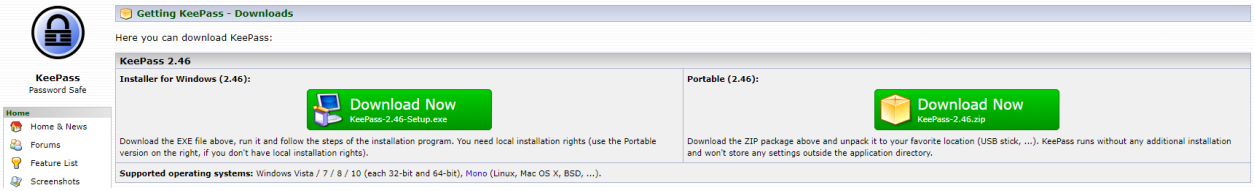
Le logiciel open source KeePass est un « coffre-fort » de mots de passe qu'il stocke dans une base de données dont l'accès est authentifié et le contenu chiffré.

Les fonctions de sécurité du logiciel Keepass sont les suivantes :

- génération de mots de passe robustes
- génération de clés maîtres robustes
- authentification de l'utilisateur (contrôle d'accès par mot de passe et/ou fichier clé)
- chiffrement/déchiffrement des données de la base de données
- intégrité de la base de données (protection et vérification)
- effacement des données temporaires
- chiffrement des données temporaires
- déconnexion automatique de la base de données pour prévenir une perte de données et un accès permanent à la base
- mécanisme d'« obfuscation » des mots de passe et des identifiants de connexion (par exemple « login » de compte Internet) à travers le presse-papiers et la simulation de frappe clavier.

1.1. Installer KeePass

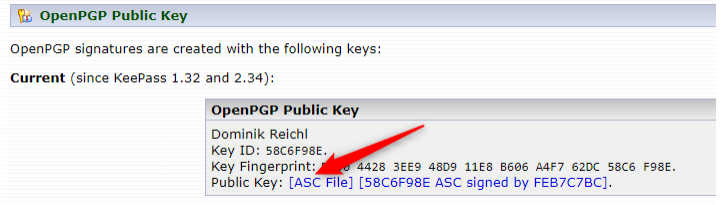
http://keepass.info/download.html

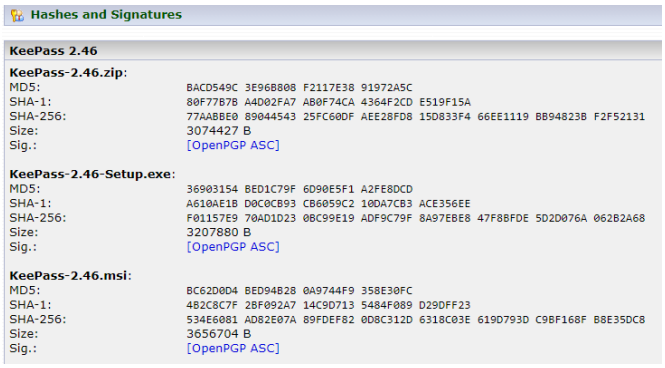


1. Téléchargez la version 2.* dans un dossier Keepass. Sauf si vous désirez installer le logiciel sur clé USB, préférez la version Installer.

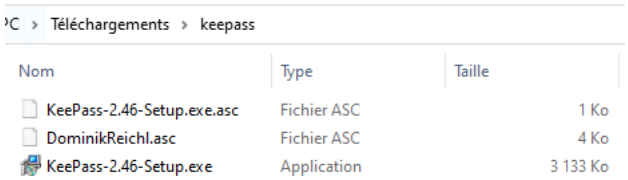
Vérifiez l'intégrité et l'authenticité du fichier téléchargé en visitant la page https://keepass.info/integrity.html#publickey

2. Téléchargez la clé publique de Keepass dans votre dossier





3. Téléchargez la signature du package que vous avez téléchargé dans votre dossier



Vous devez disposer de trois fichiers

4. Importez la clé publique de keepass en ligne de commande

```
gpg --import DominikReichl.asc
gpg: key A4F762DC58C6F98E: 1 signature not checked due to a missing key
gpg: key A4F762DC58C6F98E: public key "Dominik Reichl <dominik.reichl@gmx.de>"
imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg: no ultimately trusted keys found
```

5. A l'aide de votre clé privée, signez la nouvelle clé importée après avoir vérifié son empreinte.

```
gpg --edit-key dominik.reichl@gmx.de
gpg (GnuPG) 2.2.20-unknown; Copyright (C) 2020 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.


pub  rsa4096/A4F762DC58C6F98E
     created: 2016-06-08  expires: never       usage: SC
     trust: unknown       validity: unknown
sub  rsa4096/DD7276AC1E43A881
     created: 2016-06-08  expires: never       usage: E
[ unknown] (1). Dominik Reichl <dominik.reichl@gmx.de>

gpg> trust
pub  rsa4096/A4F762DC58C6F98E
     created: 2016-06-08  expires: never       usage: SC
     trust: unknown       validity: unknown
sub  rsa4096/DD7276AC1E43A881
     created: 2016-06-08  expires: never       usage: E
[ unknown] (1). Dominik Reichl <dominik.reichl@gmx.de>

Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
  m = back to the main menu

Your decision? 3

pub  rsa4096/A4F762DC58C6F98E
     created: 2016-06-08  expires: never       usage: SC
     trust: marginal      validity: unknown
sub  rsa4096/DD7276AC1E43A881
     created: 2016-06-08  expires: never       usage: E
[ unknown] (1). Dominik Reichl <dominik.reichl@gmx.de>
Please note that the shown key validity is not necessarily correct
unless you restart the program.

gpg> sign

pub  rsa4096/A4F762DC58C6F98E
```

```
     created: 2016-06-08  expires: never       usage: SC
     trust: marginal      validity: unknown
 Primary key fingerprint: D950 4428 3EE9 48D9 11E8  B606 A4F7 62DC 58C6 F98E

     Dominik Reichl <dominik.reichl@gmx.de>

Are you sure that you want to sign this key with your
key "Christophe Mangon <c.mangon@helmo.be>" (57BA8E3B77876CC5)

Really sign? (y/N) y

gpg> save
```

6. Vérifiez que la nouvelle clé publique est renseignée de confiance dans votre trousseau GPG

```
gpg -k
…
pub   rsa4096 2016-06-08 [SC]
      D95044283EE948D911E8B606A4F762DC58C6F98E
uid           [  full  ] Dominik Reichl <dominik.reichl@gmx.de>
sub   rsa4096 2016-06-08 [E]
…
```

7. Vérifiez l'authenticité et l'intégrité du fichier téléchargé

```
gpg --verify KeePass-2.46-Setup.exe.asc KeePass-2.46-Setup.exe
gpg: Signature made Thu Sep 10 11:52:44 2020
gpg:                using RSA key D95044283EE948D911E8B606A4F762DC58C6F98E
gpg: Good signature from "Dominik Reichl <dominik.reichl@gmx.de>" [full]
```

8. Et maintenant seulement, après avoir validé l'intégrité et l'authenticité de votre téléchargement, vous pouvez installer le logiciel Keepass.

9. **La passe-phrase que vous allez utiliser pour votre coffre-fort Keepass est la plus importante ! Elle doit être sûre et vous devez être certain de vous en souvenir !!!**

10. Suivez la documentation si nécessaire pour utiliser le logiciel https://keepass.info/help/base/index.html