UNIVERSITÉ DE LYON

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

Aramis
AGRÉGATION RHÔNE-AUVERGNE DES MÉTIERS DE L'INFORMATIQUE DANS LE SUPÉRIEUR

Authentification multifacteur

ESUP-OTP

Hakim YAHIAOUI
Benjamin PIERROT

Qu’est-ce que le MFA ?

Pour nous connecter à un appareil ou à un service en ligne, nous utilisons généralement des noms d’utilisateur et des mots de passe afin d’authentifier notre identité et d’avoir accès à nos comptes.

Mais les mots de passe sont désormais vulnérables et faciles à compromettre. De plus, les attaques de type phishing se multiplient ces dernières années.
Pour atténuer les risques liés à l’identité, une couche de sécurité supplémentaire sous la forme d’une méthode de vérification additionnelle est aujourd’hui utilisée par de nombreux services. Cette méthode est généralement appelée « vérification en deux étapes » ou « Authentification multifacteur (MFA) ».

Quel intérêt ?

* Permet d’améliorer la sécurité de l’organisation
* Les mots de passes sont vulnérables aux attaques (par force brute)
* Ils peuvent être volés par des tiers (phishing)
* Protéger des comptes sensibles (administrateurs, données de recherches, ...)

- Quelque chose que vous connaissez

* Des mots de passe ou des codes PIN mémorisés

- Quelque chose que vous avez

* Un smartphone ou une clé USB sécurisée

- Quelque chose que vous êtes

* une empreinte digitale ou
  une reconnaissance faciale

MFA dans le projet CAS Apereo

L’authentification MFA est facilement intégrable dans le projet CAS apereo via des modules complémentaires à intégrer et des configurations à adapter.

Les principales méthodes existantes :

- Simple
- Duo Security
- Twilio Authy
- Acceptto
- YubiKey
- WiKID
- FIDO
- Swivel Secure
- Google Authenticator

Malheureusement, la plupart ne sont pas libres, sont chers et ne sont pas disponibles en mode auto-hébergé.

CAS Simple

Fonctionnement

- Méthode gérée au niveau du serveur CAS, pas de tiers
- Envoi d'un mail ous SMS avec un code aléatoire
- Se base sur des attributs de l'annuaire LDAP
- Filtre via un groupe

Trusted Device

- Permet de ne saisir le MFA qu'une fois par semaine
- Une saisie par nouveau matériel
- Choix enregistré en base sur les 2 nœuds CAS (répliquée en multi-maître)

ESUP-OTP

Acteurs du projet

- Université Paris 1 Panthéon-Sorbonne
- La Rochelle Université
- Université de Rouen Normandie

Solution financée et distribuée par le consortium Esup-Portail.

Présenté aux JRES 2017 et utilisé par plusieurs établissements depuis.

Licence libre MIT, tout est ainsi ouvert gratuitement à tous : l'ensemble des sources, documentations et présentations .

Alternative aux différents fournisseurs, mode auto-hébergé.

Architecture

3 briques nécessaires :

- **Module esup-otp-cas**
  - À intégrer sur le service CAS (2 noeuds)

- **Esup-otp-api**

  - Brique métier qui calcule les jetons et autres secrets
  - Stocke les informations saisies (Choix méthodes, numéros, mails, applis, ...)
  - Offre une API REST

- **Esup-otp-manager**

  - Partie frontale d'ESUP-OTP
  - Présente une interface web réactive à l'usager
  - Dialogue avec Esup-otp-api

Esup-otp-manager

Utilisateur final :

Accède à l'interface manager pour choisir ses méthodes de MFA
Indique les informations (numéro, mail)
Scanne le QR Code pour utilisation TOTP et push

Gestionnaire :

La liste peut être faite à partir d'un groupe LDAP
Activer/désactiver des méthodes d'un utilisateur
Renseigner un numéro mobile, mail ou réinitialiser les OTP d'un utilisateur
Dépanner un utilisateur bloqué

Administrateur :

Sélectionner les méthodes qui doivent être disponibles pour les utilisateurs finaux
Les modifications sont prises en compte instantanément

Méthodes MFA

Codes aléatoires à usage unique

- Envoi par SMS ou par mail

Codes de secours à imprimer

- liste de codes à usage unique

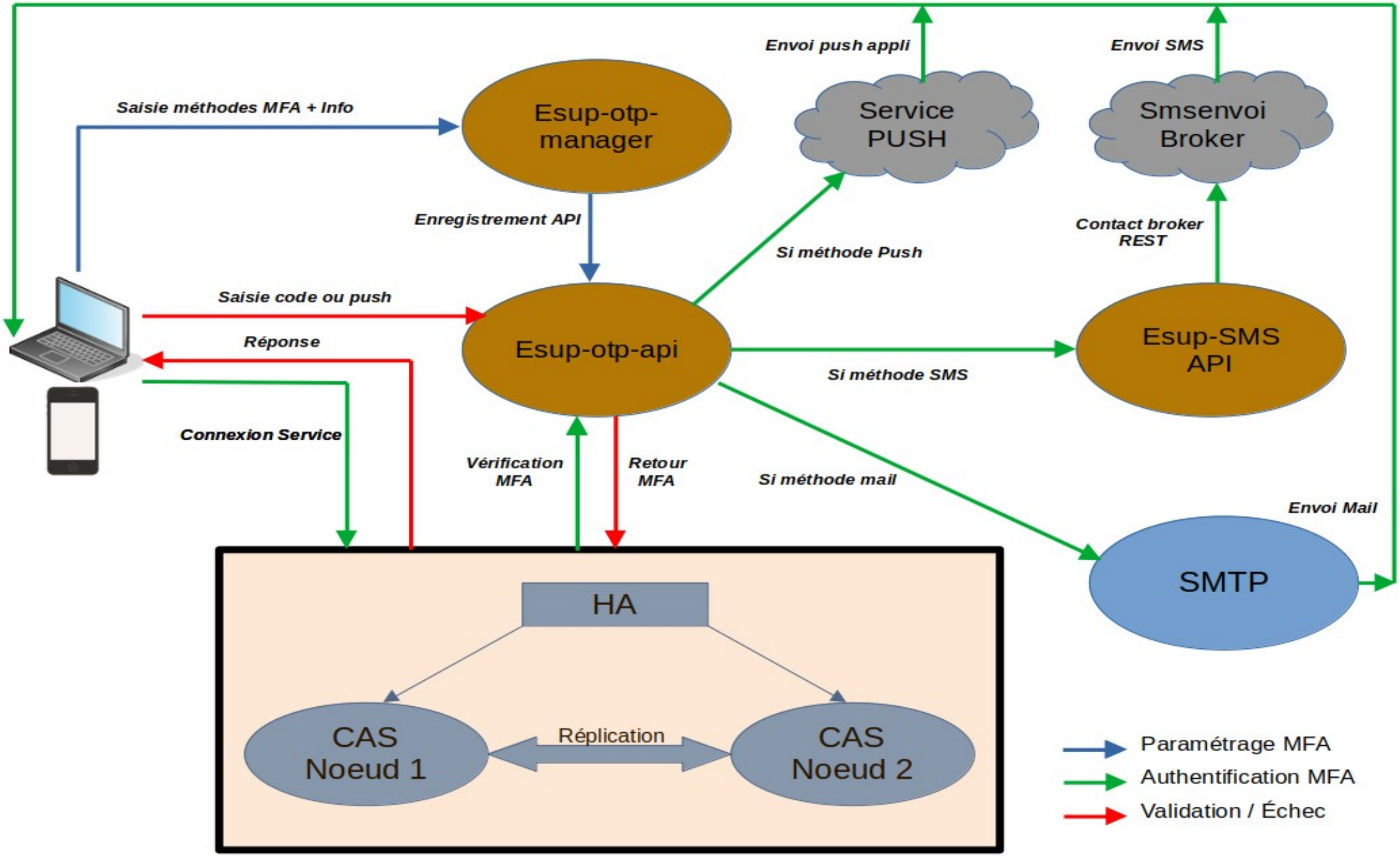
TOTP

- Code à usage unique basé sur le temps
- Google Authenticator, FreeOTP

Push

- Validation par téléphone (notification)
- Application EsupAuth disponible sur Android et IOS

- *Solution par code de secours : non retenue*


Envoi push appli
Envoi SMS
Saisie méthodes MFA + Info
Esup-otp-manager
Service PUSH
Smsenvoi Broker
Enregistrement API
Contact broker REST
Si méthode Push
Saisie code ou push
Réponse
Esup-otp-api
Esup-SMS API
Si méthode SMS
Connexion Service
Vérification MFA
Retour MFA
Si méthode mail
Envoi Mail
SMTP
HA
CAS Noeud 1
Réplication
CAS Noeud 2
Paramétrage MFA
Authentification MFA
Validation / Échec

Démonstration

Retour d’expérience

Solution en production depuis environ 1 an

- **Migration progressive**
  - Informaticiens (obligatoire)
  - ZRR, services sensibles, présidence (obligatoire)
  - Plusieurs directions (obligatoire)
  - Autres Employés (facultatif)
  - Étudiants (rentrée 2024-2025)

- **Mode mixte**
  - MFA facultatif
  - MFA obligatoire

- **Sensibilisation forte faite par notre RSSI en raison du contexte de sécurité**

- **Ajout des utilisateurs victimes de phishing**

Quelques chiffres

635 utilisateurs

- 468 obligatoires
- 167 facultatifs

Méthodes paramétrées :

- TOTP : 18 %
- Push : 11 %
- SMS : 68 %
- Mail : 36 %

Accueil

- Outil majoritairement bien reçu par les utilisateurs
- Formation faite aux administrateurs
- Facile à prendre en main
- Très peu de support
- Demande des directions

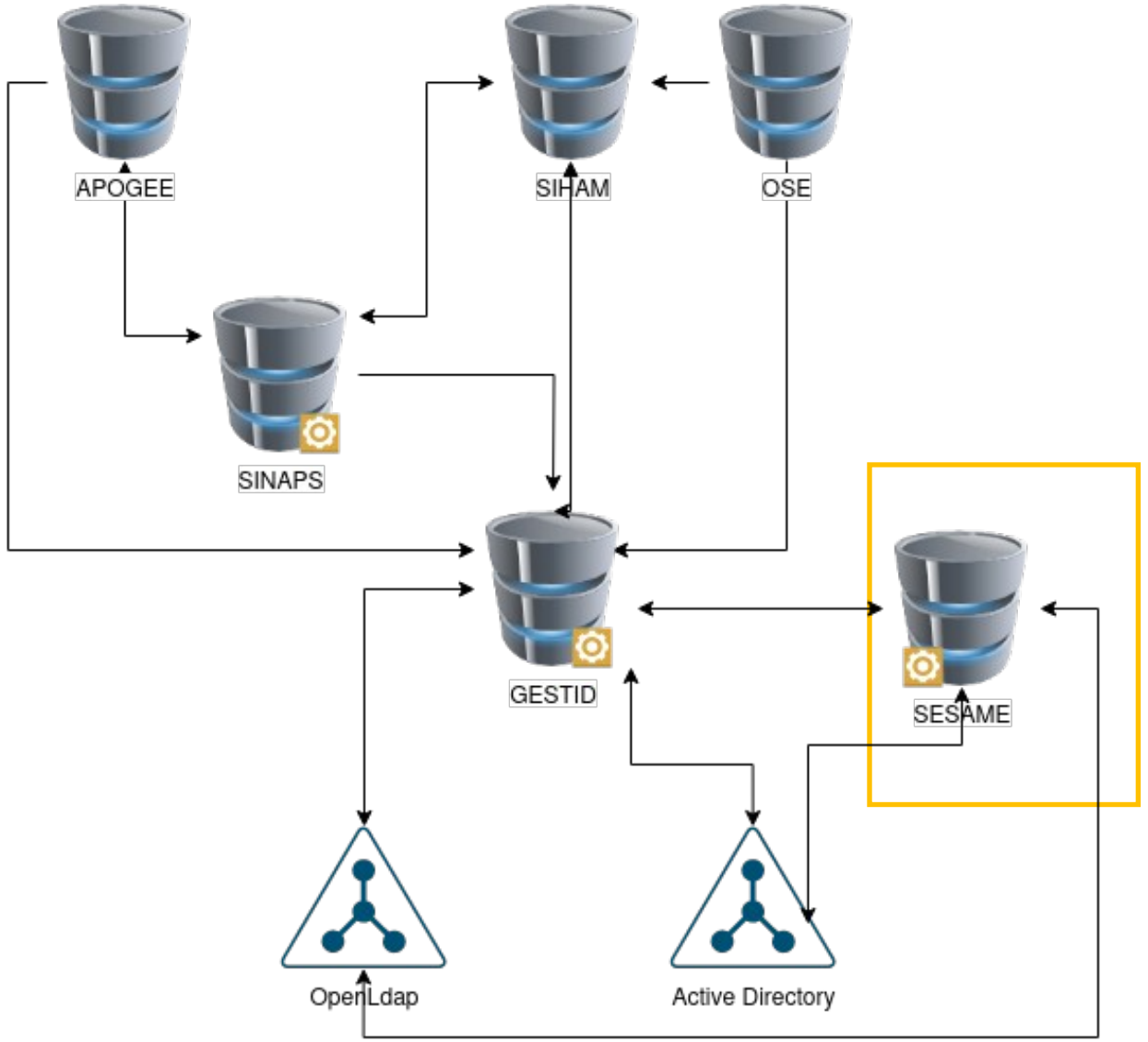
Conclusion

- **Outil complet, nombreuses méthodes**
- **Facile à utiliser**
- **Sécurise fortement le SI**
- **Données privées stockées localement par l'utilisateur lui-même**
- **Possibilité d'utiliser plusieurs modes (obligatoire/facultatif/mixte)**
- **Délégation du support**
- **Développeurs du projet très réactifs**
- **Mises à jour fréquentes**

- **Points d'attention :**

- Bonne communication indispensable
- Infrastructure CAS complexifiée
- Lors des MAJ majeures, il faudra prendre en comptes ces nouvelles briques
- Reprise de la charte graphique

Intégration de l’application au SI de l’UJM



Architecture SI

Fonctionnalités de Sésame

- Activation de compte
- Changement de mot de passe
- Modification du quota
- Gestion des groupes collaboratifs
- Invitation des personnes extérieures
- Boîte à outils pour le pôle proximité
- Administration messagerie Partage
- **Activation désactivation du MFA**

Mon compte
Double authentification
Mon quota de stockage
Signature de Mél.
Charte informatique
CROUS
Gestion des comptes
Gestion des FAQ
Gestion des Groupes
Gestion comptes Wifi
Gestion comptes extérieurs
Autres fonctionnalités
Gestion de mes alias

Double authentification

Gestion de votre double authentification (MFA)

La double authentification vous permet de sécuriser l'accès à votre compte UJM, notamment en cas de vol de mot de passe. Elle consiste à envoyer un code de vérification sur une adresse électronique personnelle une application installée sur votre smartphone ou un sms sur votre numéro de portable.

En savoir plus sur le MFA

☐ Actuellement la double authentification n'est pas activée pour votre compte.

Activer la double authentification

Mon compte
Double authentification
Mon quota de stockage
Signature de Mél.
Charte informatique
CROUS
Gestion des comptes
Gestion des FAQ
Gestion des Groupes
Gestion comptes Wifi
Gestion comptes extérieurs
Autres fonctionnalités
Gestion de mes alias

Double authentification

Gestion de votre double authentification (MFA)

La double authentification vous permet de sécuriser l'accès à votre compte UJM, notamment en cas de vol de mot de passe. Elle consiste à envoyer un code de vérification sur une adresse électronique personnelle une application installée sur votre smartphone ou un sms sur votre numéro de portable.

En savoir plus sur le MFA

Actuellement la double authentification est activée sur votre compte.

Paramétrer ses méthodes de réception du code

ATTENTION : le paramétrage des méthodes de réception nécessitent que vous soyez sur le réseau de l'Université ou que vous soyez connecté en VPN.

Vous appartenez à une catégorie de population pour laquelle la double authentification est obligatoire et ne peut être désactivée.

Fonctionnement avec 3 groupes LDAP

- Un groupe double authentification facultative
- Un groupe double authentification obligatoire
- Un groupe double authentification manuel (phishing)

Questions


UNIVERSITÉ
DE LYON
UNIVERSITÉ
JEAN MONNET
SAINT-ÉTIENNE