



# Des coffres forts à mots de passe

Serge Aumont

RSSI Université de Rennes 1

- Des centaines de mots de passe partagés par les équipes (mots de passe système, bases de données, services externes, ...)
- Pas d'outil de gestion unifiée, pas d'interface pratique et sûr.
- De mauvaises pratiques pour se simplifier la vie :
  - Un même mot de passe pour plusieurs services
  - Des mots de passe simplistes
  - Pas de renouvellement
  - Trop souvent usage d'un compte avec tous les privilèges

# L'existant de la DSI

- Des cahiers papiers dans un coffre ou ... dans les tiroirs des bureaux.
- Pas de taxonomie : on ne sait pas toujours à quoi sert un mot de passe noté sur un support papier.
- On ne sait pas qui y a eu accès.
- On ne sait presque jamais comment le changer.
- Risques :
  - perte ou indisponibilité
  - divulgation accidentelle
  - etc.

# Le besoin

- Un outil **sûr** (confidentialité, intégrité, disponibilité)
- Simple et pratique, accepté de tous.
- Facilitant la mise œuvre d'une politique de mot de passe sur l'ensemble du périmètre de la DSI.
- Mêmes besoins pour d'autres composantes.

# Le produit KeePass

**KeePass 2 est retenu parce que :**

- **Certifié par l'ANSSI (une version windows seulement).**
- **Produit spécifiquement dédié aux mots de passe.**
- **Richesse fonctionnelle : métadonnées (date de création, d'expiration, historique des changements, documentation des entrées, etc.) autotype, onglets, recherche, dossier,**
- **Support natif de webdav avec gestion des écritures concurrentes.**

## Concilier

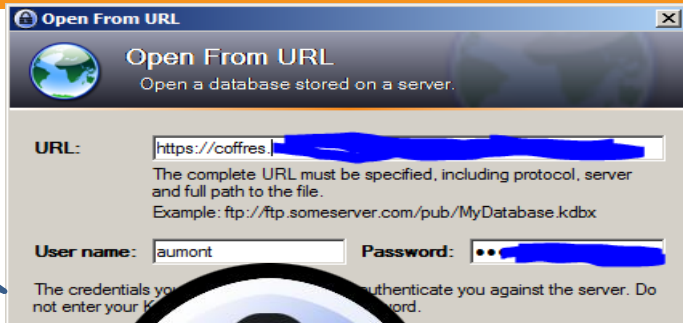
- Principe du « besoin d'en connaître »
- Aucune duplication d'information
- Pour chacun, au plus 3 coffres à connaître

## Choix des coffres :

- 1 par équipe (direction, proximité, système, réseau, applicatifs)
- 1 coffre finances + 1 coffre RH
- RSSI

# Serveur de coffres

Contrôle  
d'accès



Open From URL  
Open a database stored on a server.

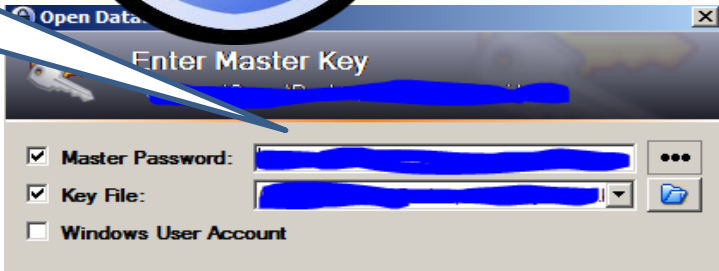
URL:

The complete URL must be specified, including protocol, server and full path to the file.  
Example: ftp://ftp.someserver.com/pub/MyDatabase.kdbx

User name:  Password:

The credentials you enter will be used to authenticate you against the server. Do not enter your keyboard.

Protection en  
profondeur  
(chiffrement)

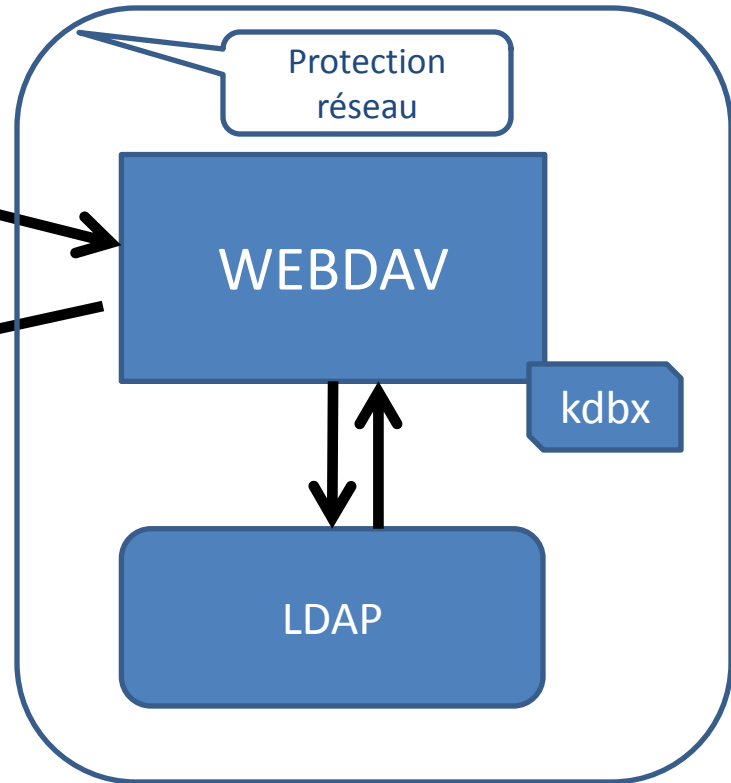


Enter Master Key

Master Password:

Key File:

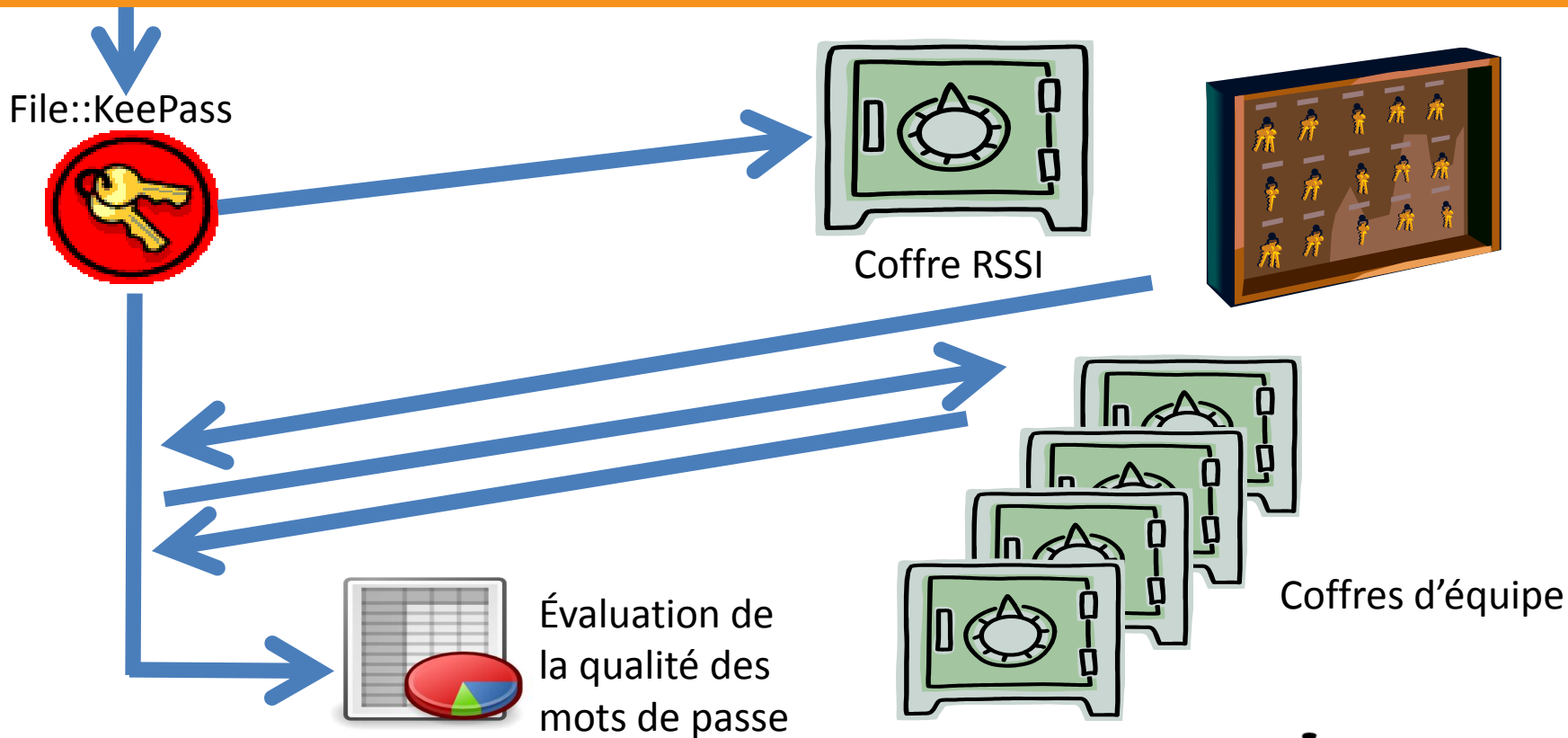
Windows User Account



# Le coffre RSSI

- **Le coffre RSSI contient les passphrases des autres coffres.**
- **Ce coffre est donc le plus sensible, clé composite (1 fichier + 1 passphrase)**
- **Les passphrases sont générées avec un plugin KeePass et distribuées par mails chiffrés S/MIME**
- **Interdiction d'imprimer ou de fixer sur tout autre support les passphrases et les coffres.**

- **Les coffres sont sauvegardés comme le reste du serveur.**
- **En plus, une sauvegarde sur clé USB (SLC) pour faire face à une panne grave impactant le service de coffre.**



- **Service en passe d'être ouvert aux composantes de l'université sur la base d'un contrat de service.**
- **Gérant technique du coffre désigné par le DU**
- **Recouvrement par le RSSI à défaut par le FSD et le DSI conjointement**

- **Participation active des personnels donc amélioration sensible des pratiques.**
- **Bonne disponibilité.**
- **La problématique des mots de passe figurant dans les scripts d'administration reste entière.**
- **Relatif échec sur l'exigence de documentation.**

# Question ?