Apple Keychain

Séminaire « gestion des mots de passe »

2RCE – CASSIS

Dijon, le 16 mars 2023

Site universitaire du Creusot – Pôle Numérique et Informatique

Jérôme PERNOT

Présentation

- Keychain d'Apple (trousseau Apple) est un système de gestion et de stockage des mots de passe, des certificats et des clés privées pour les utilisateurs de Mac, iPhone, iPad et autres appareils Apple,
- Keychain a été introduite avec macOS 8.6 en 1999 avec une amélioration en 2003 (clés publiques/privées), en 2013 (synchronisation Icloud) et enfin en 2021 avec de nouvelles fonctionnalités (générateur de mots de passe...).

Fonctionnement

- Keychain permet le stockage des informations sensibles telles que des noms d'utilisateur, des mots de passe, des numéros de carte de crédit et des identités numériques, qui peuvent être utilisées pour remplir automatiquement des formulaires en ligne,
- Les informations sont stockées de manière sécurisée afin de faciliter leur utilisation dans les applications de l'utilisateur.

Stockage crypté

- Les informations sont protégées grâce, notamment, à l’utilisation de clés de chiffrement dérivées du mot de passe de l'utilisateur,
- Les informations ne peuvent être déverrouillées que si l'utilisateur saisit son mot de passe d’ouverture de session,
- Les informations sont stockées et sécurisées grâce à l’utilisation d’un algorithme de chiffrement symétrique (AES 128 en local et AES 256 lors de la synchronisation Icloud).

Synchronisation

- Lors de l’utilisation de plusieurs appareils Apple, tels qu'un iPhone, un iPad et un Mac, il est possible de synchroniser le contenu de Keychain via iCloud,
- Cette fonctionnalité sera paramétrable sur chaque système Apple (macOS et iOS), sous Windows dans les navigateurs Edge et Chrome (via un plugin),
- Cette synchronisation n’est pas encore disponible sous Chrome OS et sous Linux.

Gestion des accès

- Keychain permet de contrôler les applications qui souhaitent accéder aux informations sensibles,
- L’utilisateur peut ainsi autoriser certaines applications à accéder aux informations d’authentification (nom d'utilisateur, mot de passe) mais pas aux informations liées aux cartes de crédit,
- Une application peut accéder, avec autorisation de l’utilisateur à votre trousseau en arrière-plan ou uniquement lorsque l'application est active.

Gestion des mots de passe

- Keychain nécessite la configuration et l'utilisation d'une authentification à deux facteurs lors de l'utilisation d'Icloud,
- Keychain peut générer, à la demande de l'utilisateur, des mots de passe aléatoires et complexes afin de renforcer la sécurité des comptes en ligne,
- Keychain stocke les mots de passe créés par l'utilisateur ce qui permet une saisie automatique lors de la consultation de sites Web en particulier.

Utilisation de Touch ID et de Face ID

- Si votre appareil est équipé de Touch ID ou de Face ID, vous pouvez utiliser ces fonctionnalités pour déverrouiller votre Keychain,
- Ces options permettent d'ajouter une couche de sécurité supplémentaire en s'assurant que seul l'utilisateur autorisé peut accéder aux informations stockées dans Keychain.

Certificats et clés privées

- Keychain peut stocker des certificats numériques et des clés privées, qui sont souvent utilisés pour sécuriser les connexions SSL/TLS et d'autres types de communications sécurisées.

Gestion des identités numériques

- Keychain peut stocker des identités numériques, telles que des certificats de signature numérique et des certificats de chiffrement de courrier électronique,
- Cette option de configuration permet aux utilisateurs de chiffrer et de signer des messages électroniques de manière sécurisée.

Résumé

- Keychain offre, aux utilisateurs de l’écosystème Apple, un niveau de sécurité élevé tout en permettant une utilisation pratique dans les applications de l'utilisateur,
- Le processus de synchronisation des secrets via Icloud est particulièrement bien intégré dans cet écosystème.

Conclusion

- Dans l'ensemble, Keychain fournit des mesures de sécurité robustes pour assurer la sécurité de vos données sensibles,
- Cependant, il est toujours vivement recommandé de prendre des précautions supplémentaires, telles que l'utilisation de mots de passe forts et surtout le maintien de votre parc à jour avec les derniers correctifs de sécurité,
- Keychain n’est une application Open Source et n’est pas labellisée par l’ANSSI à l’inverse de Keepass.

Questions/Réponses

Je me suis largement inspiré des propositions de ChatGPT Bing (présentation, plan, résumé et conclusion) pour réaliser cette présentation.

Pour illustrer mon propos, je vous propose de faire un rapide comparatif entre Keepass et Keychain en posant la question suivante :

Je souhaite disposer d'un comparatif entre Keepass et Keychain.
Ce comparatif sera structurée de la manière suivante :
Introduction, avantages et inconvénients de Keepass et de keychain et enfin une conclusion.

Merci