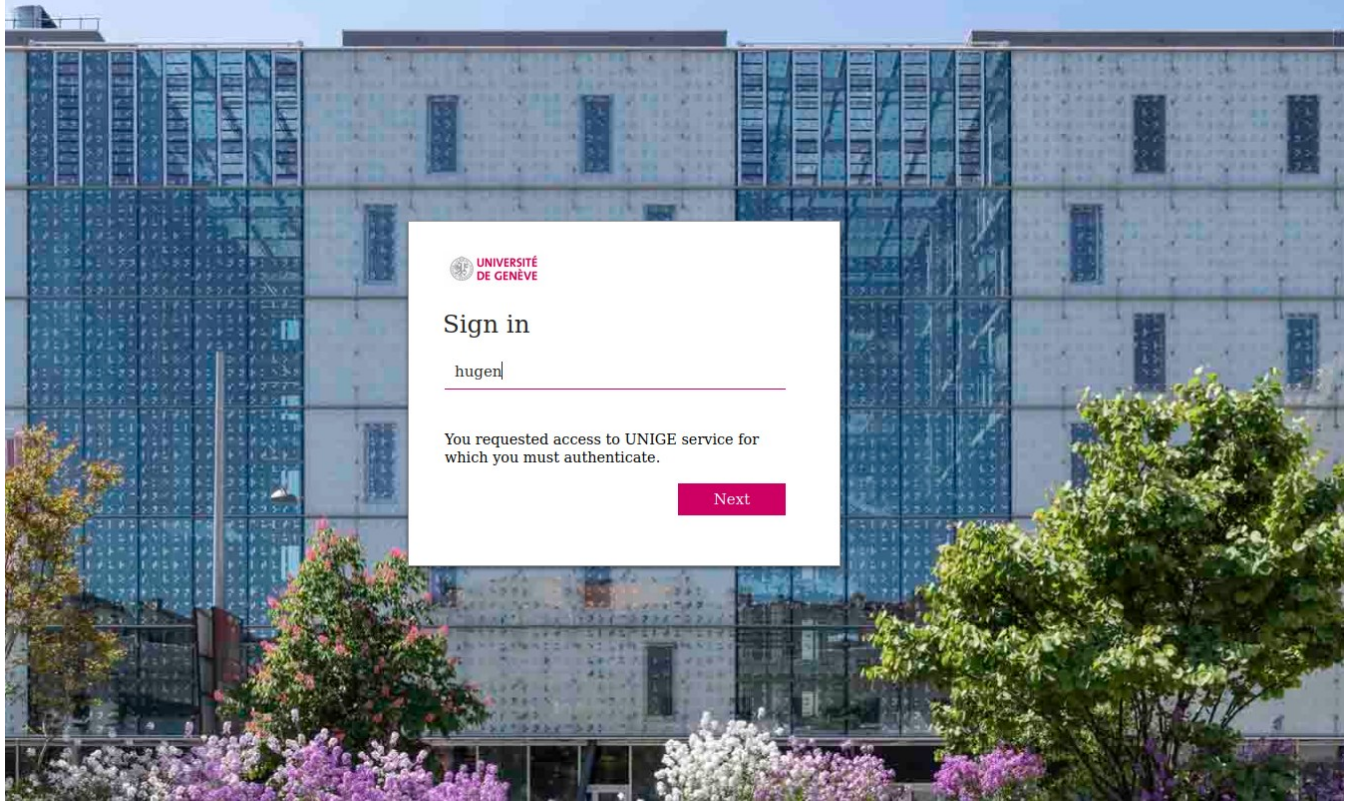
Digital Innovators

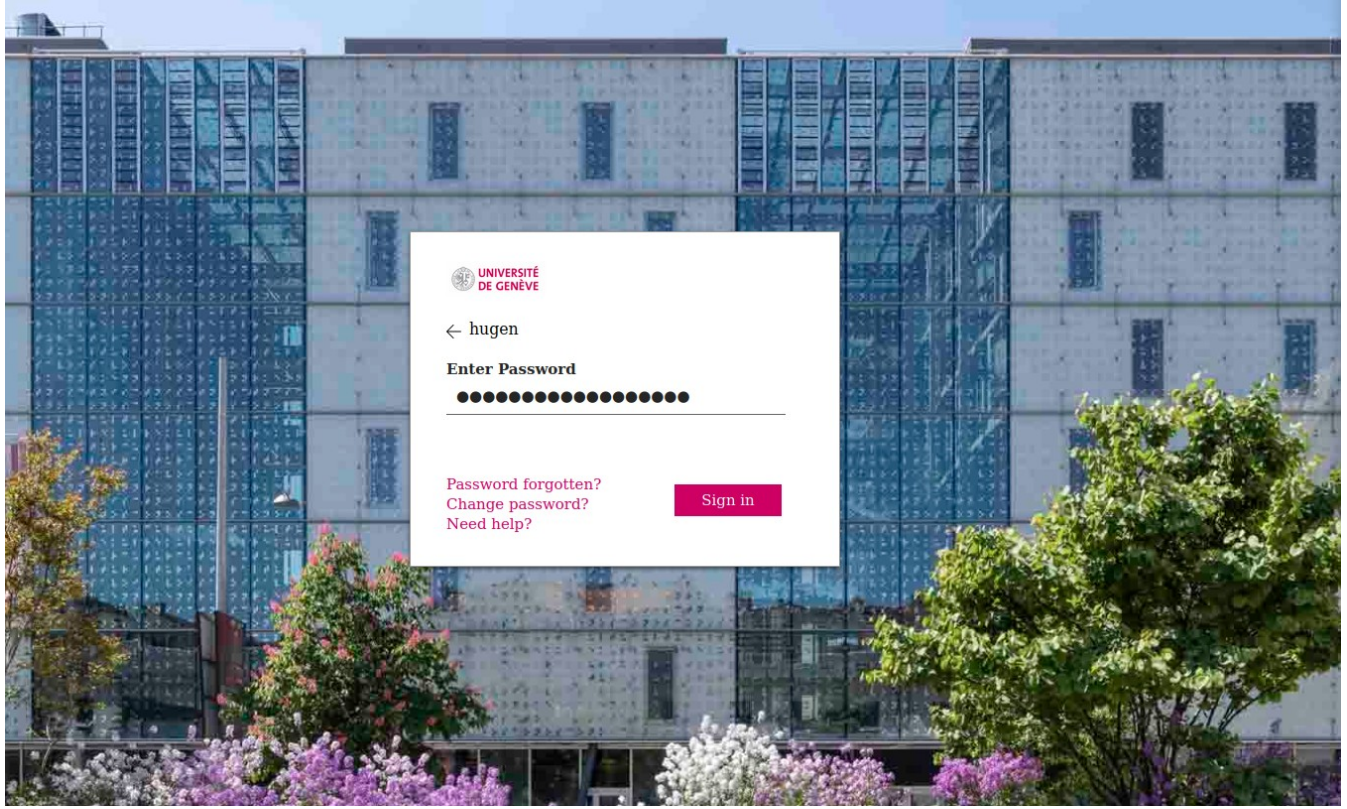
Séminaires d'innovation numérique

L'authentification multifacteur (MFA) pour sécuriser l'accès aux ressources numériques

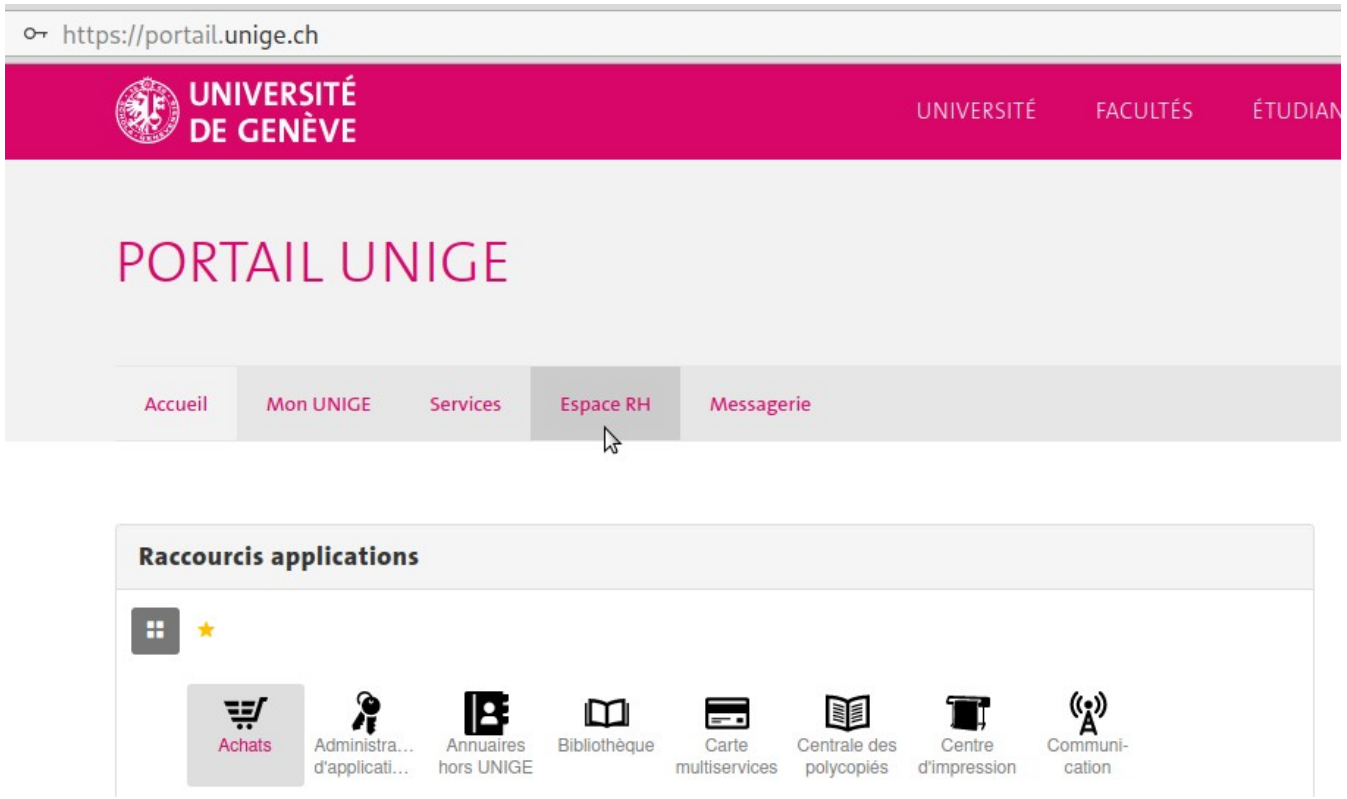
Alain Hugentobler



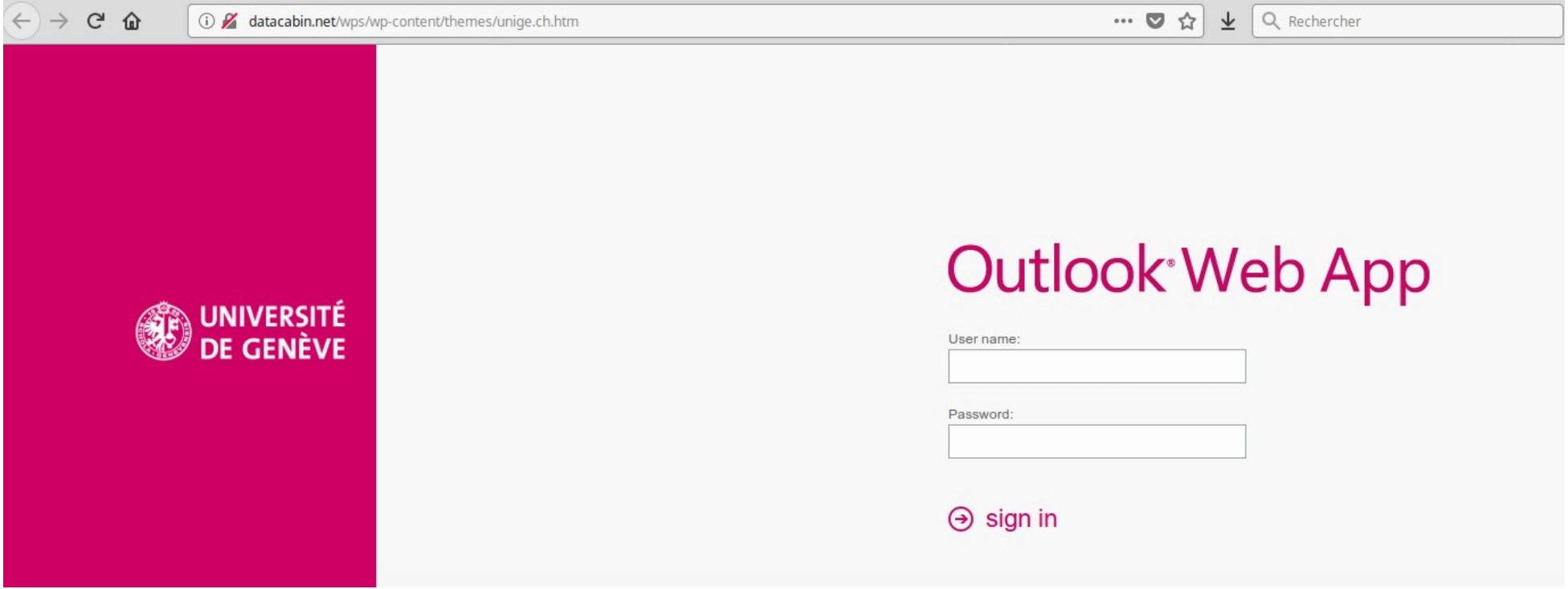
L’authentification traditionnelle requiert un nom (**username**)



Puis le mot de passe associé au nom (**password**)



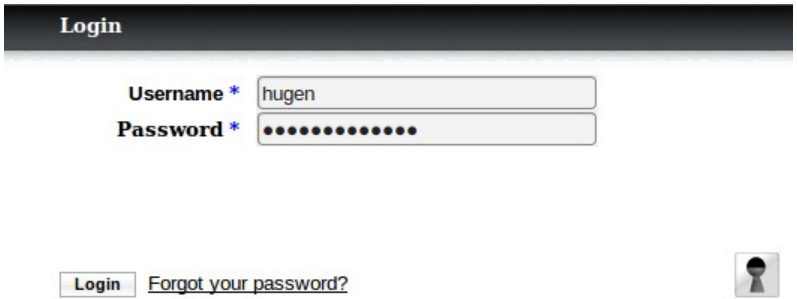
L'accès à la ressource (portail.unige.ch) a été possible avec la classique authentification **username/password** .



Nous subissons, à répétition, des campagnes d'hameçonnage (**phishing**) qui ont pour but de récupérer les identifiants de nos utilisateurs.

La combinaison **nom/mot de passe** n'est donc plus suffisante pour protéger les accès ; elle est notamment sensible à :

- Hameçonnage (Phishing)
- Ingénierie sociale
- Shoulder surfing
- Partage
- Réutilisation
- Brute force (John the ripper, Hascat, ...)
- Malware
- Enregistreurs de frappe (Keyloggers)
- ...

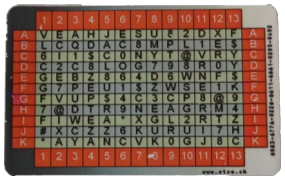


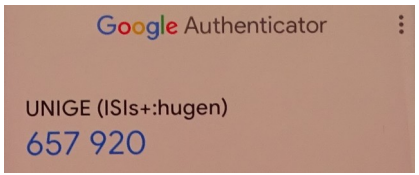
Nous protégeons donc les ressources importantes avec un second facteur d'authentification à usage unique et limité dans le temps. L'accès à l'onglet **Espace RH** du portail nécessite un second facteur d'authentification :

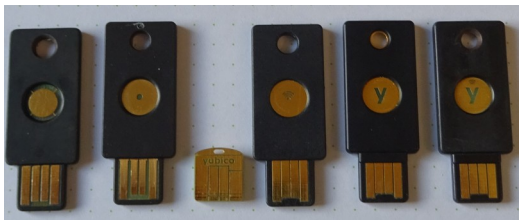
L’authentification multifacteur ou *authentification forte* ajoute une ou plusieurs étapes au processus d’accès aux ressources.

Ces étapes utilisent des moyens de validation indépendants basés sur :

- Une information connue (ex. mot de passe)
- Quelque chose que l’on possède : matériel (ex. Yubikey)
- Une caractéristique physique (ex. empreinte digitale)
- La localisation (géographique ou réseau)
- Le temps ; l’accès aux ressources peut être restreint à certaines plages horaires

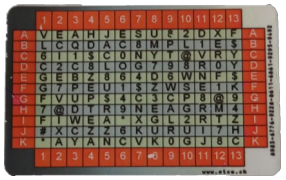


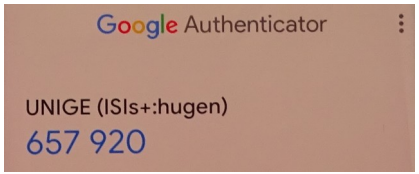


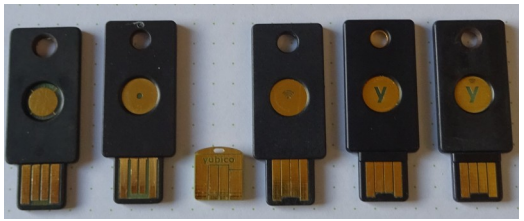


Pour le choix des méthodes d'authentification nous considérons :

- Le niveau de sécurité adapté
- Sa disponibilité sur diverses plate-formes
- La facilité de mise en œuvre et les coûts récurrents
- L'ergonomie
- Les coûts de support engendrés par la complexité de la méthode



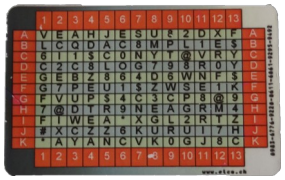


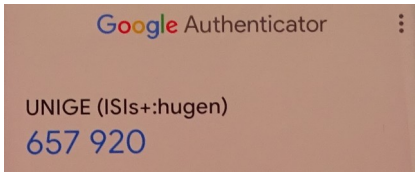


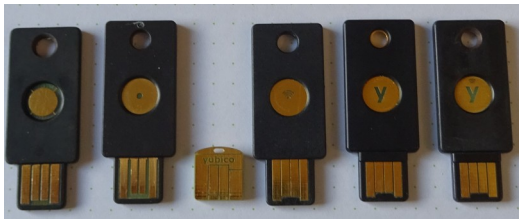
Plus de 15’000 comptes sont enregistrés sur l’infrastructure MFA **ISIs+** de l’Université de Genève.

Les méthodes d’authentification proposées sont :

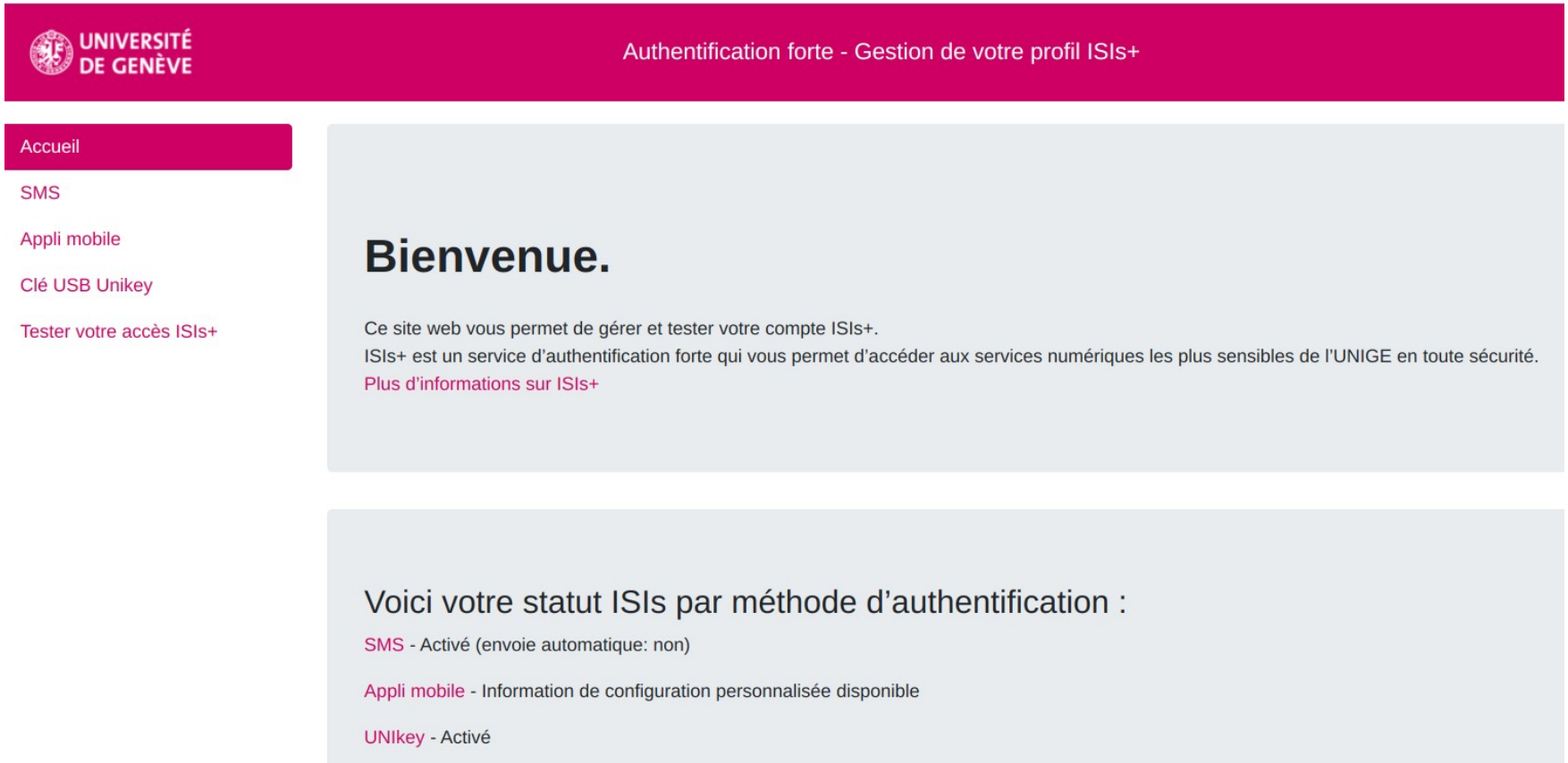
- Calcul de codes TOTP (RFC6238) via des applications
- Réception de codes valables 3 minutes via SMS
- Clé UNIKey (Yubikey OTP)
- Codes fournis par le CAD valables une seule fois pendant une semaine



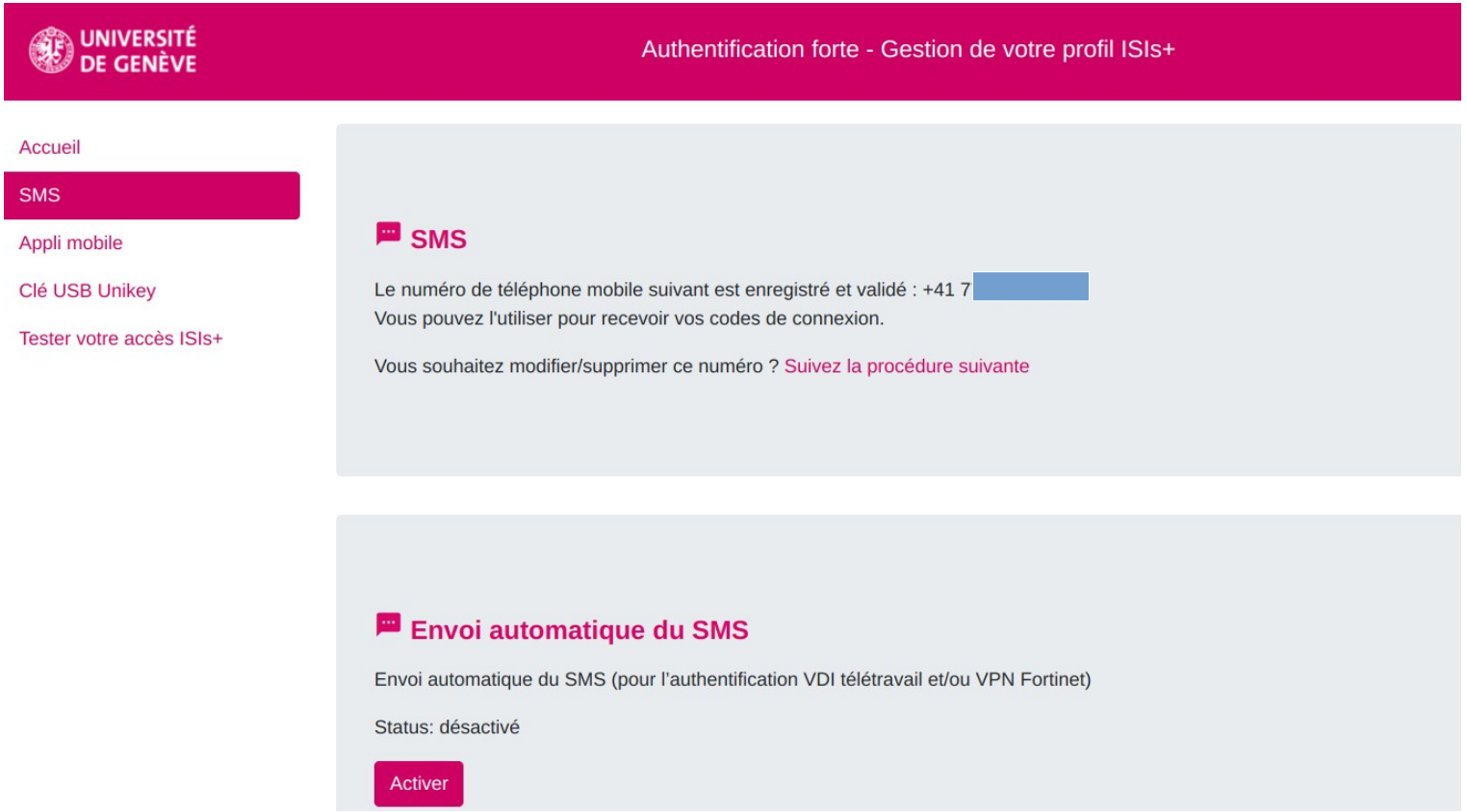




Le site isisplus.unige.ch permet de contrôler vos paramètres MFA :



On peut choisir de ne pas recevoir automatiquement de SMS lors d'accès VPN ou VDI :



On peut initialiser une application mobile qui fournira le code TOTP:

UNIVERSITÉ DE GENÈVE

Authentification forte - Gestion de votre profil ISIs+

- Accueil
- SMS
- Appli mobile
- Clé USB Unikey
- Tester votre accès ISIs+

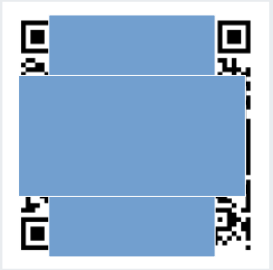
1 2 3

Appli mobile

Configurer l'application avec votre secret

Une clé secrète individuelle a été générée pour votre compte. Vous devez l'ajouter dans votre appli

Pour ce faire il vous suffit de scanner le QRCode ci-dessous:

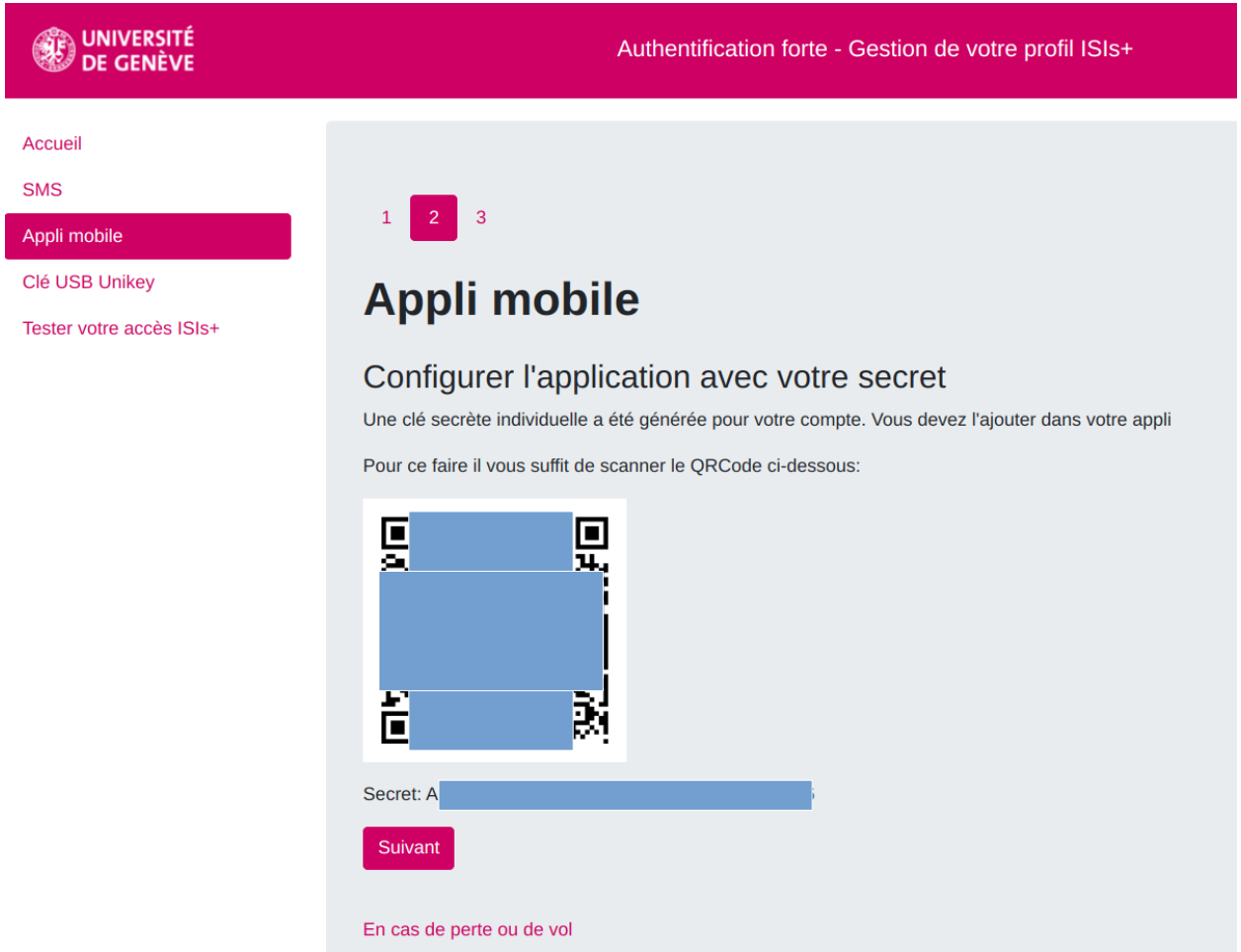


Secret: A

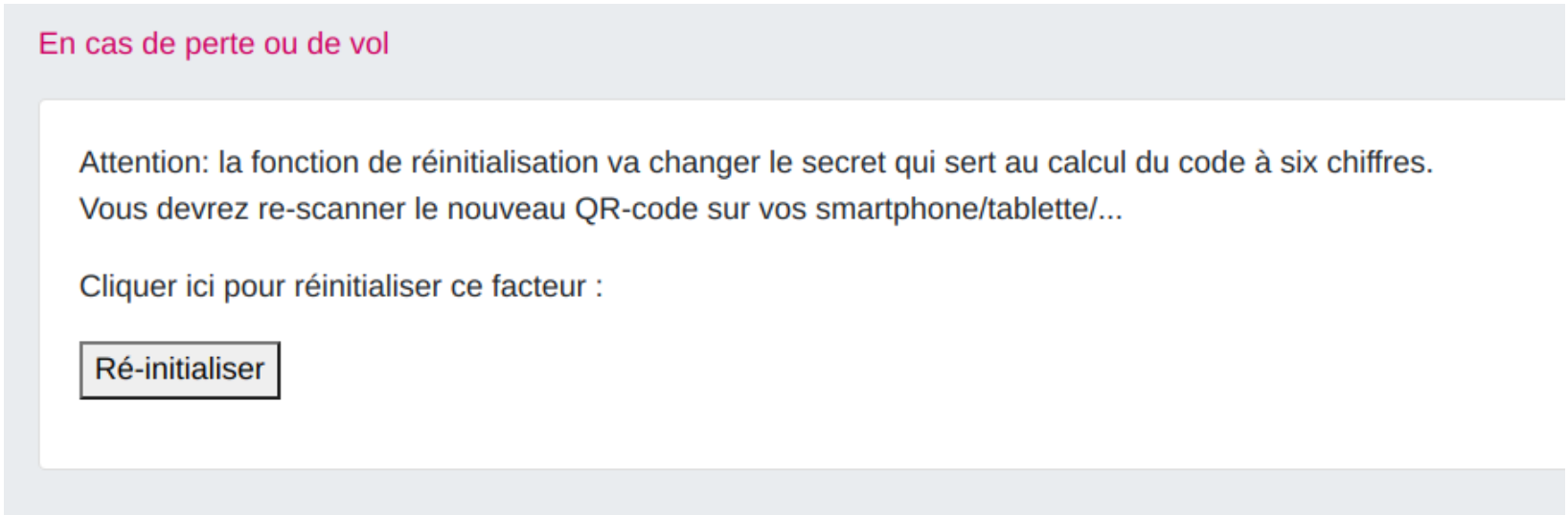
Suivant

En cas de perte ou de vol

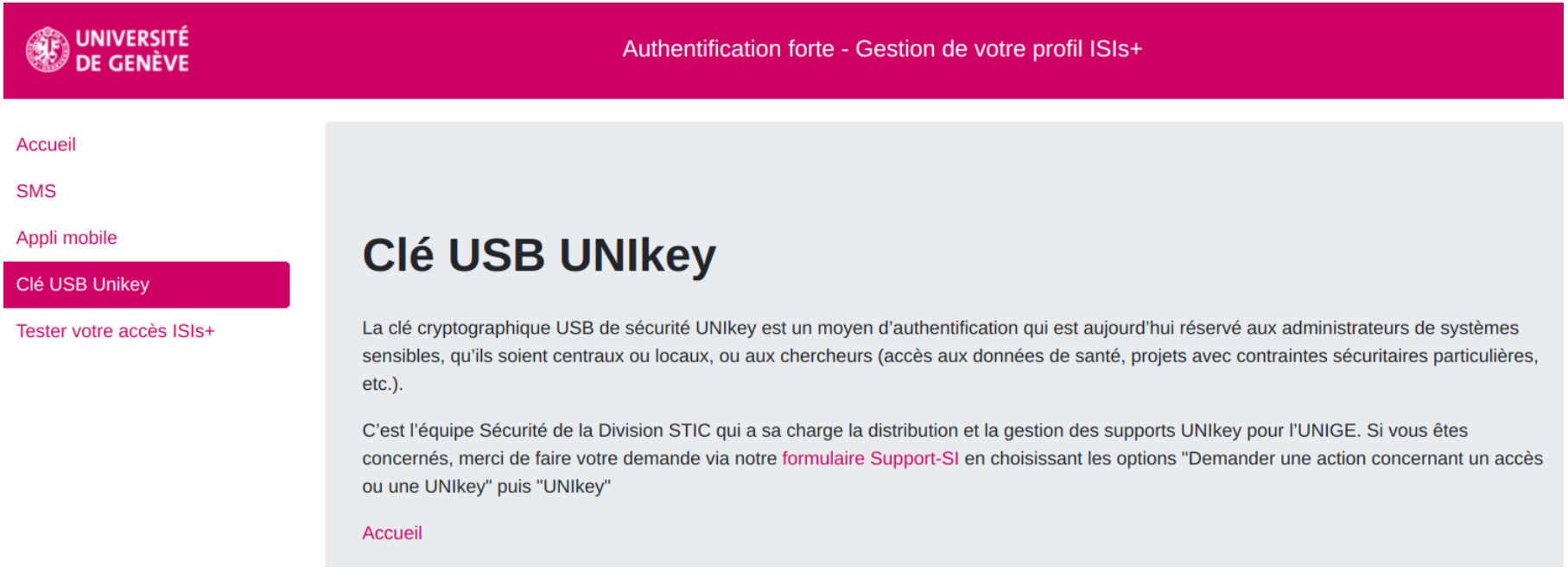
Notez le lien en bas : *En cas de perte ou de vol*



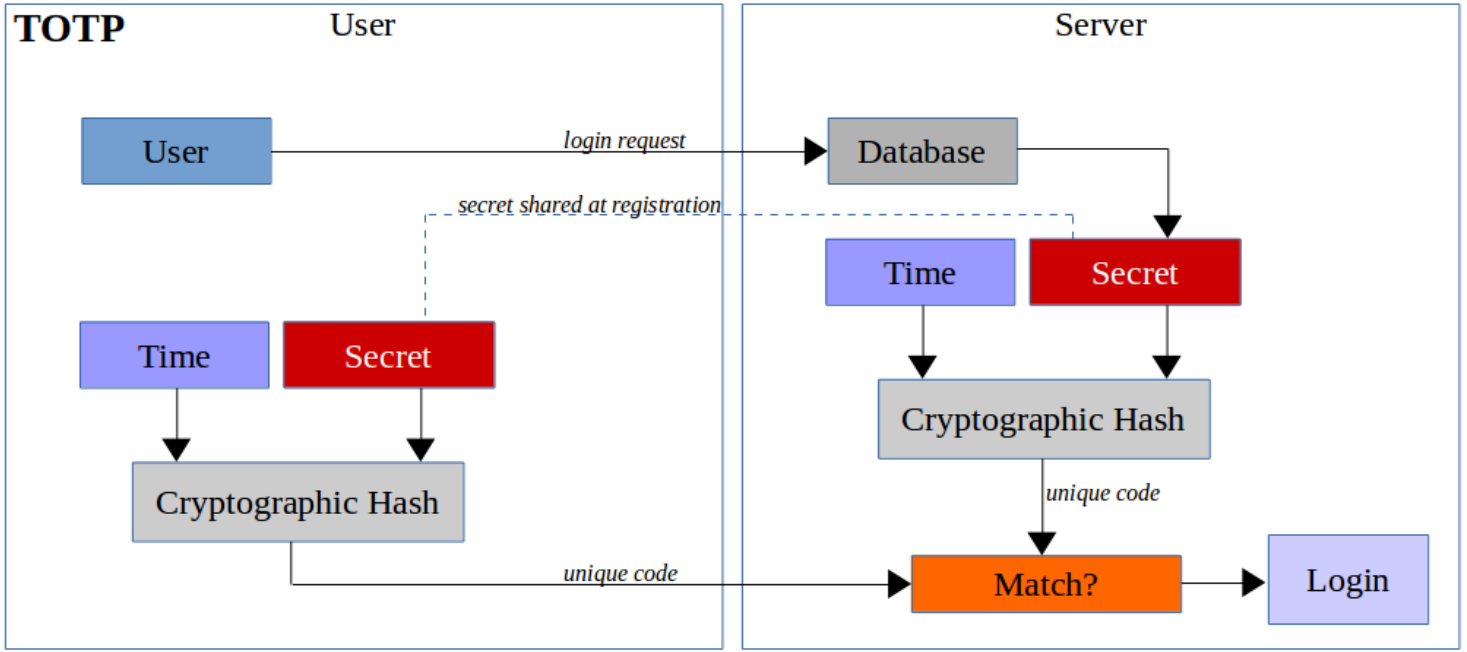
On peut réinitialiser le secret qui sert pour le calcul du code TOTP si besoin : vol, perte, compromission, ...



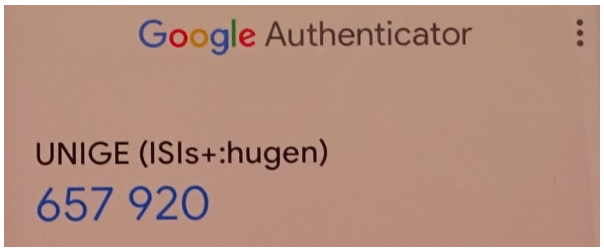
La clé UNIkey (Yubikey)est réservée aux administrateurs de systèmes sensibles, mais peut également être enregistrée si vous en possédez déjà une.



Le RFC6238 décrit l'algorithme Time-based One-Time Password.

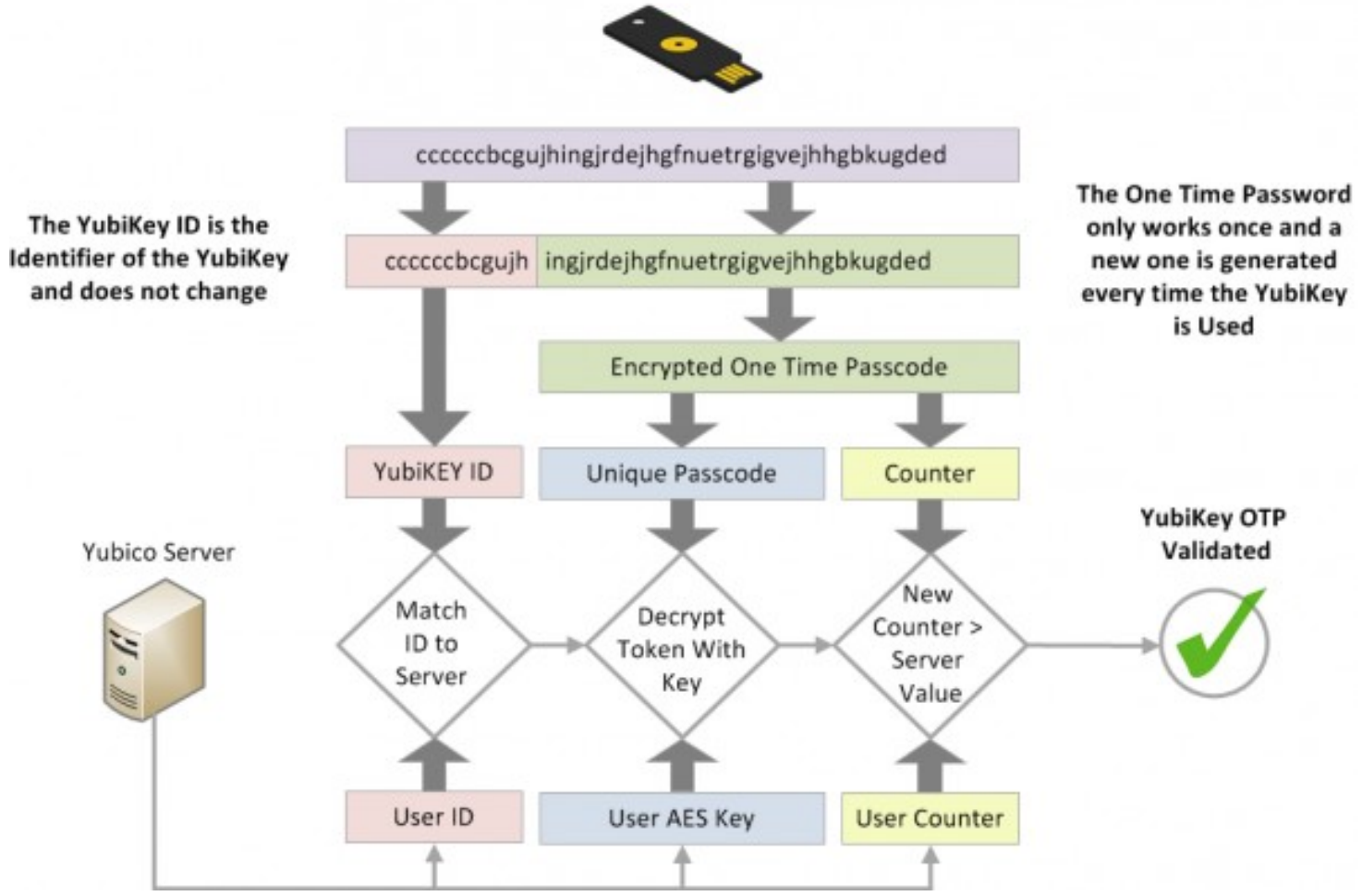


Le RFC6238 décrit l'algorithme Time-based One-Time Password.

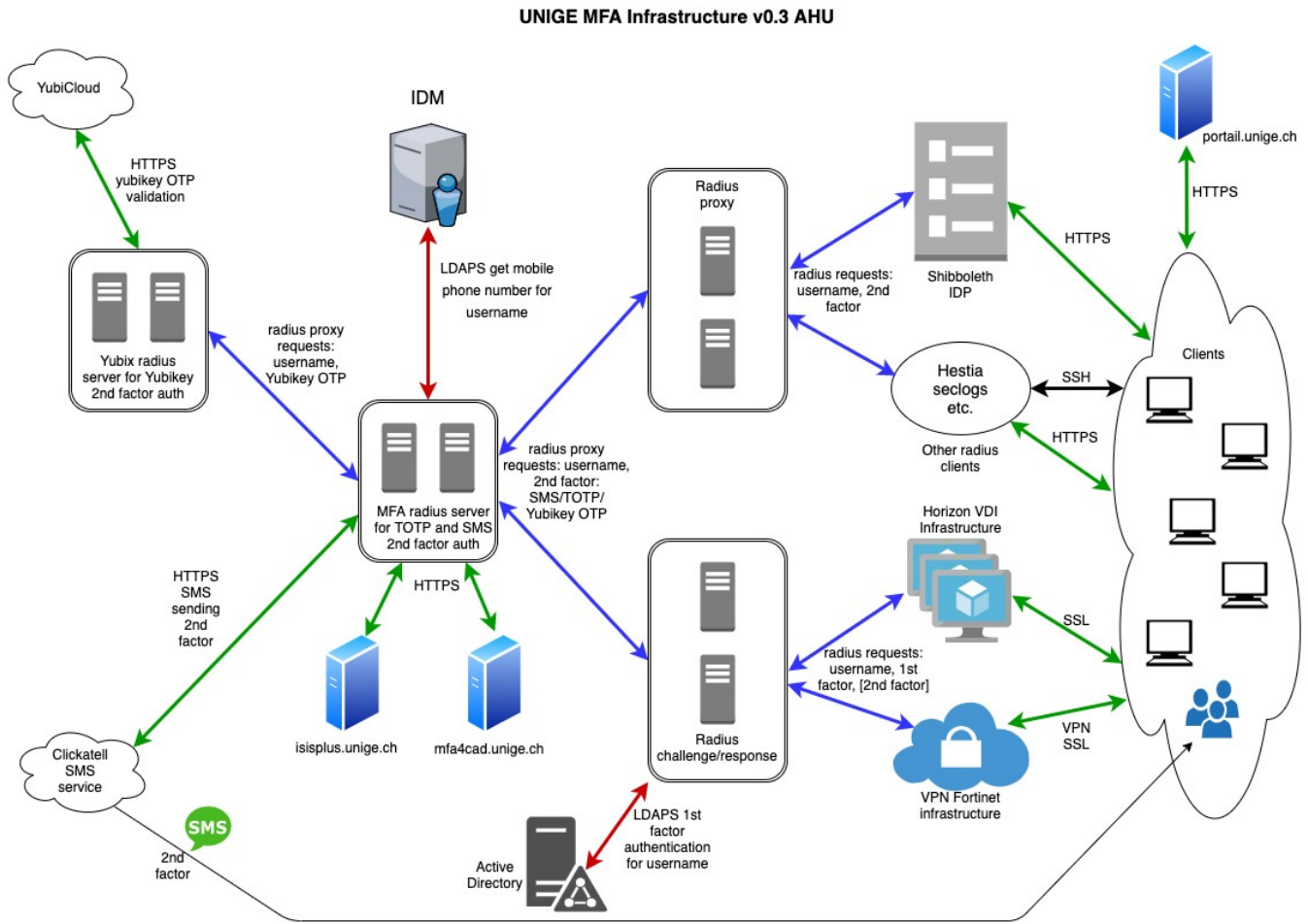


Un OTP Yubico est une chaîne de 44 caractères à usage unique, sécurisée et chiffrée. Les 12 premiers caractères sont constants et sont associés au compte du propriétaire, les 32 caractères restants font office d'OTP.

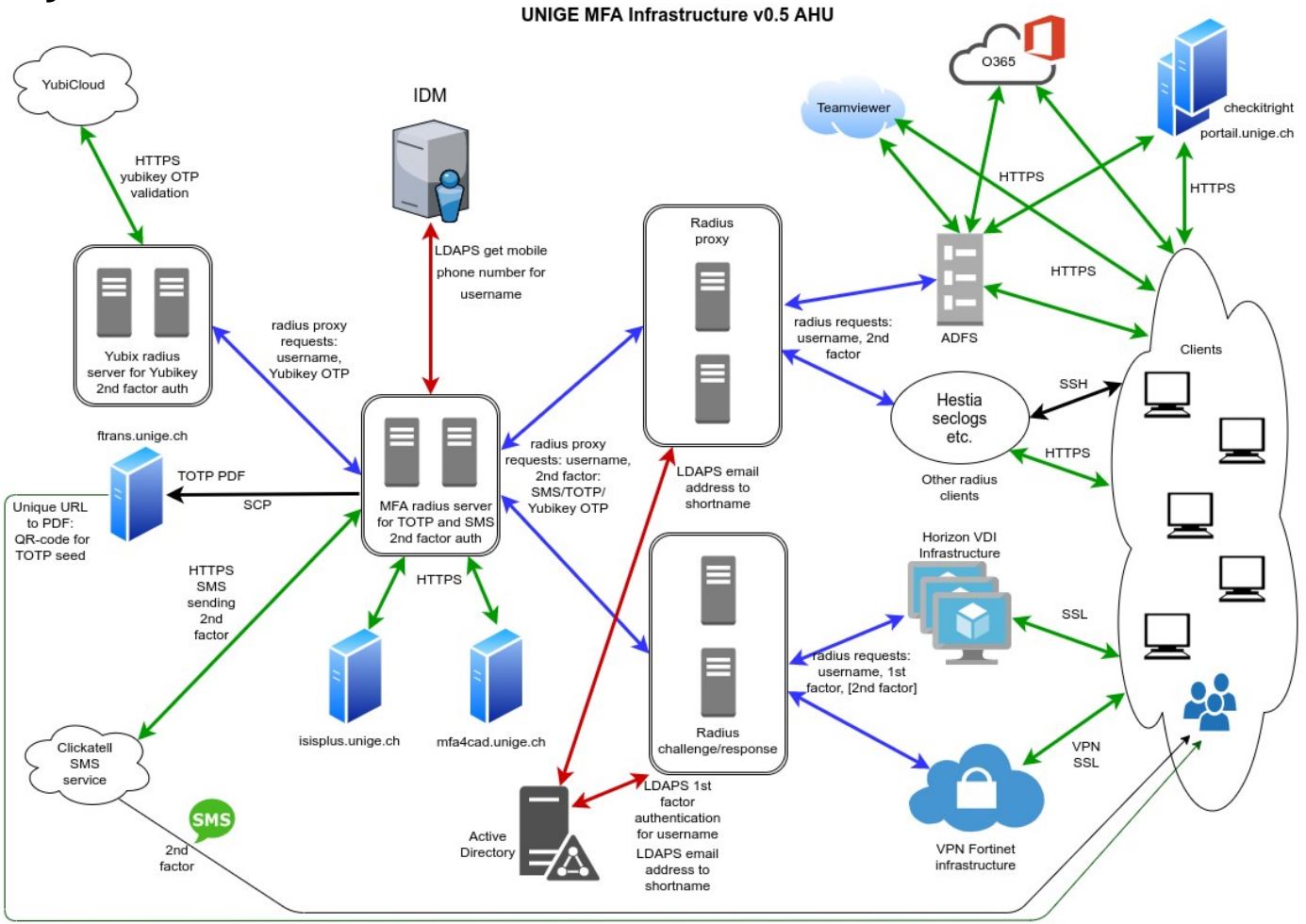
```
ccccccbcejgugvdbfuccnhdvetdukicgvuclurjrlctf
ccccccbcejgurflvvicvlgrgetulrccgncvlekhudgbi
ccccccbcejguughunnhfgutltcgnnihrvvgillvkvfrt
ccccccbcejgugbiednlglnhuieldntitlevnvdfgubin
ccccccbcejgujeuerthkhihhhuvenegvvcflvcdvgckk
```


cccccbcgujhingjrdejhgfnuetrgigvejhhgbkugded
The YubiKey ID is the Identifier of the YubiKey and does not change
cccccbcgujh
ingjrdejhgfnuetrgigvejhhgbkugded
The One Time Password only works once and a new one is generated every time the YubiKey is Used
Encrypted One Time Passcode
YubiKEY ID
Unique Passcode
Counter
YubiKey OTP Validated
Yubico Server
Match ID to Server
Decrypt Token With Key
New Counter > Server Value
User ID
User AES Key
User Counter

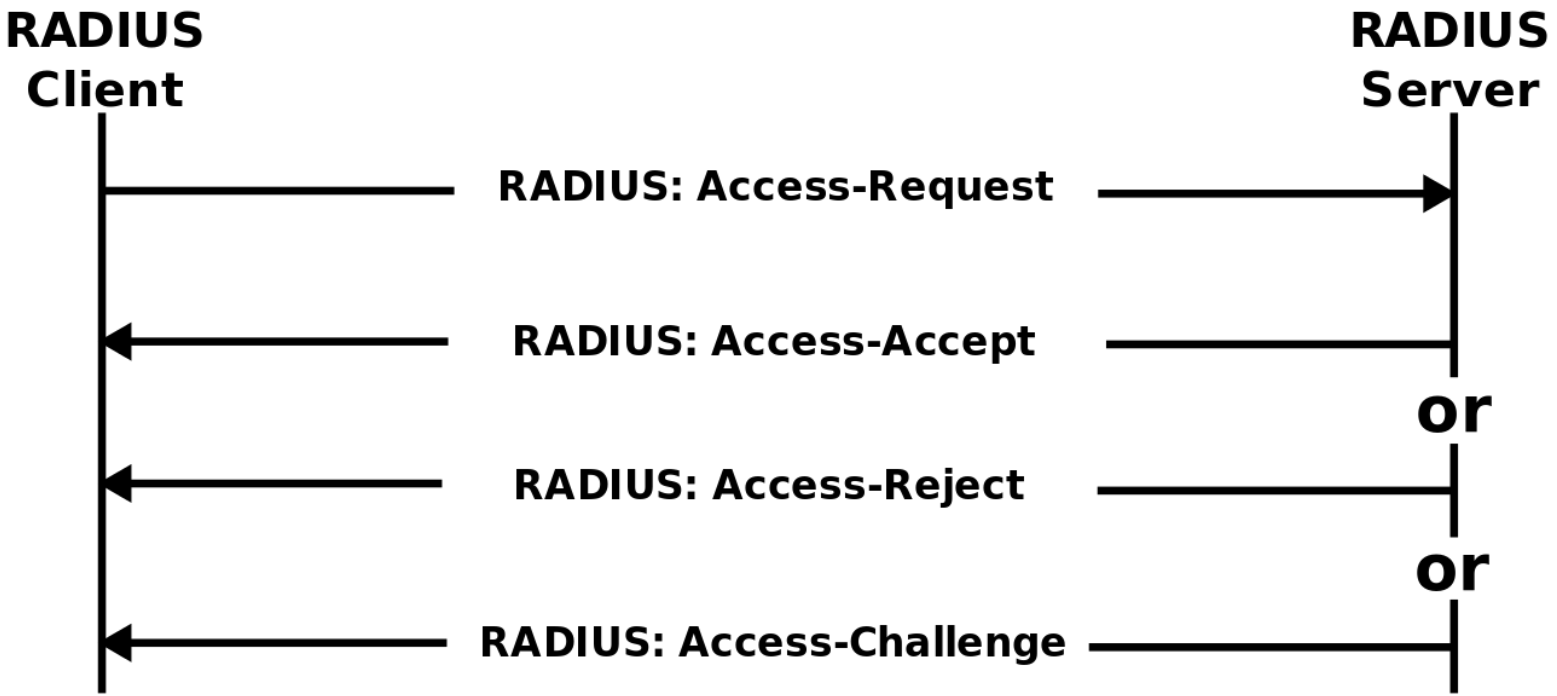
L’infrastructure MFA a évolué depuis 2016 (SSO-shibboleth + MFA)



Jusqu'à aujourd'hui avec ADFS



Le tout est basé sur un protocole simple et robuste : RADIUS



Questions ?

Google Authenticator
UNIGE (ISIs+:hugen)
182 003
hugen@xpeno
667 255
Mattermost (SWITCH alain.hugen...
092 424
netmgr-214-14
524 979
hugen@Syno
284 568
infomaniak
Impossible de prendre une capture d'écran en raison de la politique de sécurité.
354 283

Merci pour votre attention :-)