FIDO2

Maxime Besson

Rappels

FIDO2

- Un mécanisme d'authentification pour le web
  - Basé sur le chiffrement asymétrique (clé privée)
- Resistance au phishing
- Mécanismes anti rejeu (*challenge*), anti clonage (*compteur*)
- Vie privée
  - sauf fonctionnalités entreprise (*attestation*)

Deux types de périphériques

- itinérant
  - Typiquement: clé USB spécialisée (Yubikey, Winkeo. . .)
- plateforme
  - Windows Hello, FaceID, Android
  - “Passkeys”: synchronisées entre périphériques

Démonstration

Fonctionnement

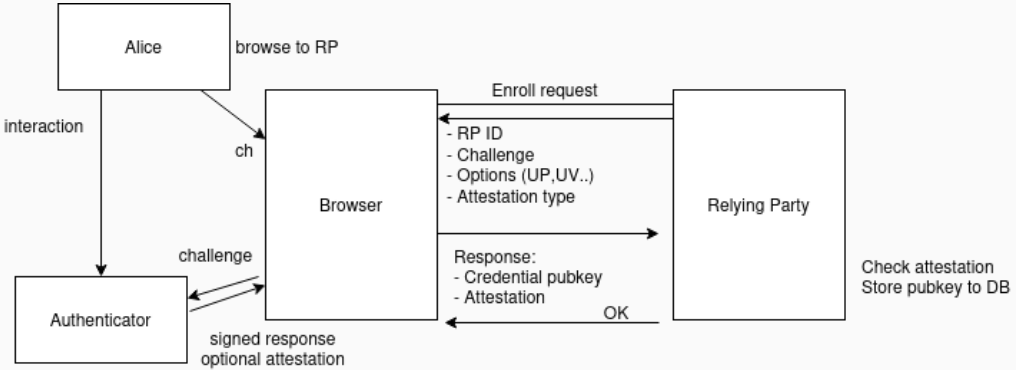
Enregistrement

- En général en self-service
- Avec ou sans attestation
- Possible d'exiger un code PIN
- Possible de permettre l'utilisation passwordless

Attestation

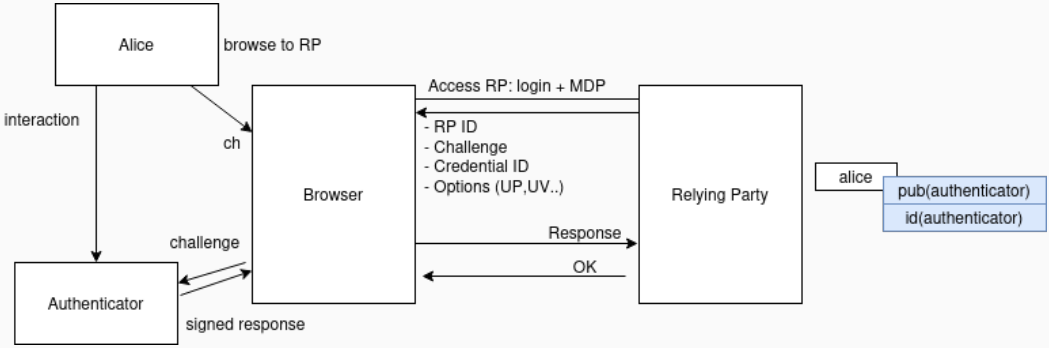
- Permet de vérifier le modèle de périphérique utilisé
- Nécessite un certificat racine connu
- Utilisation de métadonnées (MDS)

Résumé


Alice
browse to RP
interaction
ch
Browser
Enroll request
- RP ID
- Challenge
- Options (UP,UV..)
- Attestation type
Relying Party
challenge
Response:
- Credential pubkey
- Attestation
OK
Check attestation
Store pubkey to DB
Authenticator
signed response
optional attestation

Authentification

- L'opération la plus simple
- Part du principe que la clé publique de l'authentificateur est déjà connue par le serveur



Support dans LemonLDAP::NG

Attestation

- Uniquement les types `packed` et `fido-u2f`
- Possibilité d'imposer une attestation valide

Enregistrement

- Les certificats racines doivent être manuellement renseignés
- Possibilité de filtrage par modèle de clé (AAGUID) via des plugins

Authentification

- 2FA
- Passwordless depuis la v2.20