Authentification multifacteur avec edu-ID

L'**authentification multifacteur** (ou **MFA**, **authentification forte** ou encore **authentification à deux facteurs**) est parfois requis pour divers services afin d'augmenter le degré de sécurité de nos applications (plus d'infos sur notre blog). En plus de votre mot de passe, il vous sera demandé soit

- un **code à usage unique**, généré dans une application prévue à cet usage, appelée **TOTP** (comme **Google Authenticator**),
- de valider une demande **authentification sans mot de passe** utilisant la technologie **Passkey**

L'identité edu-ID inclut l'utilisation de l'authentification multifacteur, et son activation est facile. Pour lire la documentation officielle de SWITCH sur la MFA et l'edu-ID, rendez-vous ici: https://eduid.ch/help?lang=fr#two-step-login.

Activation

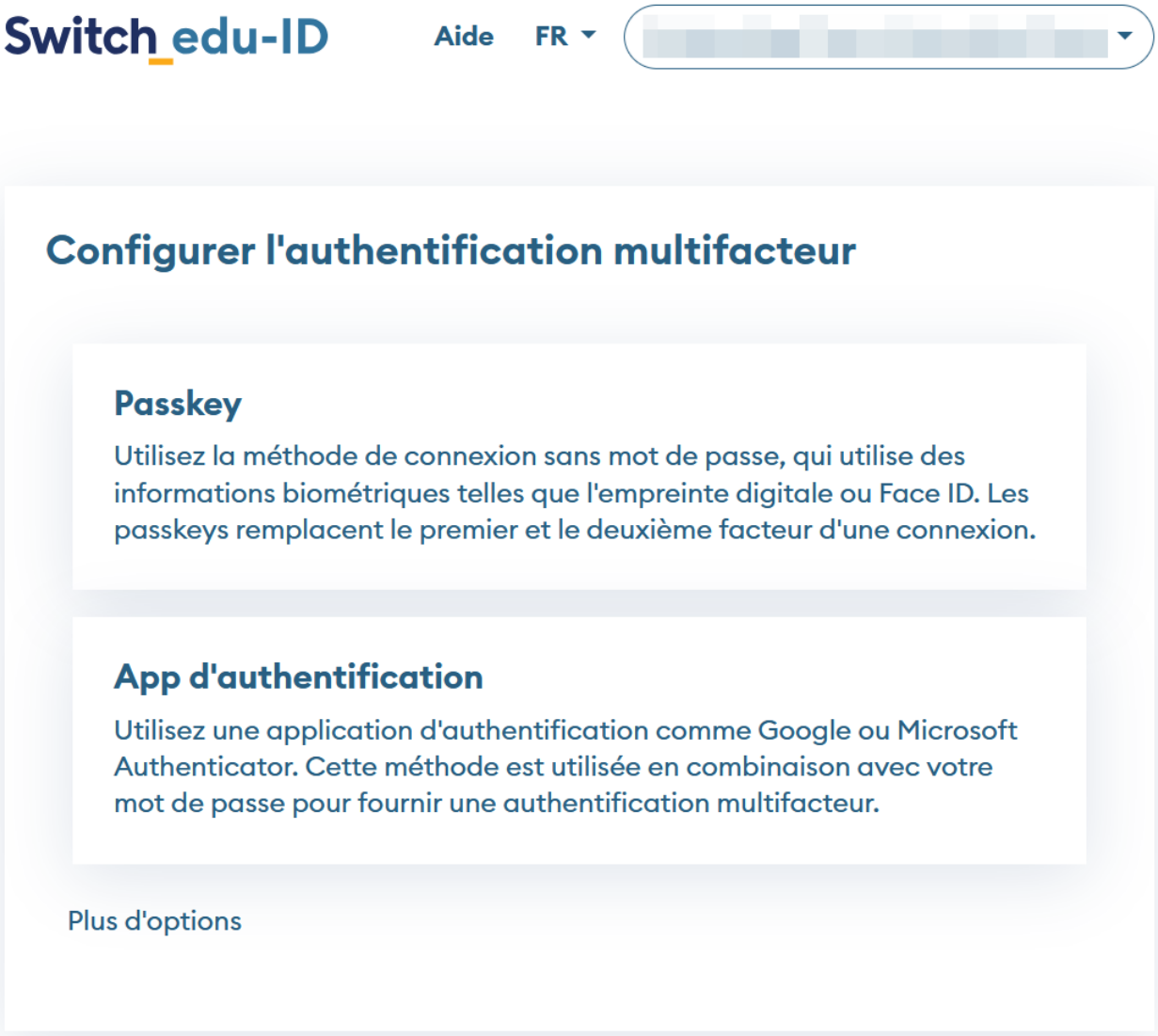
(adapté de la documentation de SWITCH)

Pour **activer** l'authentification en deux étapes, rendez-vous sur votre compte SWITCH edu-ID à l'adresse https://eduid.ch et cliquez sur l'onglet **Sécurité** et cliquez sur le bouton On à côté de **Authentification multifacteur**,



ou allez *directement aux paramètres de l'authentification en deux étapes* (https://eduid.ch/mfa/initial).

Activez ensuite l'une des méthodes d'authentification en deux étapes. Nous vous recommandons d'utiliser une **application mobile d'authentification** pour obtenir vos codes.



App d'authentification

Il vous saura d'abord demandé un numéro de téléphone portable au cas où vous auriez besoin de récupérer votre compte :



Ensuite, il vous faut enregistrer votre clé secrète qui servira à générer les codes :



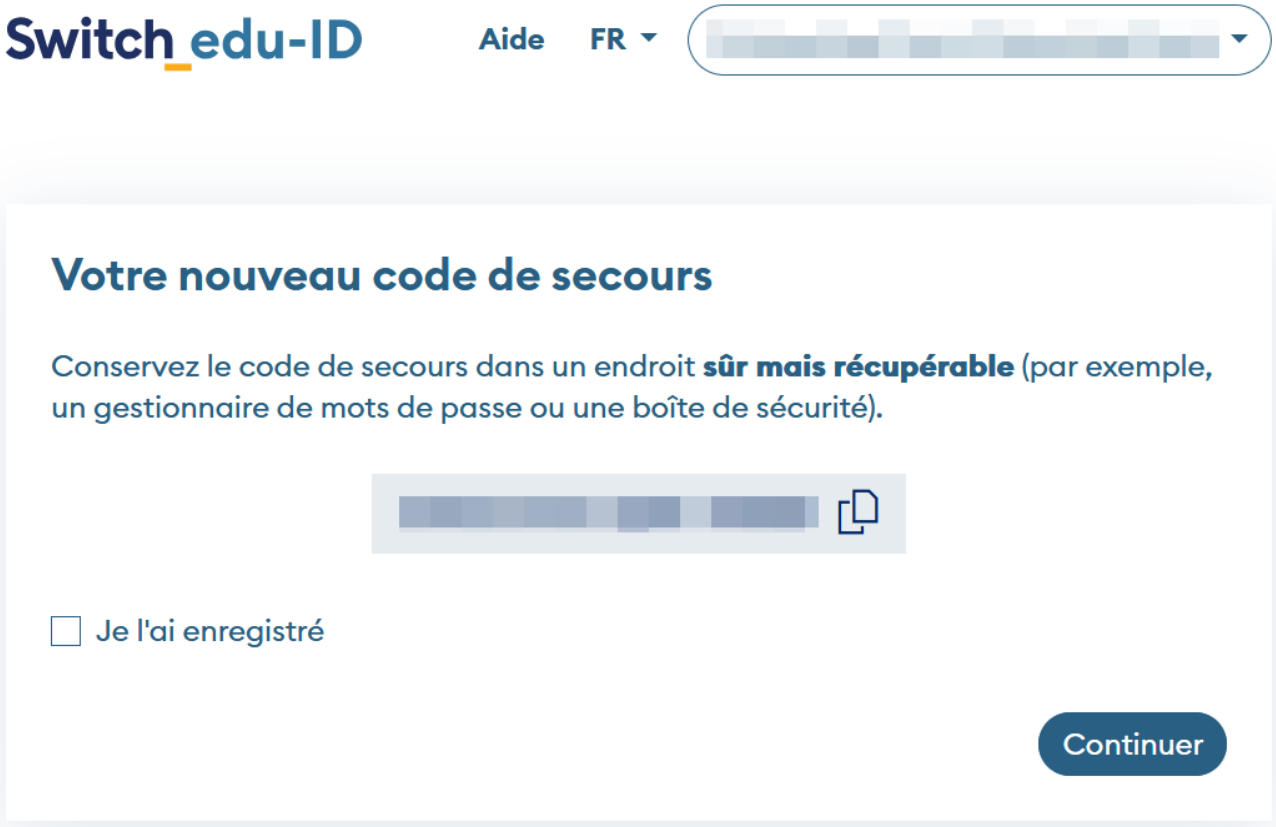
Les applications mobiles suivantes fonctionnent entre autres : **Ente Auth**, Twilio Authy, FreeOTP, Google Authenticator, Microsoft Authenticator, BitWarden Authenticator, ou encore OTP Auth. (D'autres applications qui supportent le standard *TOTP* peuvent également être utilisées.) Plus d'informations sur iBarry.ch. L'application Ente Auth ou l'extension de navigateur 2FAS peuvent être utilisés sans téléphone mobile.

La plupart des applications d'authentification mentionnées ci-dessus fonctionnent également pour d'autres fournisseurs de services, comme Google, Facebook, etc.

> De plus en plus de gestionnaires de mot de passe offrent la possibilité de gérer à la fois vos mots de passe ainsi que le 2e facteur au sein d'une seule et unique app, comme le trousseau macOS (dernière version) ou

BitWarden (version premium). Cela a aussi l'avantage d'être synchronisé sur différents devices.

N'oubliez pas de bien prendre note de votre code de secours et de le sauvegarder.



Passkey

Les *Passkeys* sont une nouvelle technologie d'authentification hautement sécurisée, désormais prise en charge par les principales plateformes internet ainsi que par **SWITCH edu-ID**. Une fois configurées, elles permettent une connexion réellement *sans mot de passe* — plus besoin de saisir votre mot de passe. Vous trouverez plus d'informations ici :

https://eduid.ch/help?lang=fr#two-step-login
ainsi qu'un article de présentation ici :

https://www.ibarry.ch/en/safe-devices/passkeys/

Bien que les Passkeys soient considérées comme le futur standard de l'authentification sécurisée, la technologie est encore émergente. Leur compatibilité varie : tous les systèmes d'exploitation, applications ou appareils ne les prennent pas encore en charge, et plusieurs méthodes de configuration coexistent. Il est important de noter que les Passkeys sont configurées **par appareil**, ce qui signifie que vous devrez généralement en créer une sur chaque ordinateur, téléphone ou navigateur que vous utilisez — sauf si vous utilisez un

gestionnaire de mots de passe synchronisé comme BitWarden, qui permet d'utiliser la même Passkey sur plusieurs appareils.

Vous trouverez plus d'informations dans la FAQ de SWITCH.

Si vous rencontrez des problèmes ou des incompatibilités lors de la configuration ou de l'utilisation des Passkeys, veuillez les signaler au helpdesk.



Il est possible d'activer plus d'une méthode de connexion, et de multiples Passkey.

Désactivation de la MFA

Si vous désactivez la MFA, vous risquez de ne plus avoir accès à certaines ressources ou services qui requiert un 2e facteur. Il vous faudra recommencer le processus de 0 si vous souhaitez la réactiver par la suite.

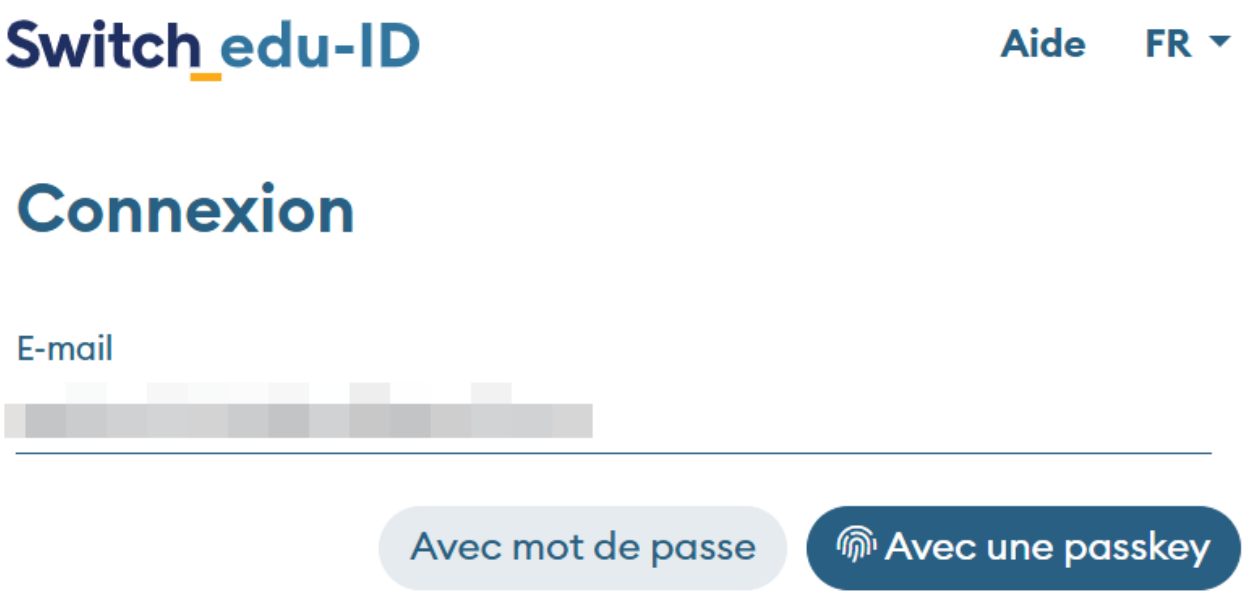
Pour **désactiver** l'authentification en deux étapes, retournez vers l'onglet *Sécurité* et cliquez sur le bouton Off à côté de l'option *Authentification multifacteur* (https://eduid.ch/account/security).



Vous devrez peut-être réinitialiser ou revérifier le code de vérification si vous réactivez ultérieurement une méthode particulière.

Connexion

Lorsque vous vous connecterez à une page nécessitant un deuxième facteur, après avoir entré votre adresse email, selon votre configuration MFA, vous devrez sélectionner soit d'entrer un mot de passe, soit de procéder via une Passkey :



TOTP

Si vous utilisez un mot de passe, renseignez-le



entrez ensuite le code TOTP généré dans l'app que vous aurez configurée au préalable



Questions / Problèmes

Vous trouverez réponse à plusieurs questions concernant l'authentification multifacteur sur le site officiel de SWITCH edu-ID: https://eduid.ch/help?lang=fr#two-step-login

J'ai perdu accès à mon 2e facteur, que faire?

Rendez-vous sur la page https://eduid.ch/mfa-recovery et suivez les instructions.

Créé 2021-04-08 06:42:16 UTC par Chr Gr
Mis à jour 2026-10-02 12:36:20 UTC par Chr Gr