Trousseau d'accès & mots de passe

Il ne vous aura pas échappé que nous avons de plus en plus d'identifiants et de mots de passe à fournir et il n'est pas toujours évident de trouver un mode de gestion de ces identifiants qui soit à la fois simple ET sûr. Heureusement, Mac OS X dispose de l'utilitaire *Trousseaux d'accès* qui, s'il est bien utilisé, est une excellente solution à ce problème. Nous allons voir comment il fonctionne, comment renforcer sa sécurité et utiliser certaines fonctionnalités assez méconnues et pourtant très utiles.

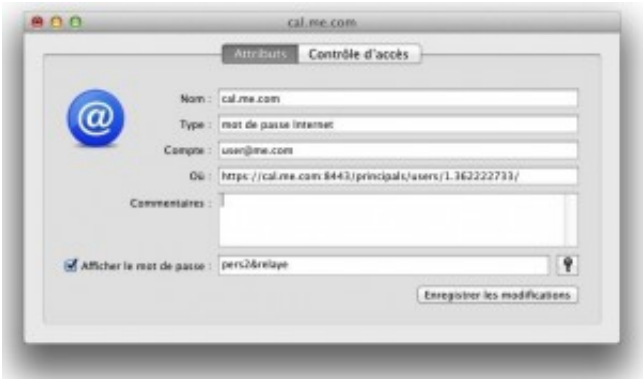
> Quand on a un nombre important de mots de passe à mémoriser, la tentation est grande d'utiliser toujours le même ou d'utiliser des mots de passe trop faciles à "craquer". L'utilisation des trousseaux d'accès de Mac OS X permet de réduire jusqu'à 1 le nombre de mots de passe à retenir : celui qui servira à accéder au trousseau. Cela vous permet d'utiliser des mots de passe très complexes, que vous n'aurez pas à mémoriser. Nous verrons plus bas comment afficher / copier ces mots de passe en cas de besoin.

Vous avez certainement l'habitude que Mac OS X vous demande si vous vous voulez qu'il mémorise dans *Trousseaux d'accès* un mot de passe que vous venez d'entrer dans votre navigateur ou dans votre programme de messagerie, par exemple. Si vous avez répondu "oui", votre mot de passe a été stocké dans un des trousseaux, par défaut le trousseau "session" propre à votre compte utilisateur. Vous avez ainsi autorisé l'application que vous utilisiez à aller chercher l'information dans votre trousseau "session" plutôt que de vous demander le mot de passe à chaque fois qu'il est nécessaire. Un trousseau est un conteneur chiffré (on dit aussi "crypté") : seul un utilisateur possédant le mot de passe pour le déverrouiller (qui est par défaut celui de votre compte utilisateur) ou une application que vous avez autorisée, pourra ouvrir ce trousseau et accéder aux mots de passe qui y sont stockés.

Pour voir le contenu de votre trousseau, rendez-vous dans /Applications/Utilitaires/Trousseaux d'accès. Si la liste des trousseaux n'est pas affichée en haut à gauche de la fenêtre, cliquez sur "Afficher les trousseaux" dans le menu Présentation (ou tapez Cmd+K comme Keychain). Si vous avez conservé les réglages par défaut, le trousseau session sera déverrouillé : il l'a été lorsque vous avez ouvert votre session puisque, comme nous l'avons mentionné plus haut, **le mot de passe par défaut du trousseau "session" est votre mot de passe utilisateur** (cela peut être modifié, comme nous le verrons plus bas). Pour déverrouiller un trousseau : clic droit ou Ctrl-clic > Déverrouiller (ou cliquer sur le cadenas en haut à gauche de la

fenêtre *Trousseaux d'accès*).

Afficher un mot de passe non-mémorisable ou oublié dans le Trousseau d'accès

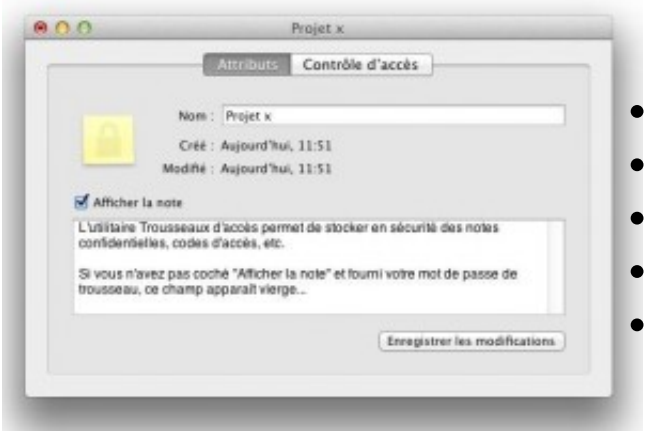


Si vous ne saisissez jamais un mot de passe, parce qu'il est enregistré dans votre trousseau, il est possible que vous l'ayez oublié, ce qui peut être un problème, notamment si vous devez configurer une autre application ou un autre appareil. Heureusement, il est très simple de l'afficher, pour peu qu'on ait le mot de passe du trousseau, évidemment : pour y voire plus clair, cliquez éventuellement sur "Mots de passe" sous "Catégorie", double-cliquez sur la ligne de l'élément du trousseau qui vous intéresse ("cal.me.com" ou "imap.gmail.com" par exemple) pour afficher les informations concernant cet élément. En bas de la fenêtre qui apparaît, cochez la case "Afficher le mot de passe". Vous devrez saisir votre mot de passe de session et le mot de passe recherché s'affichera en clair. Notez que vous pouvez également copier directement le mot de passe dans le presse-papiers, en faisant un clic droit (ou Ctrl+clic) sur l'élément.

Notez également le champ "Contrôle d'accès" en haut de la fenêtre. C'est dans cette sous-fenêtre que vous pourrez ajouter ou retirer l'autorisation d'accès par telle ou telle application, entre autres.

Que peut-on stocker dans les Trousseaux d'accès ?

L'utilitaire *Trousseaux d'accès* est assez méconnu : il est le plus souvent utilisé à la demande du système, pour stocker des mots de passe internet ou d'applications et des certificats. Mais vous pouvez également y enregistrer d'autres informations confidentielles, telles que :



- des notes sécurisées
- des codes d'accès
- des codes PIN
- des numéros de série
- toute autre information à laquelle vous voulez pouvoir accéder avec un mot de passe unique

Cela se fait très simplement par le menu Fichier > Nouvel élément de mot de passe

ou Nouvel élément de note sécurisée. Si vous stockez un code d'accès ou un code PIN via "Nouvel élément de mot de passe", ne vous préoccupez bien sûr pas de l'indicateur de sécurité : ce sont des mots de passe courts mais ils ne sont pas destinés à être utilisés sur le web et sont protégés par le chiffrement du trousseau.

Evidemment, plus ces informations sont sensibles, plus des mesures de sécurité supplémentaires seront envisagées, même si les trousseaux sont sécurisés par chiffrement Triple DES (3DES). Nous y reviendrons.

Créer des trousseaux d'accès supplémentaires

En plus du trousseau session créé automatiquement, vous pouvez créer autant de trousseaux que vous le jugez utile, contenant autant d'éléments (clés) que vous le souhaitez. Cela peut s'avérer utile pour classer les éléments confidentiels par catégorie, en fonction de leur degré de sensibilité, la fréquence d'accès, etc. Vous pouvez par exemple regrouper tous les éléments relatifs à vos comptes mails et autoriser seulement votre programme de messagerie à y accéder. Cela vous évite de vous ré-authentifier à chaque fois que programme relève votre courrier. Cette remarque ne s'applique pas, bien sûr, si vous conservez ces éléments dans votre trousseau de session avec les réglages par défaut…

Pour créer un nouveau trousseau dans *Trousseaux d'accès*, allez dans Fichier > Nouveau Trousseau. Vous devrez associer un mot de passe à ce trousseau, qui pourra être le même que celui de votre trousseau "session" ou un autre, le tout étant de ne pas l'oublier, car vous n'aurez pas de moyen de le récupérer (vous seriez obligé de supprimer le trousseau et d'en recréer un).

Comme nous l'avons vu, le trousseau par défaut est "session" : si vous n'avez rien changé, c'est dans celui-ci qu'une application stockera les informations. Cela conviendra à la grande majorité des utilisateurs, mais il est possible de changer le trousseau par défaut (clic droit ou Ctrl+clic > "Désigner [x] comme trousseau par défaut". Le trousseau par défaut apparaît en gras. Cependant, il est généralement plus simple de conserver le trousseau "session" par défaut pour stocker les mots de passe web/mail, et d'utiliser d'autres trousseaux pour stocker d'autres types d'éléments. Notez que vous pouvez déplacer des éléments d'un trousseau à un autre.

Nous allons maintenant voir comment renforcer la sécurité du trousseau "session".

Renforcer la sécurité du trousseau "session"

Comme nous l'avons vu, le mot de passe par défaut de votre trousseau "session" est

celui de votre compte utilisateur, et ce trousseau est automatiquement déverrouillé lorsque vous ouvrez… votre session utilisateur.

Si vous voulez ajouter un niveau de sécurité supplémentaire, vous pouvez modifier les réglages de ce trousseau pour qu'il se verrouille au bout de x minutes d'inactivité et/ou pendant la suspension d'activité de votre Mac. Faites un clic droit (ou Ctrl+clic) sur le trousseau > Modifier les réglages du trousseau "session" et définissez les options qui vous conviennent. Notez que toute connexion à votre trousseau par une application (Mail par exemple) remettra le délai de verrouillage au temps que vous avez défini.

Vous pouvez également **définir un mot de passe de trousseau différent de celui de votre compte utilisateur** :

1. Faites un clic droit (ou Ctrl+clic) sur le trousseau session et cliquez sur "Modifier le mot de passe…"
2. Saisissez le mot de passe actuel, entrez le nouveau et confirmez-le. Vous pouvez utiliser l'Assistant mot de passe en cliquant sur la clé à droite du champ "Nouveau mot de passe". N'oubliez pas que votre trousseau ne sera plus déverrouillé automatiquement à l'ouverture de votre session (c'est le but…) ! Il est donc préférable de choisir un mot de passe fort mais mémorisable (voir la section "Assistant mot de passe"). N'oubliez pas que si vous perdez ou oubliez ce mot de passe, **vous n'aurez pas de moyen de le récupérer** et devrez recréer un trousseau vide ! Vous pouvez le stocker en lieu sûr, **dans une image disque ou un fichier chiffré(e)**, par exemple.
3. Modifiez ensuite les réglages du trousseau, comme vu plus haut.
4. Vous pouvez également définir des options de sécurité différentes pour certains éléments du trousseau, comme nous allons le voir dans la section suivante. Certaines informations sont plus confidentielles que d'autres ce qui peut justifier un petit effort supplémentaire…

Renforcer la sécurité d'un élément de trousseau d'accès

Chaque trousseau contient généralement plusieurs éléments. Vous pouvez affiner les réglages de sécurité pour chacun d'eux, notamment pour définir quelles applications sont autorisées à y accéder. Voici comment faire :

1. Double-cliquez sur un des éléments.
2. Cliquez sur l'onglet Contrôles d'accès et authentifiez-vous si besoin.
3. Sélectionnez "Confirmer avant d'autoriser l'accès". Mac OS X vous demandera

ainsi confirmation avant de transmettre l'information confidentielle à une application.
Sauf exception, il n'est pas conseillé de choisir "Autoriser l'accès à cet élément par toutes les applications" : cela autorise l'accès sans confirmation à tout programme, quand le trousseau est déverrouillé, ce qui est un risque potentiel.

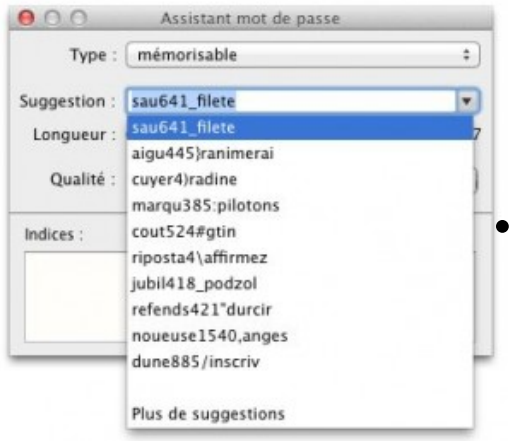
4. Sélectionnez "Demandez le mot de passe du trousseau" pour les éléments les plus sensibles, notamment tout ce qui concerne votre identification personnelle (certificats/clés privées, etc.). Cela peut être une bonne idée de créer un trousseau distinct pour ce type d'éléments.
5. Vérifiez les applications listées sous "Toujours autoriser l'accès par ces applications". Pour en supprimer une, sélectionnez-la et cliquez sur le signe "-". Il y a également un signe "+"…

L'Assistant mot de passe de Mac OS X

Sauf si sa découverte ne peut avoir aucune conséquence sérieuse, le choix d'un mot de passe fort (sûr) est très important et trop souvent négligé : il n'est pas raisonnable de protéger un accès avec le nom de son chien, quand ça n'est pas son propre prénom, et pourtant nous le voyons fréquemment ! La cybercriminalité n'est pas un mythe et ne fera qu'augmenter. Les cas de personnes qui ont eu la surprise d'avoir à rembourser un crédit qu'ils n'avaient pas souscrit ou à être dépossédé d'un bien, ne sont pas si rares… Même si les conséquences sont (en général) moins sérieuses mais tout de même problématiques, le piratage de comptes e-mails est fréquent et c'est la plupart du temps à cause de la faiblesse d'un mot de passe. Ne devenons pas totalement paranoïaques mais, pour le dire avec le sourire, "il ne suffit pas de ne pas être parano pour ne pas être suivi" !

Mac OS X dispose d'un utilitaire "Assistant mot de passe" accessible depuis les comptes utilisateurs et les Trousseaux d'accès. Cet utilitaire permet d'évaluer la qualité d'un mot de passe que vous saisissez ou en générer un automatiquement, selon les critères que vous précisez.

Les choix proposés sont :

- 

Manuel : l'Assistant mot de passe évalue la qualité du mot de passe que vous saisissez et, si elle est faible, vous donne des suggestions pour l'améliorer.
- **Mémorisable** : l'Assistant génère une liste mots de passe mémorisables dans un menu déroulant, en fonction de la longueur que vous avez définie à l'aide du curseur. Vous pouvez vous inspirer d'un d'une des suggestions pour choisir un mot de passe que vous mémoriserez plus facilement.
- **Lettres & Chiffres** : sans commentaire si ce n'est que vous pouvez définir la longueur.
- **Chiffres seulement** : idem.
- **Aléatoire** : idem.
- **Conforme à FIPS-181** : ici aussi vous définissez la longueur et l'Assistant génère un mot de passe conforme au standard FIPS-181 (**F**ederal **I**nformation **P**rocessing **S**tandards), composé d'un mélange de caractères en minuscules, majuscules, de ponctuation et de chiffres.

  De manière générale et en fonction de la sensibilité des informations à protéger, utilisez des mots de passe suffisamment longs (10-12 caractères en moyenne). Nous avons vu que Trousseaux d'accès vous évite d'avoir à mémoriser *tous* vos mots de passe, mais il y en a que l'on doit ou préfère mémoriser. Avec un peu d'imagination, il est tout à fait possible de trouver un mot de passe à la fois "solide" et facile à mémoriser : on peut *par exemple* combiner deux mots volontairement mal orthographiés (évitez les mots présents dans les dictionnaires) et les séparer d'un chiffre et d'un signe de ponctuation s'il est autorisé…

Les certificats

Un certificat est une information chiffrée (ou "cryptée") de manière à ce qu'elle puisse circuler en sécurité sur internet, via un navigateur, un logiciel de messagerie, etc. Quand vous communiquez avec un site sécurisé, vos informations personnelles, numéros de cartes de crédit, etc., ne circulent heureusement pas "en clair"…

Les certificats sont émis par des autorités de certification comme VeriSign ou Entrust, par exemple. Sans entrer dans les détails, lorsque vous vous connectez à un site dit

“sécurisé” (https://), le système vérifie la validité du certificat. S’il n’est pas valide (non répertorié ou expiré) ou introuvable, vous recevez un message d’alerte dont il est vivement conseillé de tenir compte, à moins que vous sachiez vraiment ce que vous faites.

Vous avez probablement déjà des certificats dans votre trousseau, qui vous permettent d’accéder rapidement à des sites sécurisés ou autres ressources en ligne. Si besoin, vous pouvez également en ajouter manuellement.

Ajouter un certificat à *Trousseaux d’accès* manuellement

1. Faites un double-clic sur le fichier certificat (ou Fichier > Importer si vous êtes dans Trousseaux d’accès).
2. Dans la fenêtre qui apparaît, cliquez sur le bouton “Afficher les certificats” si vous souhaitez en vérifier le contenu.
3. Choisissez le trousseau dans lequel vous voulez l’enregistrer, dans le menu déroulant.
4. Cliquez sur “Ajouter”

Notez que Trousseaux d’accès n’acceptera bien sûr d’importer que des certificats dont il connaît l’extension (encodage PKCS12 DER –.p12 ou .pfx et PKCS7 DER — .p7r,.p7b,.p7m,.p7c,or.p7s)

Mais où sont stockés les Trousseaux d’accès ?

Ils sont dans votre Bibliothèque personnelle : /Utilisateurs/VotreCompte/Bibliothèque/Keychains. A partir de Mac OS X 10.7 (Lion), cette Bibliothèque est cachée par défaut, mais vous pouvez y accéder par le menu “Aller” du Finder, en appuyant sur la touche “Alt”.

Si vous voulez rendre votre Bibliothèque visible en permanence, lancez /Applications/Utilitaires/Terminal et tapez la commande suivante :

`chflags nohidden ~/Library` (puis validez avec la touche Entrée…)

Vous pouvez créer un raccourci dans votre barre latérale, en y faisant glisser le dossier Bibliothèque. De cette manière, vous n’aurez pas à ré-exécuter cette commande après une mise à jour qui l’aurait re-masquée…

Si vous voulez re-masquer votre Bibliothèque vous-même :
`chflags hidden ~/Library`