

103

7

MFA : Authentification multi facteurs

Un must have aujourd'hui

Connaître

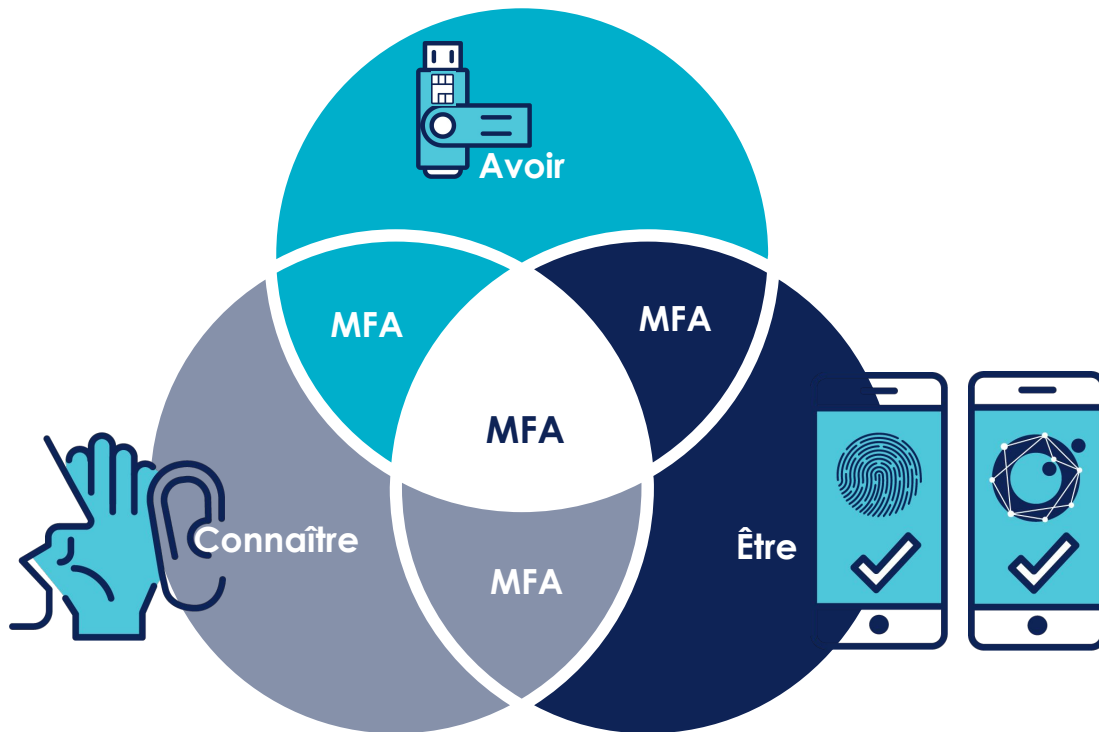
Mot de passe, Code PIN; ...

Avoir

Clé cryptographique,
téléphone, IoT, tous autres
appareils / voire objets

Être

Éléments Biométriques :
emprunt, visages, vaines,
voix, rétines, ...



Vocabulaire

Il y a des subtilités ...



SFA

Single-factor authentication

Souvent quelque chose que je sais, comme un mot de passe.



2SV

Two-step verification

Un OTP (One Time Password) est une vérification de plus. Tout en restant quelque chose que l'on sait. En utilisant des "canaux" différents ("out-of-band mechanism")



2FA

Two-factor authentication

2 facteurs d'authentification de nature différente tout en utilisant des "canaux" différents ("out-of-band mechanism")



MFA

Multi-factor authentication

Qu'en il y a 2 ou plus facteurs d'authentification de nature différente tout en utilisant des "canaux" différents ("out-of-band mechanism").

C'est un sur-ensemble de Two-factor authentication (2FA)



U2F

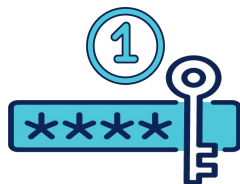
Universal 2nd Factor

C'est un périphérique d'authentification..

Norme de la **fido alliance**

fido™ | simpler
ALLIANCE | stronger
authentication

Exemple d'authentification sur d'un compte Google



Google Account

2 étapes de vérification

2

Available second steps

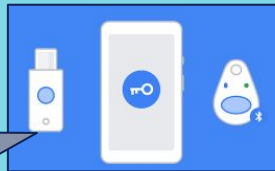
A second step after entering your password verifies it's you signing in. [Learn more](#)

	Security Key (Default) ⓘ Nokia 7 plus (Added: May 9, 4:20 AM) Last used: 4 hours ago Chrome on Mac ADD SECURITY KEY	
	Google prompts Get a Google prompt on your phone and just tap Yes to sign in. Get Google prompt on all the phones you're signed in to <input checked="" type="checkbox"/> You're signed in to 3 phones that can get Google prompt. If you sign in to more phones they will also get Google prompts.	
	Authenticator app Authenticator on Android Added: January 11, 7:09 PM CHANGE PHONE	
	Voice or text message Verified Verification codes are sent by text message. ADD PHONE	
	Backup codes 10 single-use codes are active at this time, but you can generate more as needed. SHOW CODES	

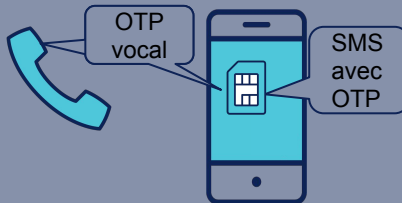
Exemple d'authentification sur d'un compte Google : étape 2

Security Key (Default) ?

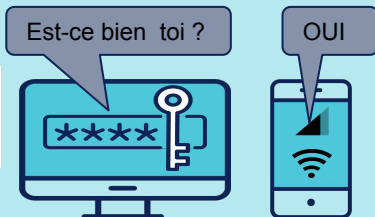
Je suis physiquement et personnellement en possession d'un "secure element". Une protection anti-phishing est réalisé avec un challenge crypto asymétrique et une vérification du domaine.



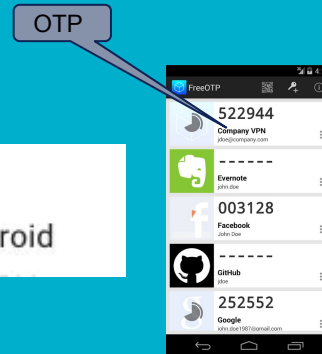
Voice or text message



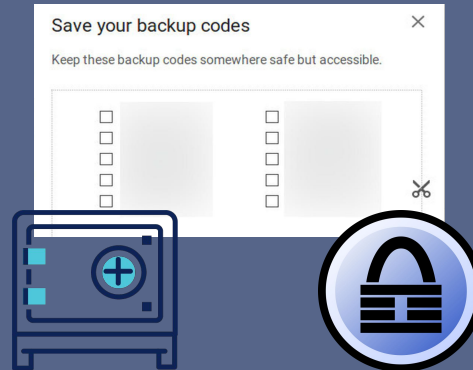
Tap Yes on your phone or tablet



Authenticator app Authenticator on Android



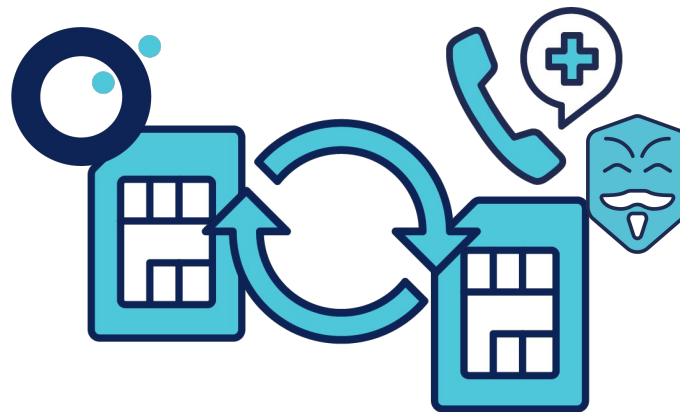
Backup codes 10 single-use codes



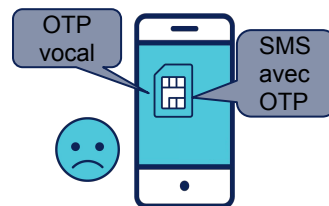
Attention 1/2 : maillon faible



au SIM Card Swapping



Voice or text message



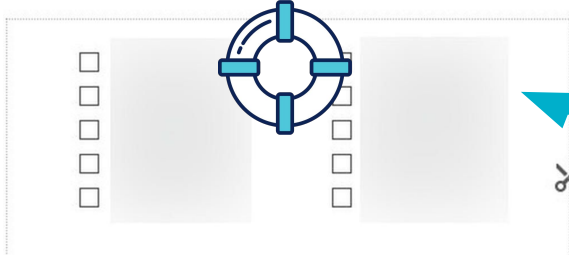
Attention 2/2 : un appareil (smartphone ou clé cryptographique) cela peut s'oublier, se perdre, dysfonctionner ou se casser



Besoin d'un plan B 1/2 : backup / restauration

Save your backup codes

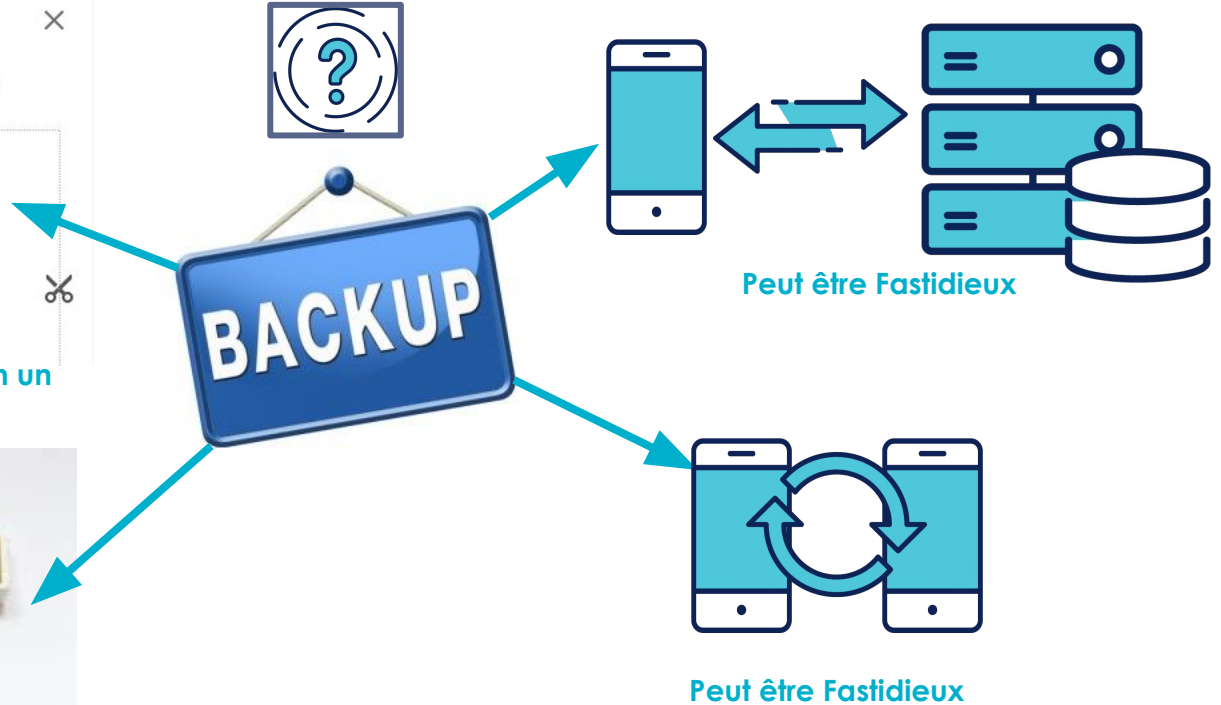
Keep these backup codes somewhere safe but accessible.



Solution temporaire de récupération un nombre limité d'OTP



Peut être coûteux et fastidieux



Besoin d'un plan B 2/2 : Révocation

Available second steps

A second step after entering your password verifies it's you signing in. [Learn more](#)

Security Key (Default) ⓘ

Nokia 7 plus (Added: May 9, 4:20 AM)

Last used: 4 hours ago
Chrome on Mac

[ADD SECURITY KEY](#)

Google prompts

Get a Google prompt on your phone and just tap **Yes** to sign in.

Get Google prompt on all the phones you're signed in to

You're signed in to 3 phones that can get Google prompt. If you sign in to more phones they will also get Google prompts.

Authenticator app

Authenticator on Android

Added: January 11, 7:09 PM

[CHANGE PHONE](#)

Voice or text message

06 15 87 72 24 **Verified**

Verification codes are sent by text message.

[ADD PHONE](#)

Backup codes

10 single-use codes are active at this time, but you can generate more as needed.

[SHOW CODES](#)



suppression d'une clé sécurisé



suppression d'un appareil



Génération d'un nouveau secret



Changement du numéro de téléphone




Génération de nouveau codes de secours

Exemple d'authentification sur d'un compte Google : étape 2


 Security Key (Default) ?




 Devenu trop dangereux !

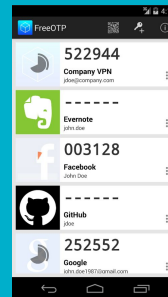
 Voice or text message



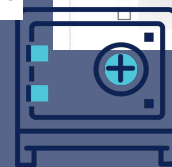
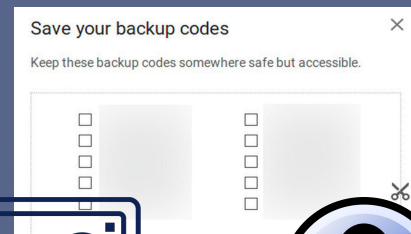
 Tap **Yes** on your phone or tablet



 Authenticator app
Authenticator on Android



 Backup codes
10 single-use codes



L'OATH ([Open Authentication](#))* est souvent utilisée

1. Install a compatible app on your mobile device or computer

See a [list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code



*OATH ([Open Authentication](#)) : à ne pas confondre avec l'[OAuth](#)

Contenu du QR-Code pour l'OATH TOTP



```
otpauth://totp/Example:alice@google.com?secret=JBSWY3DPEHPK3PXP&issuer=Example
```

Specifications sur <https://github.com/google/google-authenticator/wiki/Key-Uri-Format>

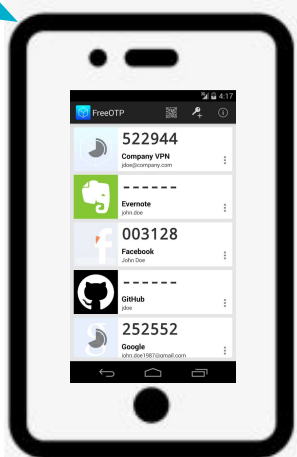
Backup du contenu du QR-Code pour l'OATH TOTP

1. Install a compatible app on your mobile device or computer
See a [list of compatible applications](#)

2. Use your virtual MFA app and your device's camera to scan the QR code



Etape classique



Etape préalable
supplémentaire



otpauth://totp/Example:alice@google.com?secret=JBSWY3DPEHPK3PXP&issuer=Example

Papier avec
le QR-code et
URL TOTP

URL TOTP



OAUTH - TOTP est actuellement un bon compromis.



OATH-TOTP

Avec lock screen (pour quoi pas biométrie),
chiffrement du stockage de masse et sauvegarde des
secrets



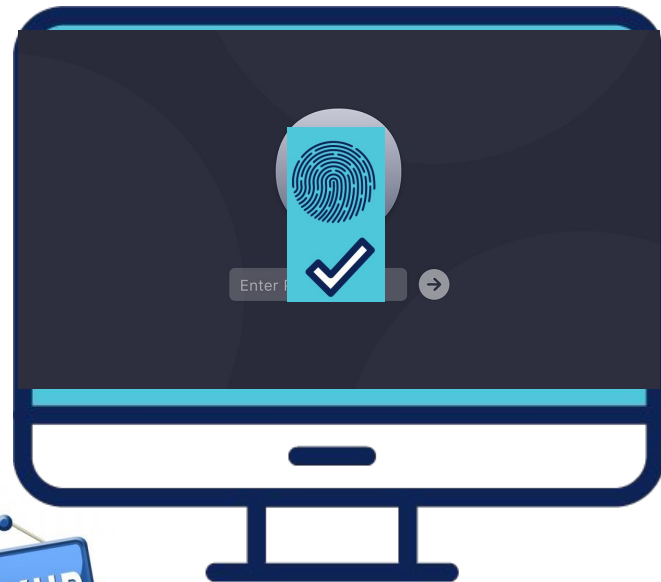
Moyen d'authentification MFA bien répandu
actuellement.
Remarque l'OTP est calculé localement (offline) sur
autant d'appareils en parallèle souhaités.



Google Authenticator est perfectible ...

Notamment avec son système de migration depuis mai
2020 (otpauth-migration://offline?data= uri).

Mais il y a d'autre solution disponible.



Exemple d'authentification sur d'un compte Google : étape 2



Le plus sécurisé avec anti phishing.

Visiblement pas encore compatible NFC. Peut-être faut-il désactiver les autres MFA (cf. "Protection Avancée" de Google)

Doit pouvoir faire de "l'auto-sign in".

Ne pas oublier le backup.

 Security Key (Default) ?



La solution mobile est encore perfectible...

L'utilisation de WebAuthn reste globalement

malheureusement encore marginal sur le web.

Mais cela vient. Un exemple parmi d'autre github qui est

compatible Webauthn depuis l'été 2019. cf. Bientôt la fin des mots de passe sur le Web ? (WebAuthn) | OCTO Talks



Bien pratique.

Plusieurs smartphones peuvent être supportés en parallèle



Ne pas oublier le backup.



Tap **Yes** on your phone or tablet



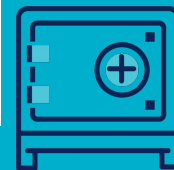
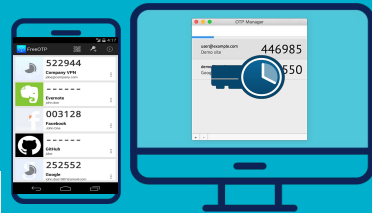
Incontournable pour le moment.

A minima pour le backup.



OATH-TOTP

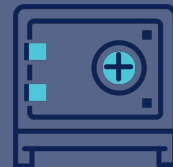
Avec lock screen, chiffrement du stockage de masse et sauvegarde des secrets



Devenu quasi optionnel avec Backup TOTP



Backup codes
10 single-use codes



MFA : en pratique ...

Des Questions ?

MFA : Multi-factor authentication



There
is
a Better
Way

Nous réalisons des missions de conseil IT et nous développons vos applications stratégiques... *Différemment.*