Installation de votre certificat racine

Pour devenir une véritable autorité de certification, vous devez obtenir votre certificat racine sur tous les appareils du monde.

> Mais nous n'avons pas besoin de devenir une véritable autorité de certification. Nous devons simplement être une autorité de certification pour les appareils que vous possédez.

Nous devons ajouter le certificat racine à tous les ordinateurs portables, ordinateurs de bureau, tablettes et téléphones qui accèdent à vos sites HTTPS. Cela peut être un peu pénible, mais la bonne nouvelle est que nous n'avons à le faire qu'une seule fois. Notre certificat racine sera valable jusqu'à son expiration.

1. Ajout du certificat racine au trousseau macOS Monterey :

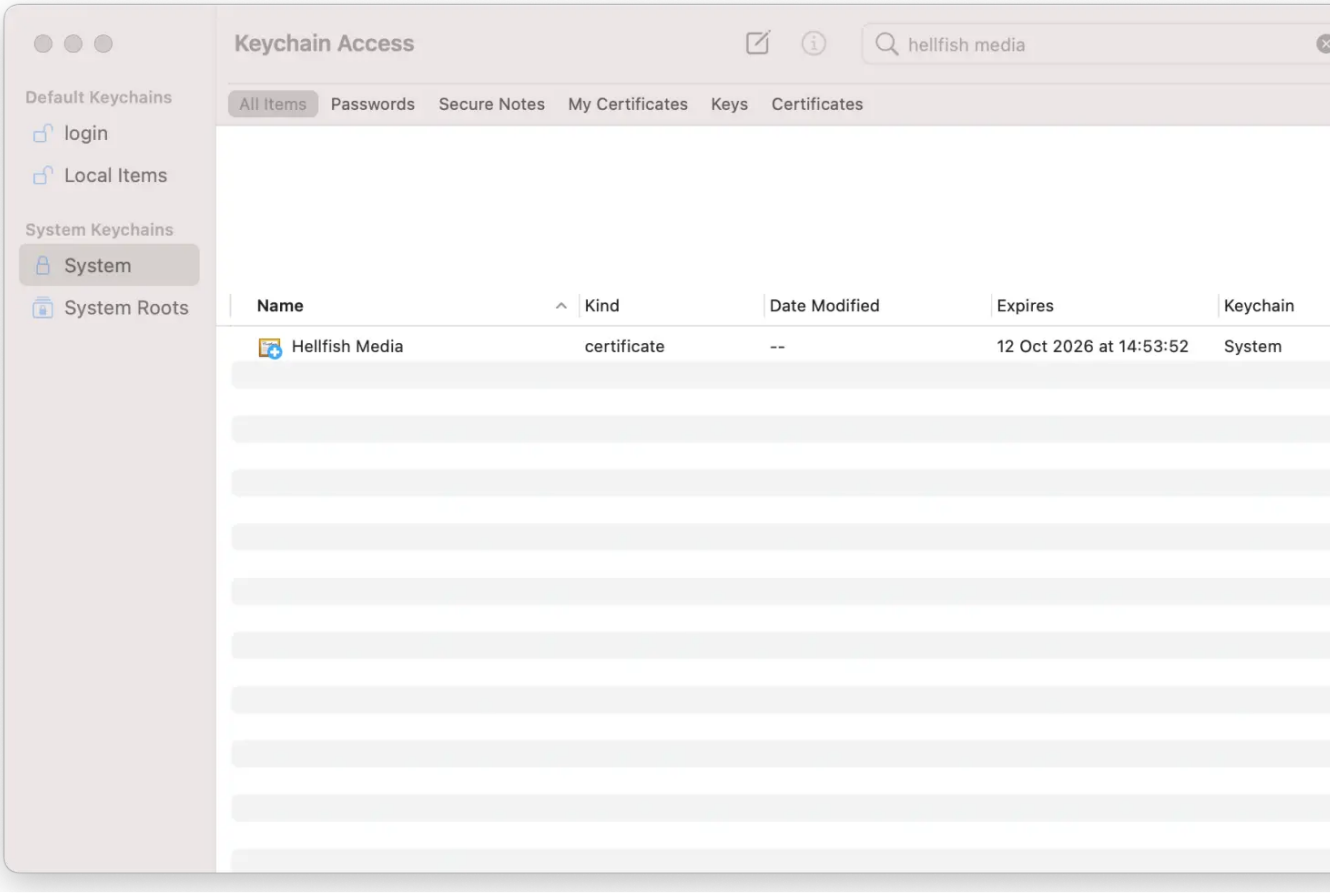
Via le CLI :

```
sudo security add-trusted-cert -d -r trustRoot -k "/Library/Keychains/System.keychain" myCA.pem
```

Via l'application Trousseau macOS :

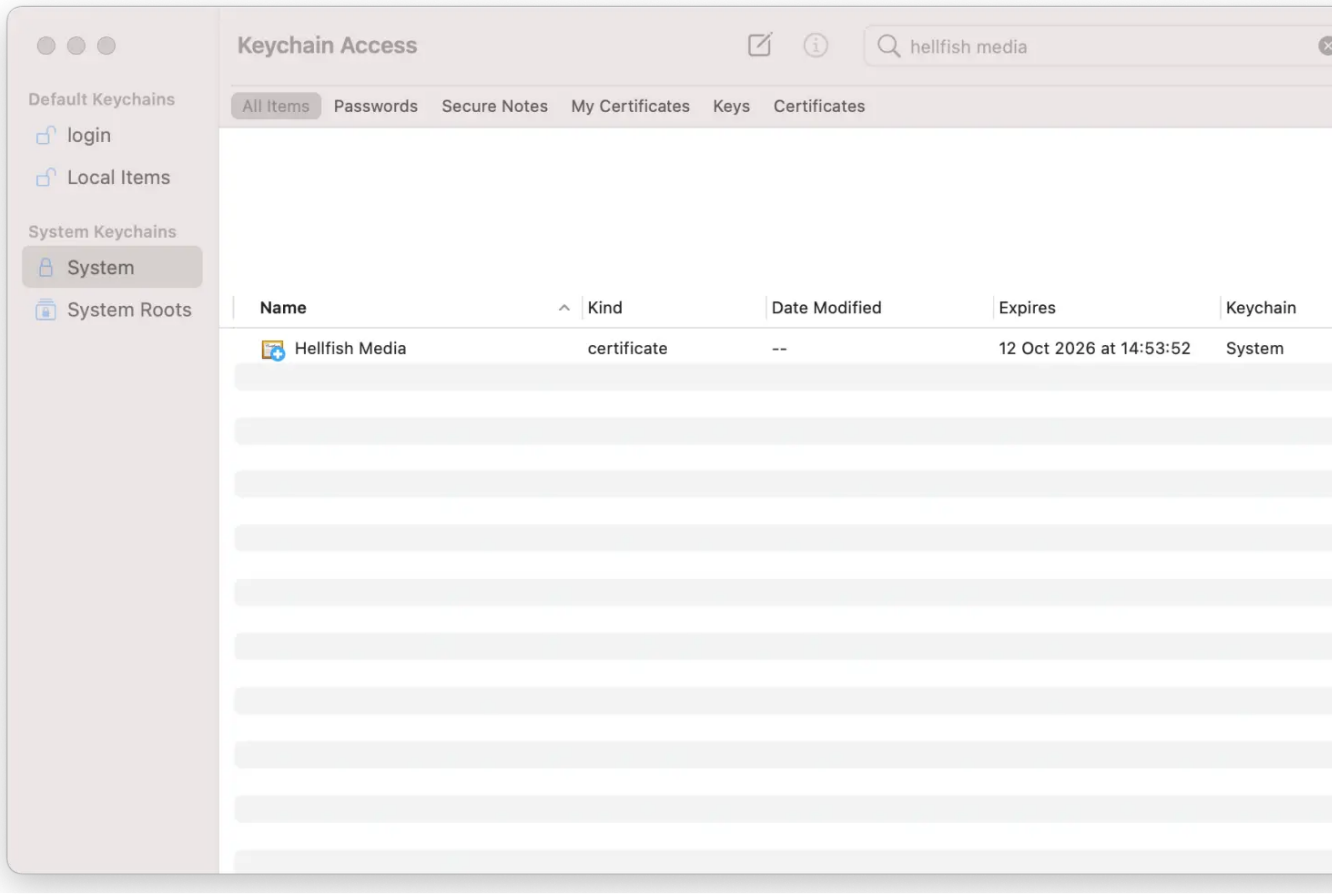
1. Ouvrez l’application Trousseau macOS
2. Si nécessaire, assurez-vous d'avoir sélectionné le **trousseau système** (les anciennes versions de macOS utilisent par défaut ce trousseau)
3. Allez dans **Fichier > Importer des éléments…**
4. Sélectionnez votre fichier de clé privée (c'est-à-dire `myCA.pem`)

5. Recherchez ce que vous avez répondu comme nom « Nom commun » ci-dessus



6. Double-cliquez sur votre certificat racine dans la liste
7. Développer la section **Confiance**

8. Modifiez la case à cocher « Lors de l'utilisation de ce certificat : » sur **Toujours faire confiance**



9. Fermer la fenêtre du certificat
10. Pendant le processus, il peut vous demander de saisir votre mot de passe (ou de scanner votre doigt), faites-

> Félicitation

2. Ajout du certificat racine à Linux :

1. S'il n'est pas déjà installé, installez le `ca-certificates` package. `sudo apt-get install -y ca-certificates`
2. Copiez le `myCA.pem` fichier dans le `/usr/local/share/ca-certificates` répertoire en tant que `myCA.crt` fichier. `sudo cp ~/certs/myCA.pem /usr/local/share/ca-certificates/myCA.crt`
3. Mettre à jour le magasin de certificats. `sudo update-ca-certificates`

Vous pouvez vérifier que le certificat a été installé en exécutant la commande suivante :

```
awk -v cmd='openssl x509 -noout -subject' '/BEGIN/{close(cmd)};{print | cmd}' < /etc/ssl/certs/ca-certificates.crt | grep nl
```

✅ Il est correctement installé, vous verrez les détails du certificat racine.

3. Ajout du certificat racine à Windows 10 :

1. Ouvrez la « Microsoft Management Console » en utilisant la combinaison de touches **Windows + R** `mmc` , en tapant et en cliquant sur **Ouvrir**
2. Allez dans **Fichier > Ajouter/Supprimer un composant logiciel enfichable**
3. Cliquez sur **Certificats** et **Ajouter**
4. Sélectionnez **Compte d'ordinateur** et cliquez sur **Suivant**
5. Sélectionnez **l'ordinateur local** , puis cliquez sur **Terminer**
6. Cliquez sur **OK** pour revenir à la fenêtre MMC
7. Double-cliquez sur **Certificats (ordinateur local)** pour développer la vue
8. Sélectionnez **Autorités de certification racines de confiance** , cliquez avec le bouton droit sur **Certificats** dans la colonne du milieu sous « Type d’objet » et sélectionnez **Toutes les tâches,** puis **Importer**
9. Cliquez sur **Suivant,** puis **sur Parcourir** . Modifiez la liste déroulante de l'extension de certificat à côté du champ du nom de fichier sur **Tous les fichiers (*.*)** et localisez le `myCA.pem` fichier, cliquez sur **Ouvrir** , puis **sur Suivant.**
10. Sélectionnez **Placer tous les certificats dans le magasin suivant** . « Magasin des autorités de certification racines de confiance » est la valeur par défaut. Cliquez sur **Suivant** , puis sur **Terminer** pour terminer l'assistant.

Revision #3
Created 24 September 2024 21:58:59 by Admin
Updated 24 September 2024 22:19:00 by Admin