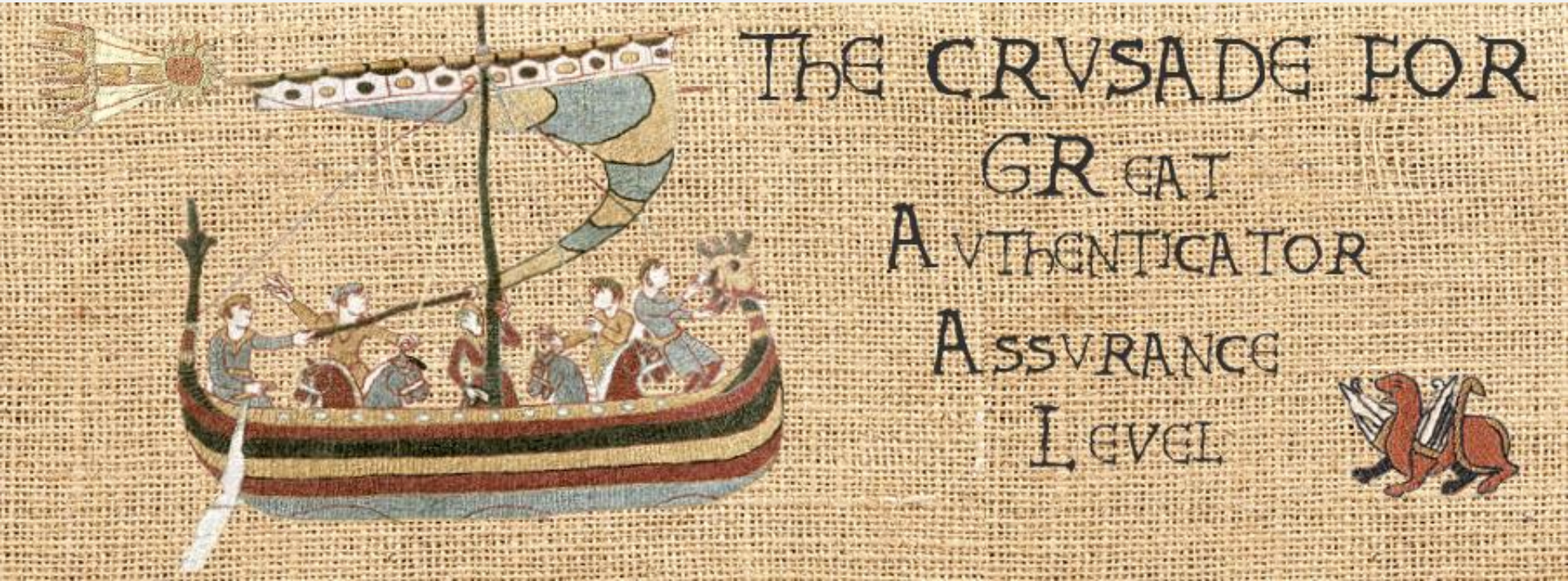
# « Le Graal » : WebAuthn
# l'authentification web renforcée pour tous

Colin Bontemps / Jérémie Boutard

17 mai 2022 / CNRS – Direction des Systèmes d'Information




# Livre 1 : « Le graal »

WebAuthn, l'authentification web renforcée pour tous

# L’authentification, l’origine

## Une authentification, deux étapes

1. L’identification: déclarer qui nous sommes
2. L’authentification: prouver qui nous sommes

## Une authentification, différents facteurs

- « ce que je connais »
- « ce que je possède »
- « ce que je suis »
- « ce que je fais »
- « où je suis »

## Une authentification, plusieurs résistances

- « simple », un seul facteur
- « forte », au moins deux facteurs (2FA, MFA)
- « renforcée », selon le contexte (Cf. DPS2)

# Le mot de passe, un facteur particulier

## Le mot de passe, la confidentialité historique

- « ce que je connais »
- Utilisé depuis la nuit des temps
  « Sésame ouvre-toi ! »
- Employé depuis les années 60 en informatique

## Le mot de passe, plusieurs formes

- Code PIN carte bancaire
- Mot de passe applicatif
- Passphrase Wifi

## Le mot de passe, des normes

- Chartes, PSSI, ANSSI, CNIL, etc.

## Le mot passe, la faiblesse informatique historique

- Premier cas de piratage: 1962 (Allan L. Scheer)
- Vol, hameçonnage

Trop faible pour assurer la confidentialité des actifs les plus sensibles

# Pourquoi l'authentification forte ?

## Besoin de sécurité du SI de gestion et de service:

- Réduire les risques de perte de confidentialité des informations sensibles

## Une solution fonctionnelle de sécurité (parmi d'autres):

- Renforcer l'authentification

## Cible de niveau de sécurité:

- NIST - Authenticator Assurance Level 3 (AAL3)

## Niveau actuel:

- NIST - AAL1 (mot de passe)
- Insuffisant

## Doit être accepté par les utilisateurs

# Quelques critères de la solution

## Fonctionnels:

- AAL3
- Token d'authentification matériel

## Techniques:

- Intégration dans le SI existant
- Passage à l'échelle
- « On premise »
- Open Source

## Utilisateurs:

- Simple et mobile
- Sans smartphone
- Adapté au contexte hétérogène

## Organisationnels:

- Facilité de déploiement
- Facilité d'approvisionnement
- Facilité d'assistance

# L’étude de marché
# Orientée expérience utilisateur dans un contexte AAL3

## Les solutions non-retenues

- Les solutions historiques propriétaires : trop chères, trop complexes à déployer
- OOB, SMS OTP (aujourd’hui, non fiable), Authenticator (type OpenOTP): utilisation d’un smartphone
- Certificats X509 type RGS***: surqualifié (AAL4), trop complexe à déployer

## La solution retenue: le standard U2F

- Ergonomique
- Ouvert
- Orienté Web, intégré aux navigateurs
- Facilité logistique
- REX des GAFAM
- POC rapide avec existant (Shibboleth)
- Qualifiée NIST - AAL3

# Un peu d'histoire : FIDO Alliance

## Consortium FIDO Alliance

- Actif depuis 2013
- Des contributeurs de poids, principalement privés : Paypal, Yubico, Google, Microsoft, RSA, Duo Security, …

## L'ambition de proposer une solution d'authentification web

- Sécurisée
- Facile à utiliser (authentification en un seul geste)
- Qui respecte la vie privée
- Facile à mettre à l'échelle

## Quelques dates clés de FIDO :

- 2012/07 : Fondation de la FIDO Alliance
- **2014/12 : Publication des protocoles FIDO U2F et FIDO UAF**, ancêtres de FIDO2 et WebAuthn
- 2016/02 : Début du travail avec le W3C pour faire de FIDO2 un standard du web
- **2018/04 : Lancement officiel de FIDO2** : WebAuthn (W3C candidate recommandation) et CTAP2. Les navigateurs Firefox, Chrome et Edge supportent déjà FIDO2.
- 2019/02 : Les mécanismes d'authentification mobile d'Android sont certifiés FIDO2
- **2019/03 : WebAuthn défini comme standard du web par W3C**
- 2019/05 : Windows Hello est certifié comme authentificateur FIDO2
- 2020/01 : Apple rejoint la FIDO Alliance. les principaux matériel et navigateurs Apple deviendront compatibles et certifiés FIDO2 cette même année

# Cas d'usage d'authentification FIDO2

**En complément du mot de passe** pour de l'authentification multi facteur

- Utilisation en complément d'un facteur existant
- Cet usage suggère en général un authentificateur externe et transportable
- Possibilité de ne demander le second facteur que dans certains cas (authentification adaptative)

**ou**

**Remplacer complètement le mot de passe**, en complément avec un facteur local biométrie ou code PIN

- Le facteur local sert à déverrouiller la clé privée pour permettre la signature du challenge.
- Exemple : Windows Hello, via empreinte digitale, reconnaissance faciale ou PIN
- Exemple : Touch ID sur MacOS ou iOS >13.3
- Exemple : Clé de sécurité FIDO2 + Code PIN

# La solution FIDO2

## Une paire de clés asymétriques générée à l'enrôlement de chaque service.

- Comme une paire de clés pour SSH, avec une paire de clés par serveur.
- Une paire de clé spécifique pour chaque site et utilisable seulement sur celui-ci.

## Authentification par signature de challenge,

- Un peu comme une authentification client TLS par certificat

## Différents types d'authentificateurs

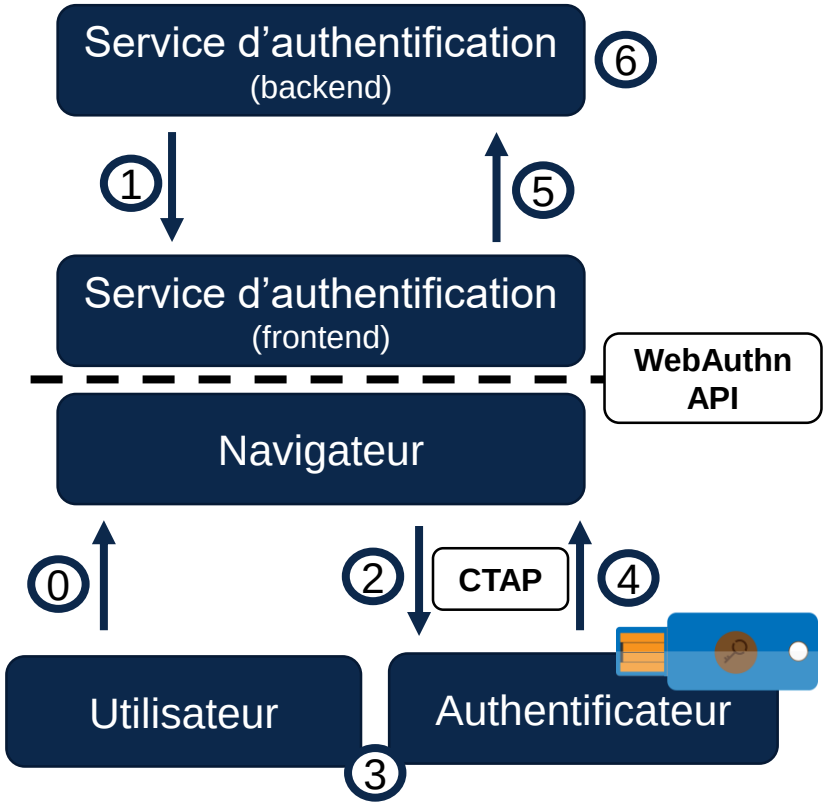
- **Platform** : intégré à l'appareil. Ordinateur ou ordiphone sur un stockage sécurisé type TPM
- **Cross-platform** : un authentificateur externe (USB, NFC ou bluetooth) type Yubikey

## Des standards 100% ouverts

- WebAuthn pour la partie web (Standard W3C 2019)
- CTAP2 pour la partie matérielle.

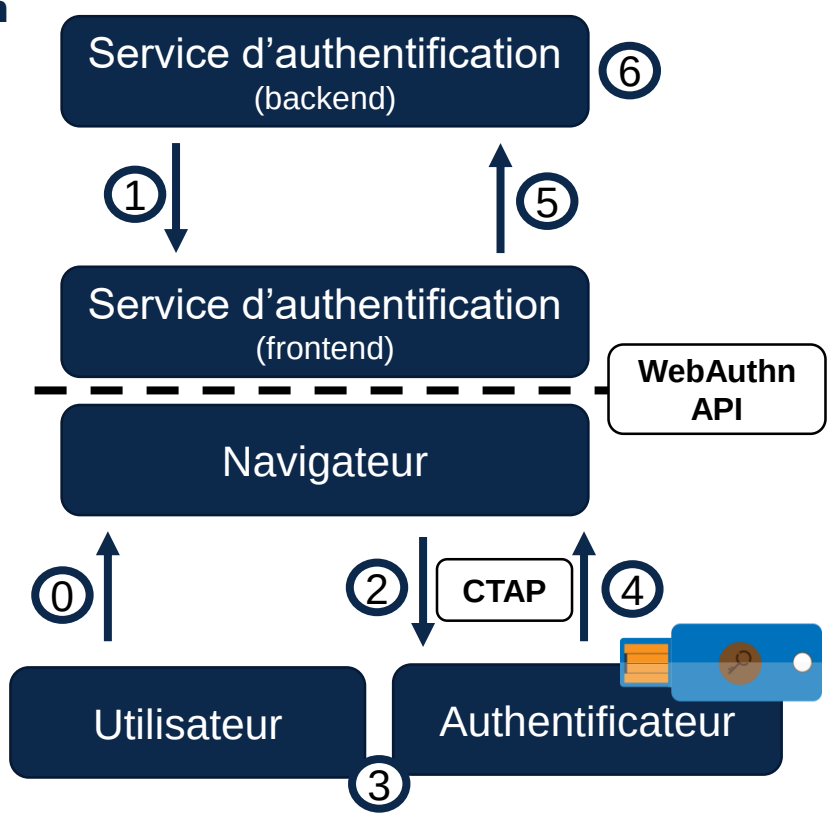
# WebAuthn en détail - enrôlement

0. L'utilisateur accède à la page d'enrôlement
1. Génération d'un challenge côté serveur envoi des infos utilisateur (optionnel)
2. Demande d'enregistrement contenant : challenge + infos utilisateur + métadonnées FIDO
3. Vérification de l'utilisateur (optionnel) génération d'une nouvelle paire de clés signature du challenge
4. Réponse avec la nouvelle clé publique +l'attestation du matériel utilisé (optionnel) +challenge signé
5. Transmission au serveur de l'ensemble
6. Vérification du challenge et de l'attestation +sauvegarde de la clé publique pour l'utilisateur si OK



# WebAuthn en détail - authentification

0. L'utilisateur accède à la page d'authentification
1. Génération d'un challenge côté serveur
2. Demande d'authentification contenant : challenge +métadonnées FIDO
3. Vérification de l'utilisateur (optionnel) +signature du challenge
4. Envoi du challenge signé + clé publique
5. Transmission au serveur de l'ensemble
6. Vérification du challenge et de la clé publique.



# WebAuthn en détail – API JavaScript

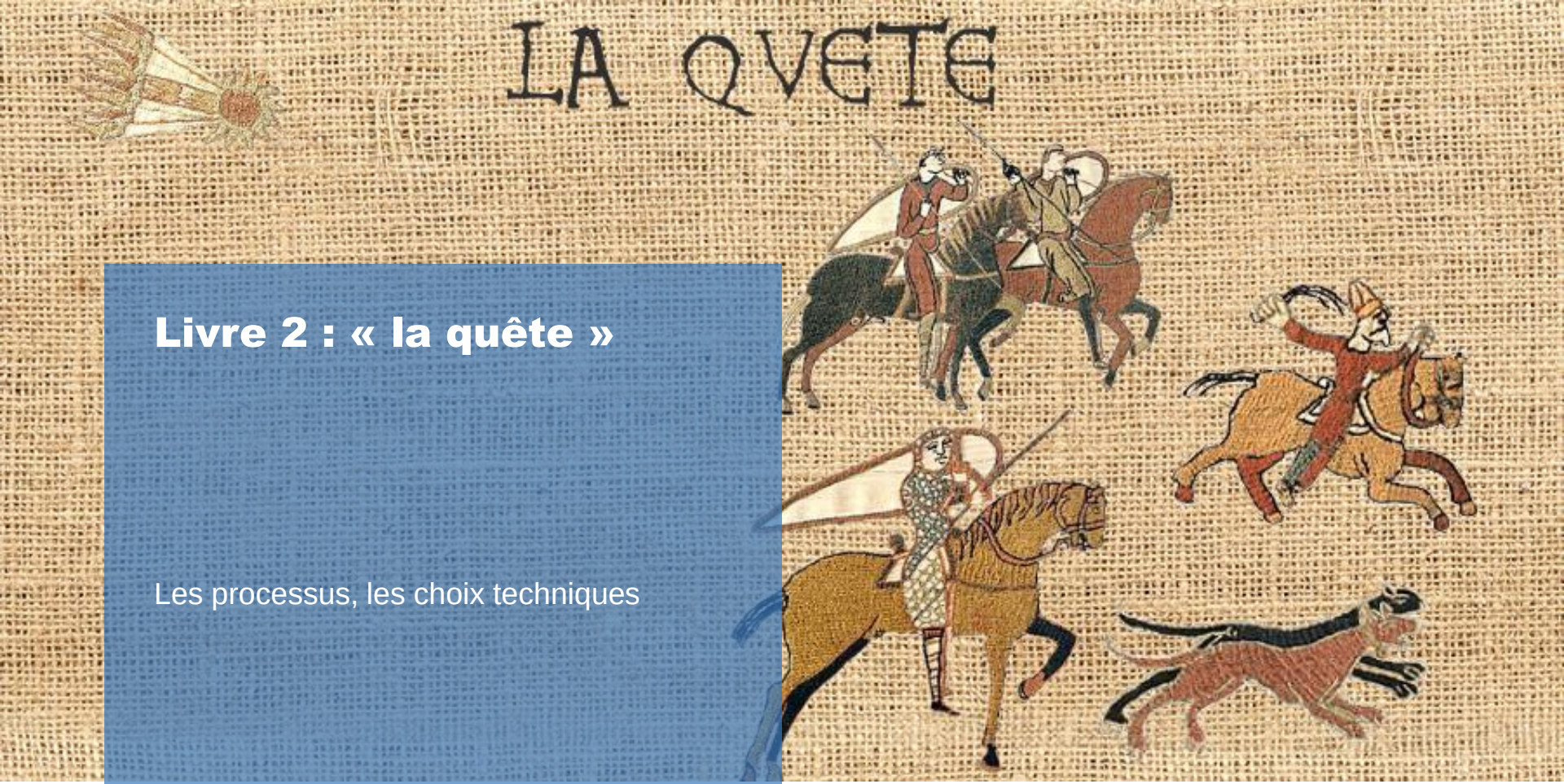
## API WebAuhn enrôlement

```
navigator.credentials.create({
    publicKey: {
        // challenge crypto aléatoire
        challenge: "...",
        // infos de l'application "relying party"
        rp: {},
        // infos de l'utilisateur
        user: {},
        // selection de l'authentificateur
        authenticatorSelection: {},
        // demande d'attestation
        attestation: "...",
        // listes d'algo supportés
        pubKeyCredParams: [{}]
    }
});
```

## API WebAuhn authentification

```
navigator.credentials.get({
    publicKey: {
        // challenge crypto aléatoire
        challenge: "...",
        // choix de la clé publique
        allowCredentials: [{}],
        timeout: "",
        // selection de l'authentificateur
        authenticatorSelection: {}
    }
})
```

Correspond à l'étape **2** sur les schémas précédents




# Livre 2 : « la quête »

Les processus, les choix techniques

# L’enrôlement self-service (ou presque)

## Concilier les exigences de l’AAL3 de certification « face à face » avec la facilité de la clé de sécurité FIDO :

1. L’utilisateur se procure une clé FIDO supportée
2. En « face-à-face » (présentiel ou à distance), il demande à se faire certifier
3. Le certificateur, par l’outil sesame.cnrs.fr, initie la demande d’enrôlement
4. L’utilisateur reçoit par mail une URL contenant un jeton qui lui permet d’enrôler sa clé FIDO
5. A la fin du processus, l’utilisateur peut s’authentifier en 2FA avec son mot de passe et sa clé FIDO

# Le processus de secours

## FIDO2 n'implémente pas de mode de secours !

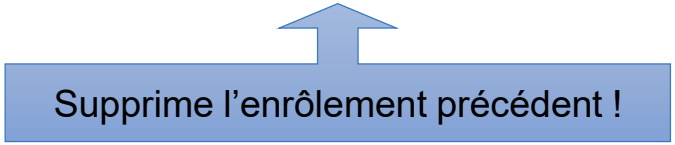
## Comment implémenter un mode de secours sans dégrader l'AAL3 ?

## Les solutions non-retenues :

- Mail OTP
- SMS
- Grilles de secours
- Quorum de confiance
- Questions secrètes
- Assistance utilisateur
- Seconde clé enrôlée

## La solution retenue

- Préconisée par la FIDO Alliance
- Enrôler une nouvelle clé



# Choix techniques

## Solutions explorées

- Intégration au SSO existant (Janus) ou IDP séparé
- Commerciales et communautaires
- Shibboleth IDP, LemonLDAP::NG, Ilex Sign&go, Forgerock AM, Duo Security, CAS …

## Choix d'un IDP séparé (pour commencer)

- Réduire le risque et les impacts sur le SSO et les applications existantes
- Pour mettre en place un pilote rapidement sur quelques applications
- Limiter les développements spécifiques sur l'IDP Shibboleth

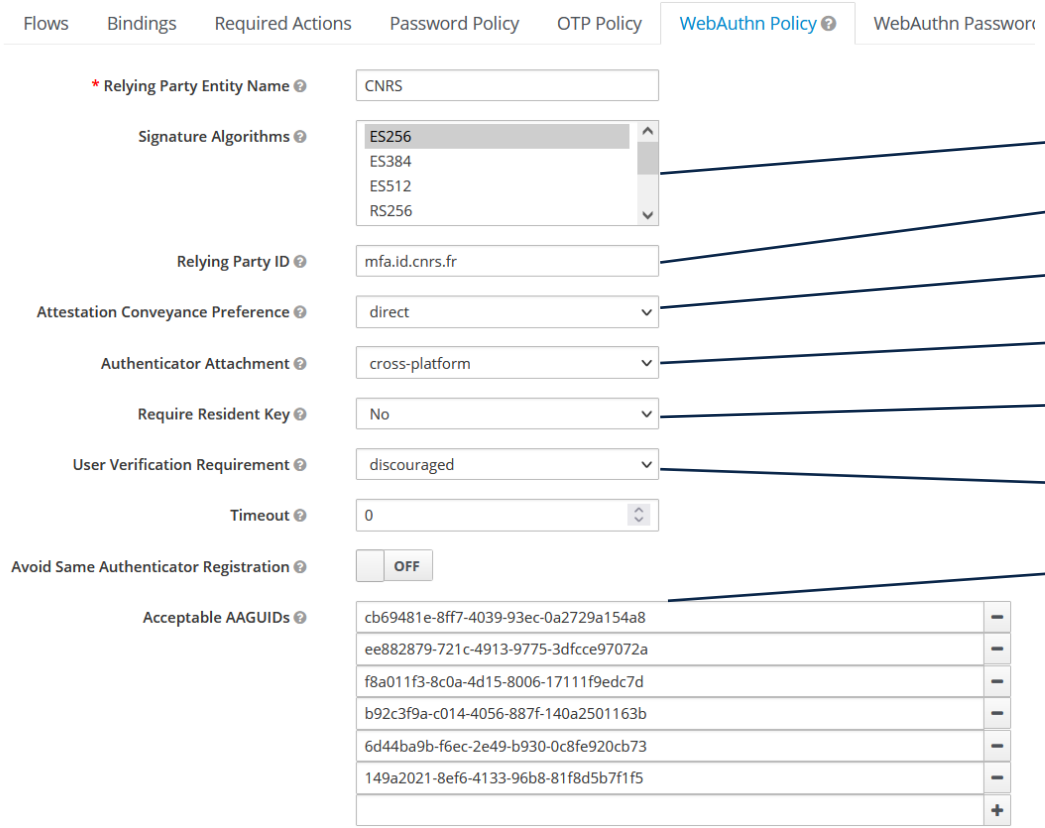
## Keycloak

- Produit communautaire RedHat
- Service d'authentification web en java
- « Clés en main », interface de configuration
- Code libre (Apache License 2.0)
- Supporté par RedHat, tarif au vCPU
- Protocoles SAML et OpenID Connect
- Support natif WebAuthn en preview, en avance sur les autres solutions
- Utilisé par d'autres établissements (CERN)

## Processus d'enrôlement

- Interfaces spécifiques dans l'application de gestion de l'authentification CNRS (Sésame)
- Développées par la DSI du CNRS

# Configuration WebAuthn dans Keycloak




- Algorithme supportés
- Identifiant du RP FIDO2
- Demande d'attestation constructeur
- Authentificateur externe
- Utile seulement pour le « loginless »
- Pas de vérification locale sur l'authentificateur
- Liste de modèles de clés de sécurité acceptés


# Livre 3 : « Avalon »

Le début d’un voyage

# Intégration dans le SI CNRS

## Infrastructure

- Hébergé sur les infrastructures du CNRS au **centre serveur de l'IN2P3**
- Déployé via Ansible
- Opéré par les équipes de la DSI

## Intégration avec les applications

- Raccordement en protocole **SAML 2.0**
- Interopérable et interchangeable avec l'IDP principal CNRS

## Intégration avec les briques IAM

- **LDAP Référentiel** partagé avec l'IDP CNRS, donc même mot de passe
- Accès à Keycloak donné par un **rôle** piloté par l'outil de gestion centralisée des habilitations CNRS.


*Le raccordement des applications sensibles à la DSI du CNRS*

# Conclusion et perspectives

## Aujourd'hui, WebAuthn en 2FA:

- Service transverse d'authentification forte AAL3
- Intégré au SI SAML 2.0 existant
- Briques intégrées (Keycloak) …
- … mais aussi du développement spécifique
- Déploiement discret en cours pour quelques applications sensibles

## Enjeux de la montée à l'échelle

- Service et assistance à plusieurs milliers d'utilisateurs
- Navigateurs et OS de maturités hétérogènes sur le support WebAuthn
- Perte des clés et mode de secours

## FIDO2, une technologie à suivre

- Support grandissant par les solutions cloud ou sur site et par les différents navigateurs et OS
- Aussi en dehors du web : SSH, VPN.

## Demain, le marché s'oriente vers des usages sans mot de passe

- Nouveaux supports authentificateurs : clé de sécurité (USB ou NFC), smartphones ou intégrés à l'OS (Windows Hello, TouchID)
- Niveaux AAL1 ou AAL2

## La norme FIDO2 continue d'évoluer