SSO
SingleSignOn

Stand: 04.01.25

créé par:
Henning Frey
Tesla Owners Club Helvetia
Postfach
6300 Zug

Table des matières:

1. Introduction

Le TOCH s'efforce d'uniformiser et de simplifier l'accès aux différents systèmes grâce à l'infrastructure informatique qu'il a mise en place. C'est pourquoi une solution de signature unique (SSO) a été mise en place. Ainsi, chaque membre dispose d'un seul login avec lequel il peut se connecter aux différents systèmes.

Malgré la simplification, la sécurité des données ne doit pas être négligée. C'est pourquoi l'accès au moyen d'un nom d'utilisateur et d'un mot de passe n'est plus autorisé. En informatique, pour sécuriser les données à protéger, on parle toujours de "quelque chose que l'on sait" et de "quelque chose que l'on a". Le mot de passe est la partie que l'on "sait". Il faut en outre une autre caractéristique de sécurité, quelque chose que l'on "a". Il peut s'agir d'un code numérique à usage unique ou d'une clé d'accès.

La nouvelle solution SSO exige donc un mot de passe, un nom d'utilisateur et un jeton à usage unique ou Passkey. Le jeton à usage unique doit au moins être disponible. Alternativement, chaque utilisateur peut en outre configurer l'accès via le nom d'utilisateur et la clé d'accès. Dans ce cas, "ce que l'on sait" et "ce que l'on a" sont réunis dans la clé d'accès.

En général, on parle ici d'authentification à deux facteurs ou d'authentification à plusieurs facteurs.

Dès réception de cette documentation, le nouveau compte est disponible pour tous les membres. L'activation de ce compte via l'adresse e-mail TOCH est décrite ci-dessous. Pour cela, il faut une application sur le téléphone portable ainsi qu'un navigateur web sur un autre appareil. Cette documentation vous guide pas à pas à travers les saisies nécessaires dans le navigateur.

Ton nom de connexion est toujours ton adresse e-mail TOCH ...@teslaowners.ch.

Ton adresse e-mail personnelle t'a été envoyée par écrit après ton inscription au club.

Ci-dessous, tu liras souvent les termes "gestion des membres" et "gestion des comptes". La "gestion des membres" est le nouveau logiciel de l'association "DigitalMembers", qui a remplacé notre ancien "Fairgate". Pour la "gestion des comptes", il s'agit simplement de la gestion du compte Single-Sign-On, avec lequel tu peux changer le mot de passe, installer de nouvelles applications Authenticator ou encore créer des Passkeys.

2. Time-Based-Token

L'une des deux composantes de l'authentification multifactorielle est l'identification par un jeton basé sur le temps. Pour ce faire, une application est nécessaire sur le téléphone portable ou la tablette. Cette app se voit attribuer un "secret" (une clé secrète). L'app peut ainsi afficher toutes les 30 secondes un nouveau code de connexion à six chiffres, que le serveur connaît au moment de la connexion. Un tel code ne peut être utilisé qu'une seule fois et n'est valable que 30 secondes

Une telle application, également appelée application Authenticator, devrait être installée par chacun avant de créer son compte TOCH. Veuillez vérifier si vous n'avez pas déjà une telle application sur votre téléphone portable pour d'autres comptes. Dans ces apps, on peut généralement enregistrer autant de comptes que l'on veut. Voici quelques exemples..

2.1. Apple App-Store

Download on the App Store

OTP Auth

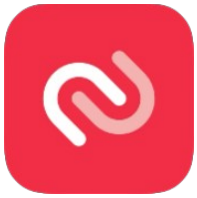
Twilio Authy

Authenticator

2.2. Google Play-Store

GET IT ON Google Play

Authenticator PRO Free 2FA



Twilio Authy

Authenticator

, Twilio Authy, Authenticator

3. Mise en place des données d'accès

Cette section décrit d'abord la première connexion, telle qu'elle doit obligatoirement être effectuée. Ensuite, le chapitre sur la modification du mot de passe et la mise en place d'un mot de passe est facultatif. Les clés d'accès ne sont pas obligatoires, mais peuvent être utilisées pour simplifier l'accès. L'utilisation d'une clé d'accès évite la saisie du mot de passe et du code token.

3.1. Première inscription

Si une application Authenticator (voir chapitre 2 à la page 4) est disponible, une première connexion peut être effectuée. Pour cela, il faut d'abord attribuer le deuxième facteur et ensuite définir le mot de passe. Effectue la connexion sur le PC ou la tablette et en aucun cas avec l'appareil sur lequel l'application Authenticator est installée. Avec cet appareil, tu devras ensuite scanner un code QR avec la caméra. Les images et descriptions suivantes te guideront pas à pas dans le processus.

Ouvre le navigateur web de ton choix et utilise le lien suivant:

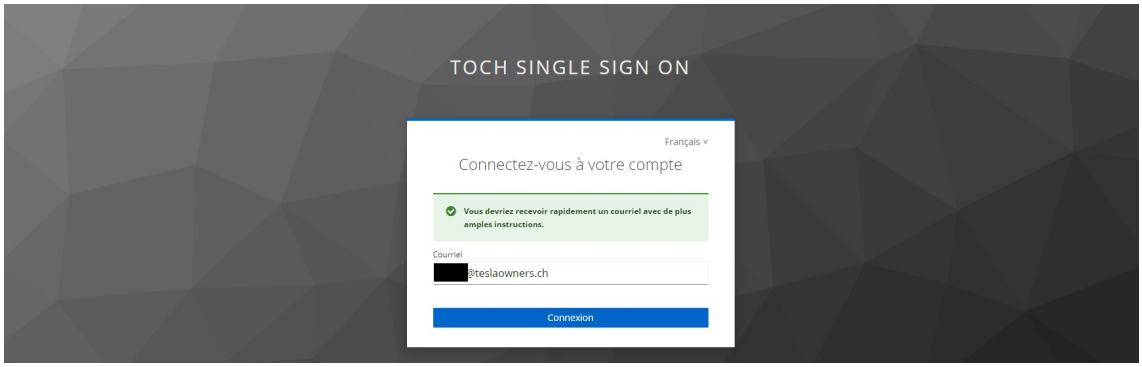
https://sso.teslaowners.ch/realms/TOCH/account/#/

Saisis ton adresse e-mail teslowners.ch comme indiqué sur l'image ci-dessous et clique sur "Connexion":

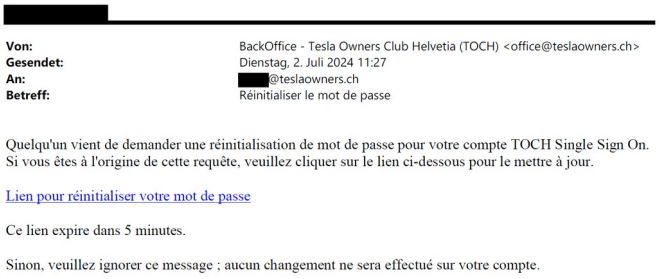
Comme tu n'as pas encore de mot de passe, clique sur "Mot de passe oublié".

N'oublie pas de cliquer sur "Soumettre" sur la page suivante.

La première étape est terminée. Tu devrais maintenant voir la confirmation suivante:



Il est temps de jeter un coup d'œil à ta boîte aux lettres. Tu as reçu un e-mail qui ressemble à l'image ci-dessous.



Von: BackOffice - Tesla Owners Club Helvetia (TOCH) <office@teslaowners.ch>
Gesendet: Dienstag, 2. Juli 2024 11:27
An: [redacted]@teslaowners.ch
Betreff: Réinitialiser le mot de passe

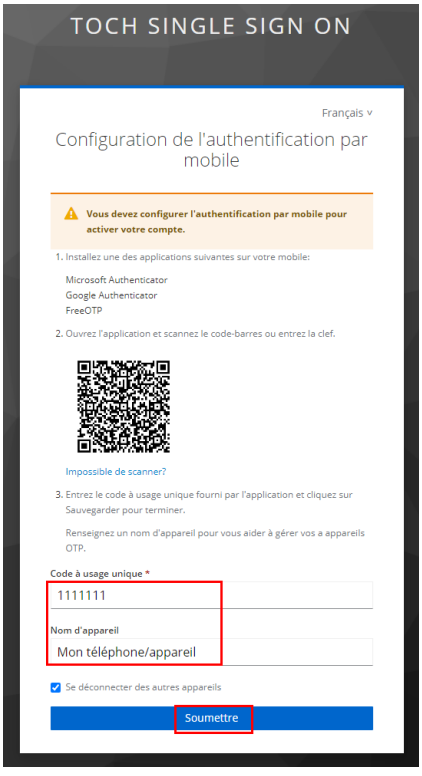
Quelqu'un vient de demander une réinitialisation de mot de passe pour votre compte TOCH Single Sign On.
Si vous êtes à l'origine de cette requête, veuillez cliquer sur le lien ci-dessous pour le mettre à jour.

Lien pour réinitialiser votre mot de passe

Ce lien expire dans 5 minutes.

Sinon, veuillez ignorer ce message ; aucun changement ne sera effectué sur votre compte.

Clique maintenant sur "Lien pour réinitialiser les informations d'identification" dans le mail ci-dessus. Une boîte de dialogue s'ouvre alors (image de droite), qui te demande de scanner un code-barres avec l'application Authenticator à l'aide de la caméra.

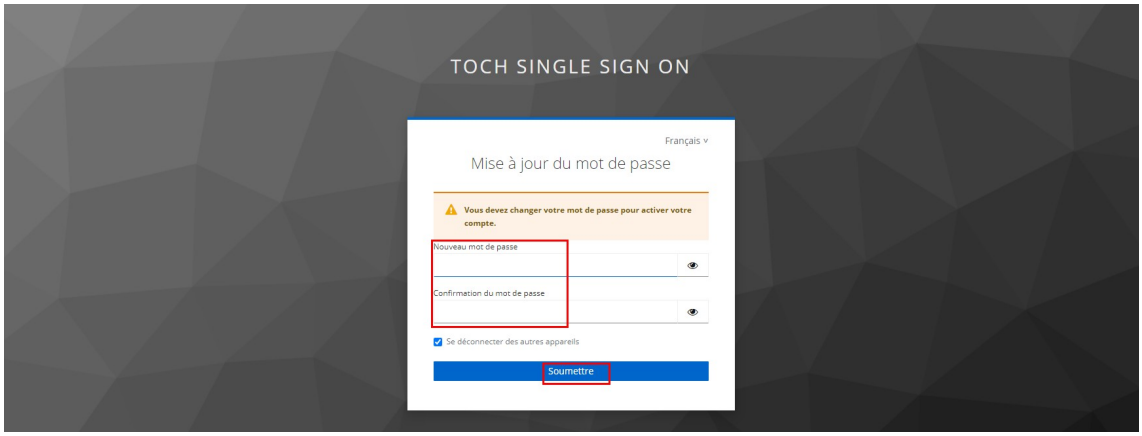


Veuillez noter que vous devez donner à l'application les droits d'accès à la caméra sur votre appareil mobile. Tu peux les retirer à la fin de ce processus.

Avec l'application Authenticator, tu scannes le code-barres. L'application obtient ainsi un "secret" (clé secrète) à partir duquel un nouveau code numérique

à six chiffres, valable une seule fois, est calculé toutes les 30 secondes. Si tu as réussi, l'appli t'indique directement le code. Pour confirmer, tu dois maintenant saisir une fois le code numérique dans le champ "Code à temps" et tu peux ensuite donner un nom à l'application ou à ton appareil mobile dans le champ "Nom de l'appareil".

Si tu as cliqué sur "Envoyer" en haut de la page, il te sera demandé de créer ton nouveau mot de passe.

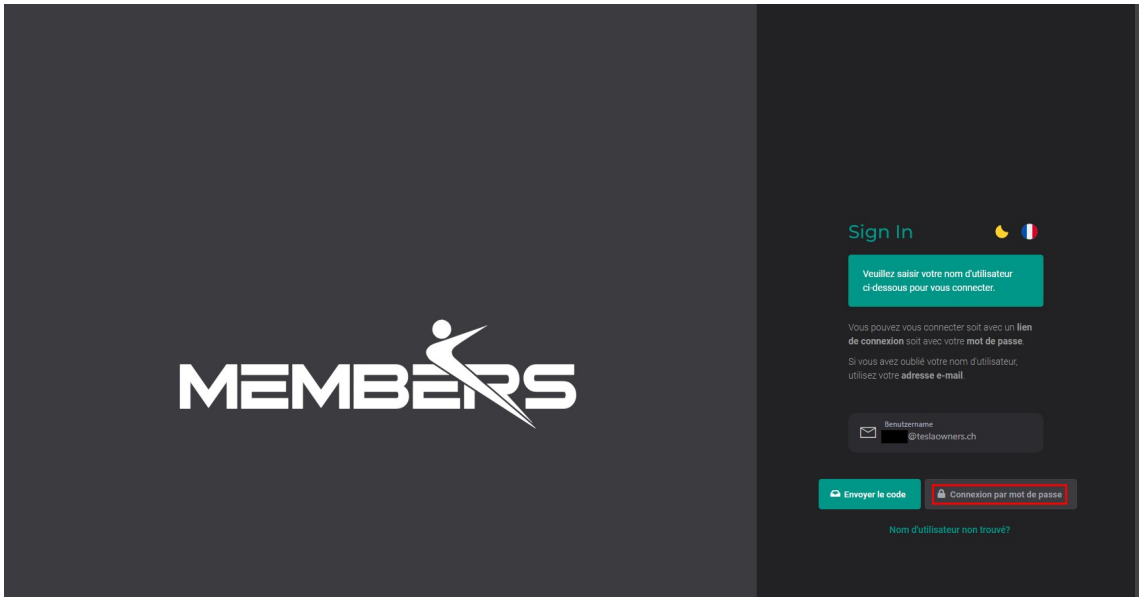


Si tu as cliqué sur "Soumettre", tu as terminé. Tu as configuré ton accès avec succès. Tu peux dès à présent t'inscrire dans la zone des membres de notre site web.

3.2. Inscription à l'administration des membres

Nous allons maintenant décrire l'inscription à la gestion des membres TOCH dans le nouveau logiciel "DigitalMembers". Clique sur le lien suivant, saisis ton adresse e-mail TOCH et clique sur "Mot de passe Login" ::

https://app.digitalmembers.ch



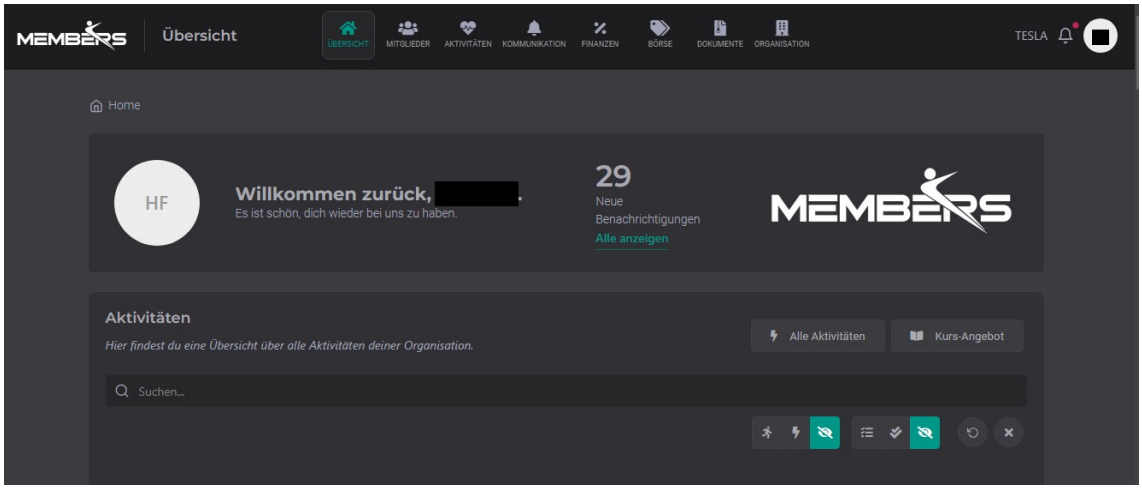
Maintenant, tu dois malheureusement saisir à nouveau ton nom d'utilisateur/adresse e-mail:

Tu seras invité(e) à saisir ton mot de passe:

Et pour finir, le code numérique à six chiffres valable de l'application Authenticator:

Attention toutefois à ce que le code ne soit certainement pas "123456", comme dans l'exemple. Le code de l'application Authenticator est toujours valable pendant 30 secondes et change ensuite. La plupart du temps, l'application indique également quand il expire.

Si tu as suivi toutes les étapes avec succès, tu es maintenant dans le nouvel espace membre:



3.3. Gérer son compte

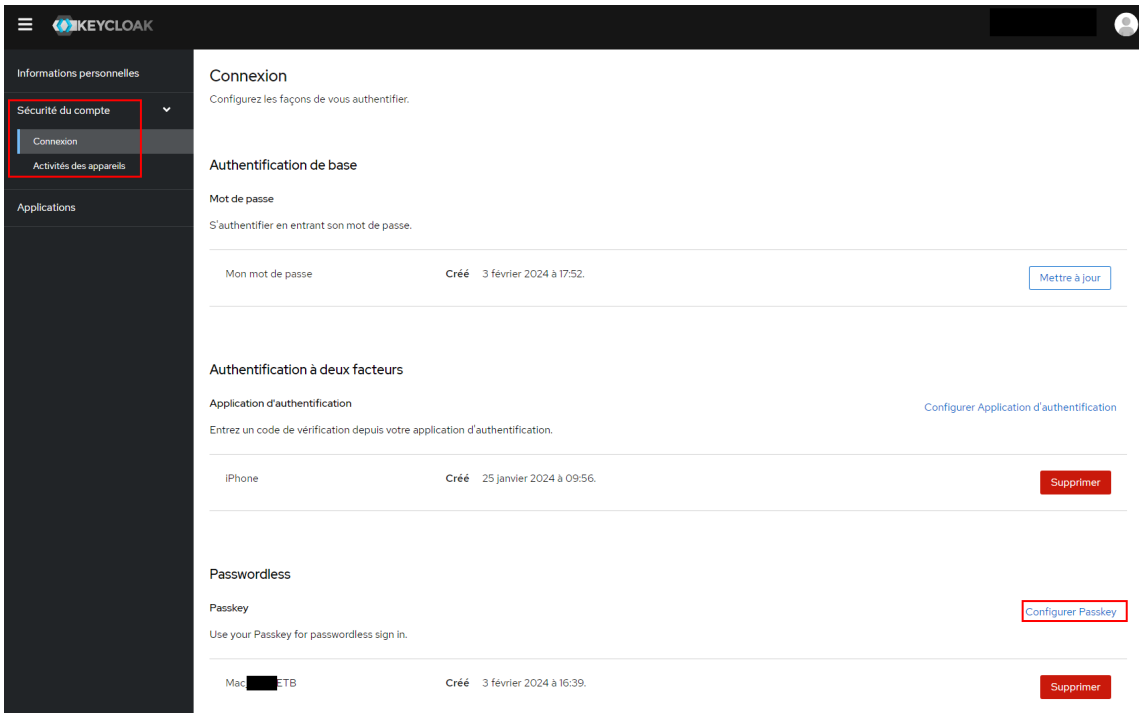
Avec les données d'accès que tu as créées auparavant, tu peux gérer toi-même ton compte. Cela se limite toutefois à la modification du mot de passe et à l'attribution de clés d'accès. Pour ce faire, tu dois ouvrir le lien suivant dans ton navigateur:

https://sso.teslaowners.ch/realms/TOCH/account/#/

La procédure d'inscription est déjà décrite dans le chapitre précédent Fehler: Verweis nicht gefunden à partir de la page Fehler: Verweis nicht gefunden après le lien vers DigitalMembers.

Veuillez noter que la modification des "Données personnelles" n'a aucun effet ici. Cela doit être fait dans la gestion des membres !

Les domaines "Inscription" et "Activité" sous "Sécurité du compte" sont intéressants pour toi:



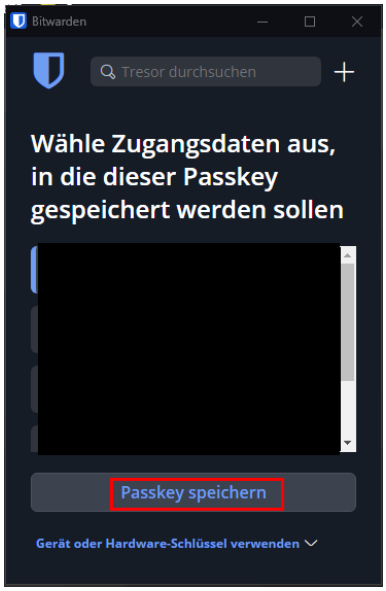
3.4. Mettre en place une clé d'accès

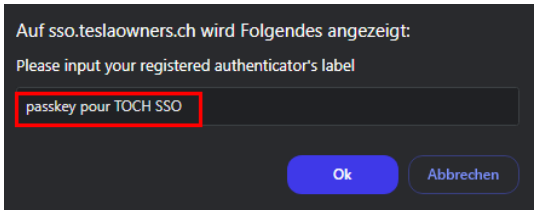
En se basant à nouveau sur le chapitre précédent Fehler: Verweis nicht gefunden à partir de la page Fehler: Verweis nicht gefunden et également sur la dernière image du chapitre précédent, tu trouveras dans la marge de droite "Configurer un passkey". Veuillez cliquer sur ce bouton pour configurer une clé d'accès

Tu dois malheureusement t'inscrire à nouveau. Il s'agit d'une mesure de sécurité prédéfinie que nous ne pouvons malheureusement pas désactiver. Ensuite, tu verras l'image suivante, sur laquelle tu cliqueras sur "Enregistrement":

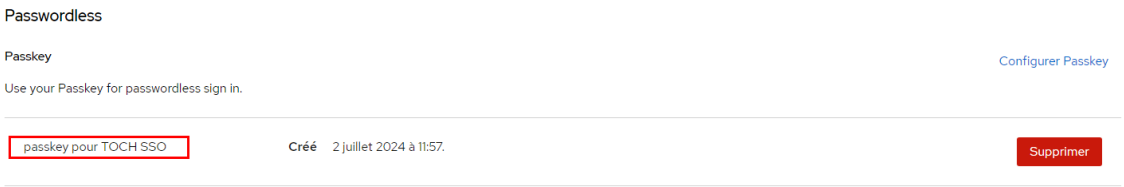
L'étape suivante dépend de la manière dont tu enregistres une clé d'accès sur ton appareil. Si tu utilises un iPhone ou un Android, tu peux le faire sur ton appareil mobile en utilisant ton empreinte digitale ou la reconnaissance faciale. Pour les PC, il existe également des claviers ou des accessoires permettant de reconnaître l'empreinte digitale. Il est également possible d'utiliser un coffre-fort à mots de passe. Voici l'exemple de l'application BITwarden.

Nous enregistrons la clé d'accès dans le coffre-fort des mots de passe et lui attribuons un nom:





Ensuite, nous voyons notre passkey dans la gestion du compte:



Pour terminer, nous décrivons ci-dessous le processus d'inscription avec une clé d'accès.

3.5. Se connecter avec Passkey

Le processus d'inscription commence à nouveau par le nom d'utilisateur, c'est-à-dire l'adresse e-mail TOCH. Peu importe que l'inscription se fasse dans la "gestion des membres" ou dans la "gestion des comptes". Le processus est toujours identique.

Nous commençons donc à nouveau par la saisie de l'adresse e-mail:

Lors de la demande de mot de passe suivante, nous voyons l'option "Essayer une autre méthode" et cliquons dessus:

Nous pourrions maintenant revenir au mot de passe, mais nous voulons continuer ici avec "Security-Token" et nous cliquons dessus:

Il nous est à nouveau demandé de fournir notre clé d'accès. Ici, nous pourrions à nouveau passer au mot de passe, mais nous restons sur "Se connecter avec une Clé de Sécurité" et nous cliquons dessus:

Maintenant, cela dépend de la clé d'accès utilisée, si elle doit être validée par reconnaissance faciale ou par capteur d'empreintes digitales. Dans l'exemple utilisé ici, le gestionnaire de mots de passe BITwarden a été utilisé, il ressemble à ceci:

Lors de l'utilisation du gestionnaire de mots de passe, un mot de passe est toutefois nécessaire, mais il s'agit du mot de passe principal du gestionnaire de mots de passe et il est donc identique pour tous les tokens stockés. Ainsi, chaque compte individuel est protégé par un token différent, mais l'utilisateur n'a besoin que d'un seul mot de passe pour accéder à son coffre-fort de mots de passe. En cas d'utilisation d'une Yubikey ou d'un produit similaire, la clé USB utilisée doit être déverrouillée par une touche.

Index des mots clés

