



Authentification renforcée

Augmenter le niveau de sécurité
de la fédération

Contexte

- Les IdP utilisent une seule méthode d'authentification : login/mot de passe
- Les IdP donnent accès à des ressources +/- sensibles
- Gestion des mots de passe ?

→ Niveau de sécurité faible

Niveaux de confiance (LOA)

- Quelle confiance peut avoir une ressource lors d'une authentification via un IdP ?
- Le niveau de confiance dépend d'un ensemble de paramètres :
 - méthode d'authentification utilisée
 - gestion des enregistrements dans le référentiel
 - ...
- Actuellement 1 seul niveau dans la fédération

Niveaux de confiance (LOA)

- Permet une différenciation de la confiance
 - suivant l'IdP utilisé
 - suivant la méthode d'authentification utilisé sur un IdP
- Permet à un SP d'accorder l'accès en fonction d'un certain de niveau de sécurité
 - encore faut-il qu'il ait les infos (ex : méthode d'authentification utilisé)
- Nécessite des engagements plus précis / gestion des référentiels

Méthodes d'authentification

- Authentification multi-facteurs
 - OTP, certificats X509, token, cartes à puce, biométrie, ...
 - combinaisons possibles
- Base pour une LOA
- Nombreuse études : peu (pas ?) de déploiements
 - difficile à déployer
 - nombreux aspects à prendre en compte (technique, urbanisation, gestion, prix, ...)
 - peu de ressources pour le faire

Authentification renforcée

- ≠ authentification forte
 - 2 facteurs (au moins)
 - Eviter si possible l'utilisation de matériels (carte à puce, token, téléphone, ..)
-
- Gain en sécurité
 - Facilité de déploiement

Authentification renforcée

- Différentes solutions évaluées
 - InWebo
 - DuoSecurity
 - LoginPeople (en cours)
- Choix de InWebo
 - Web
 - OTP
 - utilisation de token virtuel dans le navigateur
 - Support radius, VPN SSL, smartphone, ...
 - Certification ANSSI

La suite

- Déploiement InWebo au GIP
- Etude d'un IdP avec double authentification
 - propagation de la méthode d'authentification sur les SP
- Politique de sécurité
 - sensibilité de la ressource
 - origine de la connexion
 - ...

Questions ?