Password Manager

Beta Testing - POC

Merci à vous! :)

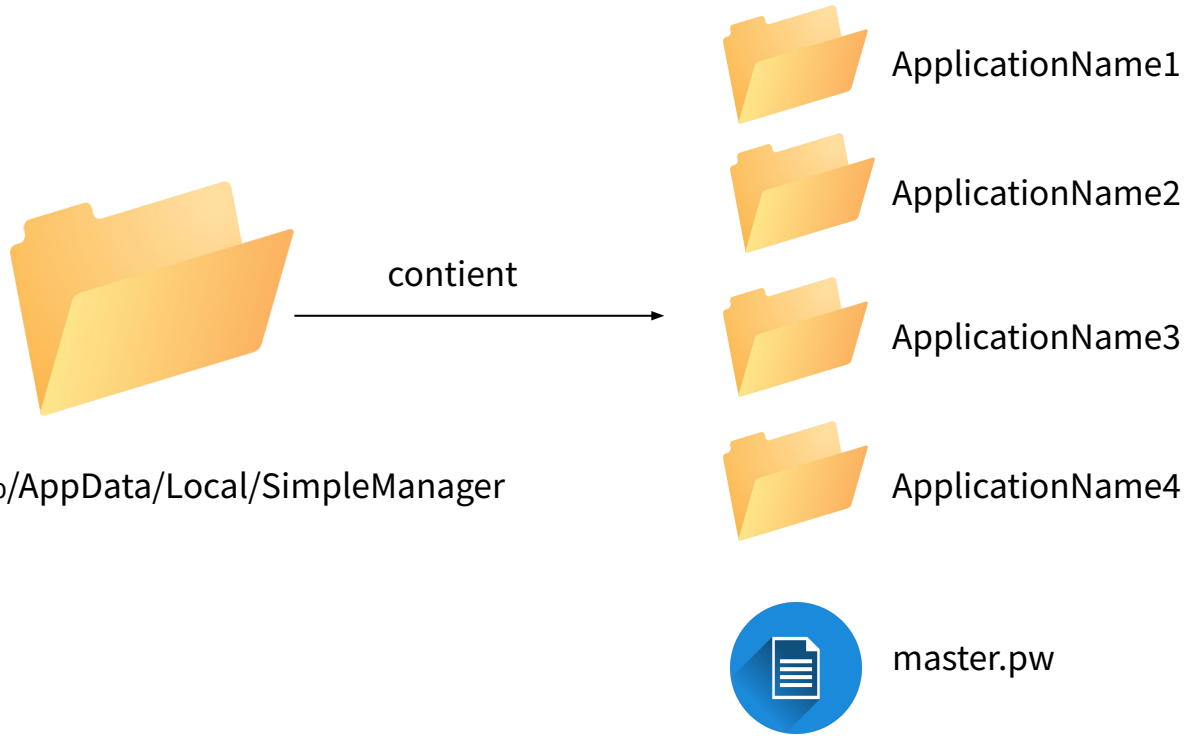
Constat: Ce petit projet à pour but de garantir la sécurité de vos mots de passe, en **offline**. Les applications tierces de gestion de mots de passe en ligne sont de plus en plus nombreuses et faciles d'utilisation, cependant leur utilisation est **online**, et ne garantit pas l'intégrité ni la confidentialité des mots de passes saisis (imaginez que les serveurs de LastPass aient une fuite…).

Concept: Un mot de passe **"maître"** sert à chiffrer et à déchiffrer les mots de passe que vous mettrez dans l'application, qui vous les sert quand l'application est ouverte.

Les détails utilisés seront présentés un peu plus bas

PS: %userprofile% fait référence au chemin de l'utilisateur du compte (par ex: C:\Users\florent)

Vue du Système de Fichiers (Windows)



Détails du fichier “master.pw”

master.pw

contient →

08b5b6491249d55a305827167308e12bd190200aa0f78b6d59b293398fb1338d1
db1fd5e8059cdfd1d2849fe528532066505867250fd29560793d279edc694a1

Le fichier “master.pw” contient le haché (sha-512) du mot de passe “maître” saisi lors de la première utilisation.
Ex: “rootroot” est saisi comme mot de passe maître, le fichier “master.pw” contiendra alors la valeur
“08b5b6491249d55a305827167308e12bd190200aa0f78b6d59b293398fb1338d1db1fd5e8059cdfd1d2849fe528532066505867250fd29560793d279edc694a1”

Authentification sur l'application

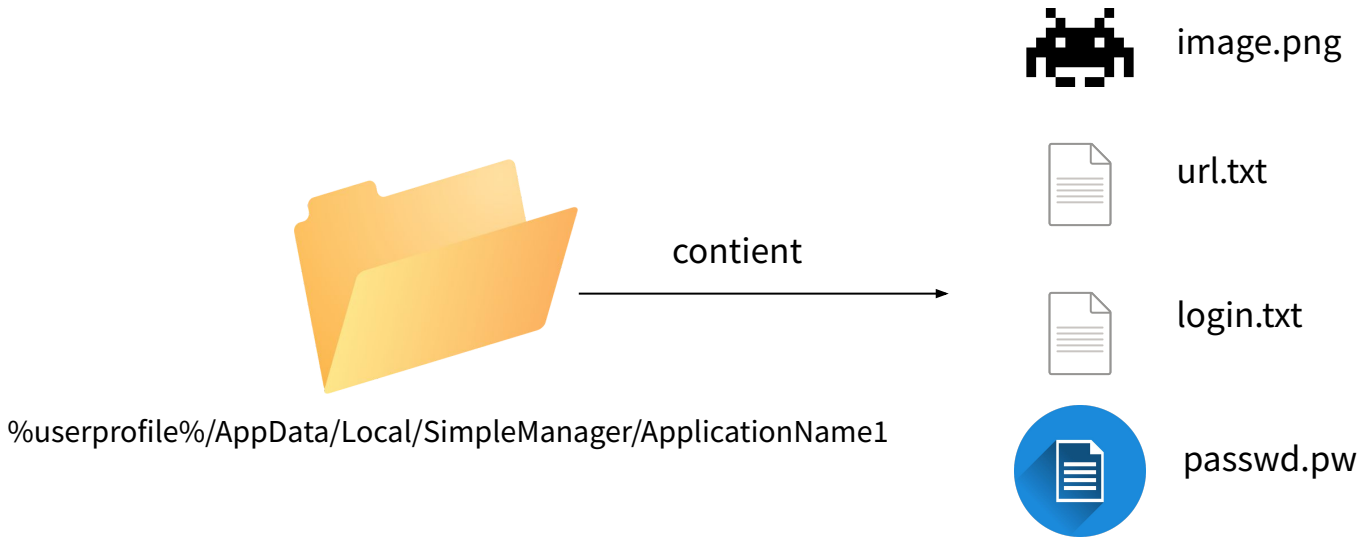
master.pw

contient →

08b5b6491249d55a305827167308e12bd190200aa0f78b6d59b293398fb1338d1
db1fd5e8059cdfd1d2849fe528532066505867250fd29560793d279edc694a1

Lors du lancement de l'application (hors première utilisation), le mot de passe maître est demandé. Une vérification est faite entre le haché du mot de passe saisi et le contenu du fichier "master.pw". Le gestionnaire de mot de passe ne servira que la page de connexion tant que le mot de passe maître n'est pas correct (**ou s'il y a une collision dans la fonction sha512**).

Vue du Système de Fichiers (Windows)



Détails du fichier “passwd.pw”

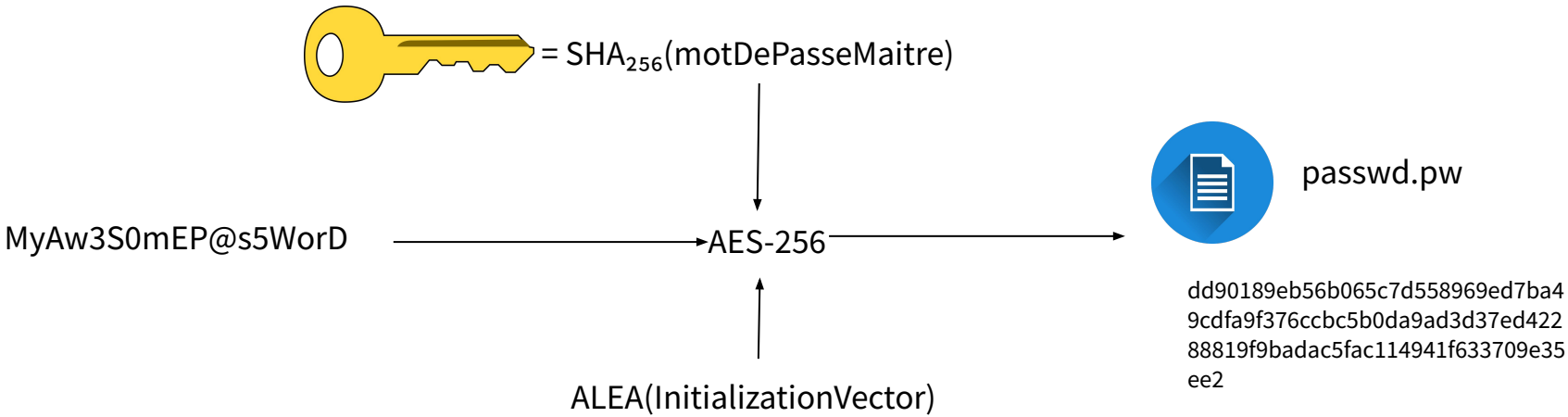
passwd.pw

contient →

dd90189eb56b065c7d558969ed7ba49cdfa9f376ccbc5b0da9ad3d37ed4228881
9f9badac5fac114941f633709e35ee2

Le fichier “passwd.pw” contient le chiffré du mot de passe saisi pour l’élément en utilisant la fonction “aes-256” avec comme clé le haché (sha-256) du mot de passe maître.

Détails du fichier “passwd.pw” (suite)



PS: une partie aléatoire est utilisée pour avoir 2 chiffrés différents pour 2 mots de passe identiques

Résumé

- Mots de passe maître haché enregistré localement
- Mots de passe chiffrés enregistrés localement
- Déchiffrement des mots de passe uniquement lors de l'affichage de l'élément
- Utilisation du mot de passe maître pour chiffrer/déchiffrer le mot de passe de chaque élément
- Ajout d'un aléa pour le chiffrement