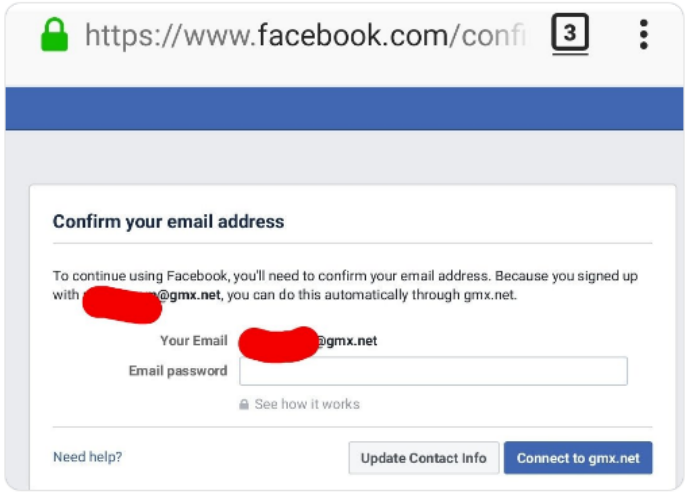
L'authentification forte

Pierre-Olivier Mercier

e-sushi
@originalesushi

Follow

Hey @facebook, demanding the secret password of the personal email accounts of your users for verification, or any other kind of use, is a HORRIBLE idea from an #infosec point of view. By going down that road, you're practically fishing for passwords you are not supposed to know!



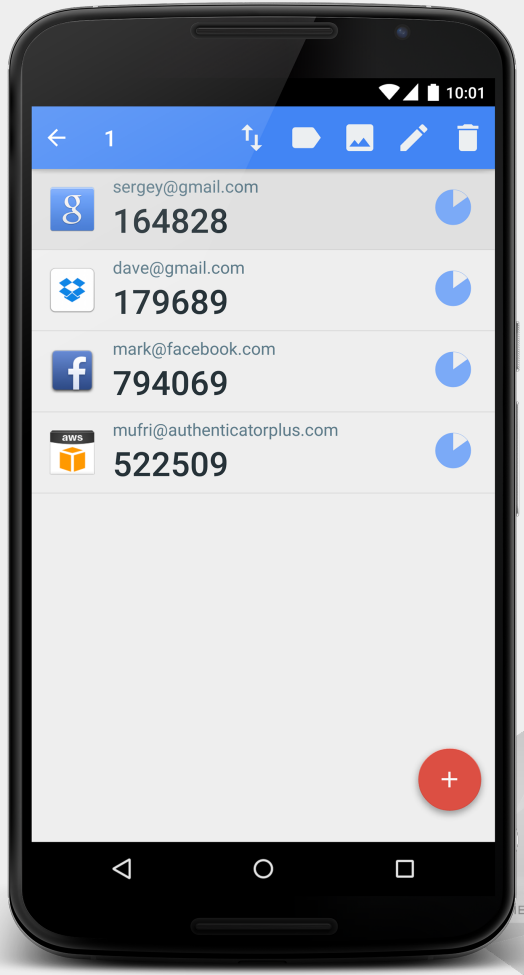
4:27 PM - 31 Mar 2019

Facteurs d’authentification :

- Ce que l’on connaît
- Ce que l’on détient
- Ce que l’on est
- Ce que l’on sait faire

Facteurs d'authentification :

- Ce que l'on connaît
- Ce que l'on détient
- Ce que l'on est
- Ce que l'on sait faire



HOTP RFC 4226

$$HMAC_{SHA1}(Key, Counter)$$

$$HMAC_h(Key, Msg) = h((Key \oplus opad) \,||\, h((Key \oplus ipad) \,||\, Msg))$$

HOTP RFC 4226

$$HMAC_{SHA1}(Key, Counter)$$

$$HMAC_{h}(Key, Msg) = h((Key \oplus opad) \,||\, h((Key \oplus ipad) \,||\, Msg))$$

TOTP RFC 6238

$$HMAC_{SHA1}(Key, time.Now()/period)$$

Périphériques à bas coût pour un déploiement maximal

Fonctionne sur USB ou NFC

Espace de stockage limité à un compteur global

Chiffrement ECDSA demandant peu de puissance

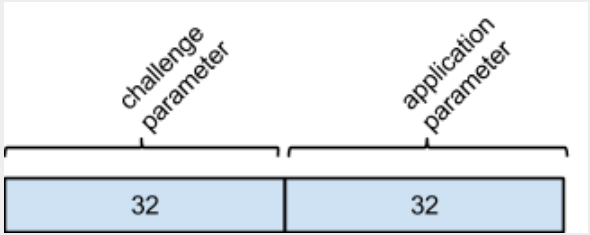
Requiert un bouton pour signaler sa présence

Deux actions possibles :

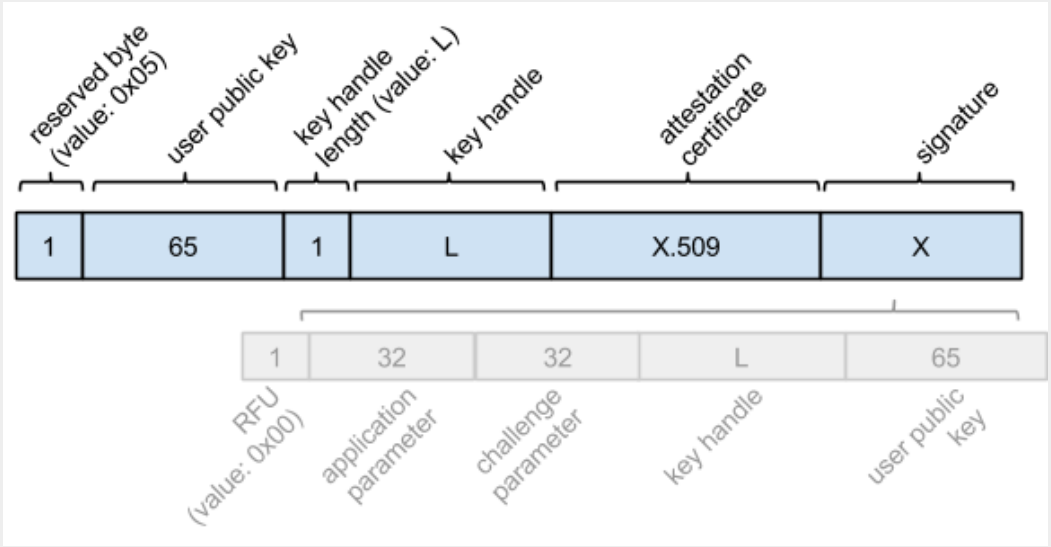
- Enregistrer un nouveau site
- Authentifier une demande d'accès

Enregistrement

Requête



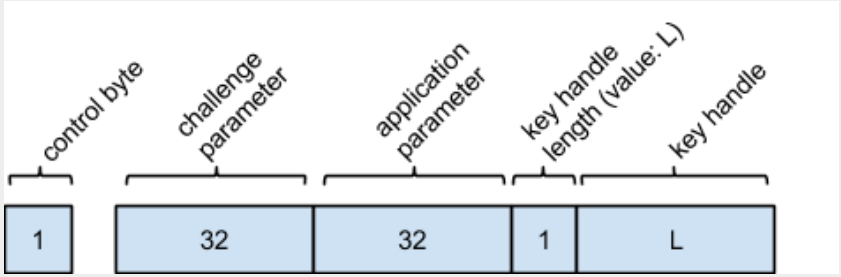
Réponse



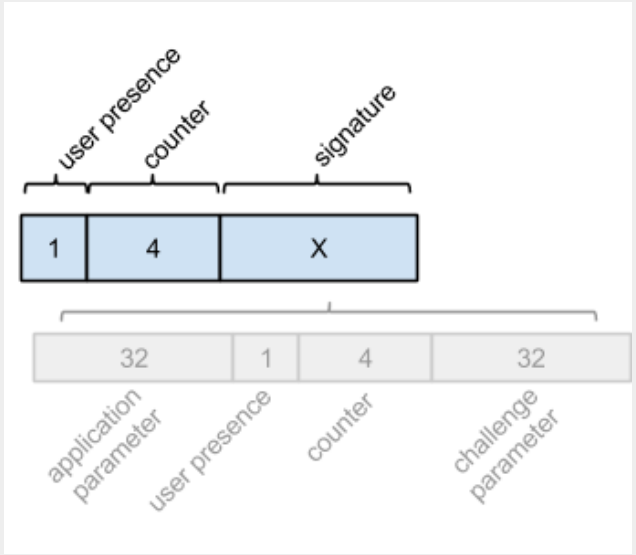
EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

Authentification

Requête



Réponse



EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE