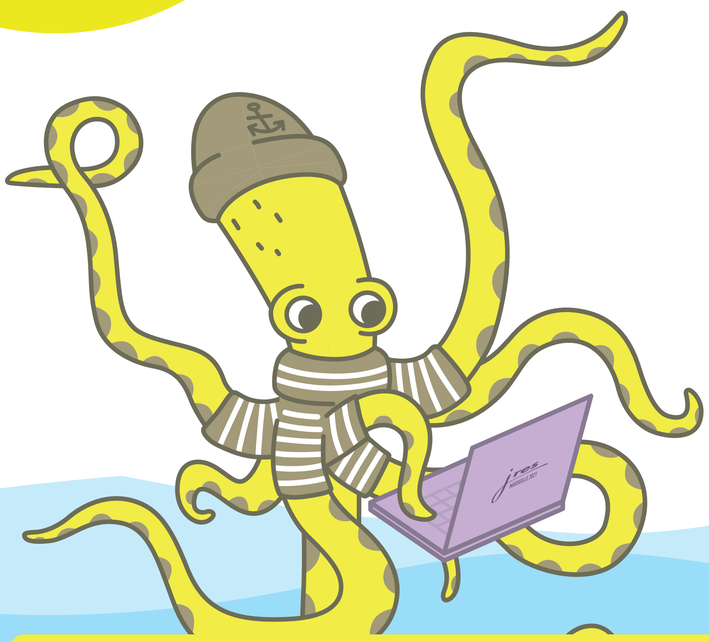
jres MARSEILLE 2021 2022

esup portail

ESUP-OTP

Solution libre et open source pour la gestion de l'authentification forte

Aymar Anli, Vincent Bonamy
Université Paris 1 Panthéon-Sorbonne, Université de Rouen Normandie



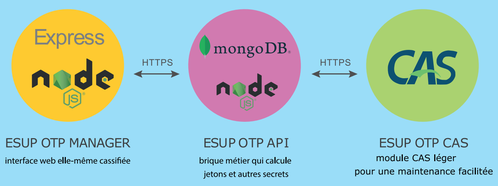
La plupart des établissements de l'ESR utilise CAS.

ESUP-OTP est une alternative libre aux MFA proposées nativement dans Apereo CAS.

Une solution d'authentification multi-facteurs :

- libre	licence MIT
- auto-hébergée	souveraineté numérique
- simple d'installation	environnement classique ESR
- simple d'usage	interface web ; l'utilisateur choisit sa/ses MFA
- gestion facilitée	interface web permettant le dépannage des utilisateurs

Architecture logicielle



Couverture fonctionnelle

Utilisateurs finaux

gestion des mots de passe à usage unique
activation / désactivation des MFA disponibles
renseignement du n° portable, appareillage du smartphone
impression de codes de secours, initialisation algorithme OTP

Gestionnaires

définis depuis un groupe / attributs CAS
dépannage des utilisateurs

Administrateurs

sélection des méthodes et des transports proposés

MFA disponibles

Code temporel (TOTP) 

Codes de secours à imprimer 

Notification - Esup Auth 

Badgeage de carte Esup NFC 

Code à usage unique sms ou mail 

Installation et intégration

Installation d'ESUP-OTP

esup-otp-api et esup-otp-manager : NodeJS via npm
esup-otp-cas : module CAS

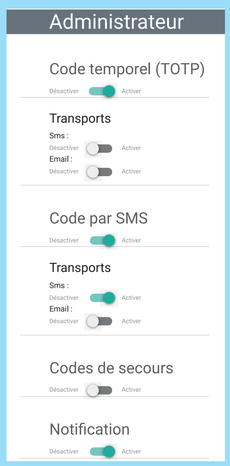
les fichiers README suffisent pour une installation rapide

Activation de la MFA

multiples possibilités ... le plus souple, par script Groovy

```
cas.authn.mfa.groovy-script.location=file:/etc/cas/config/mfaGroovyTrigger.groovy
```

```
class SampleGroovyEventResolver {
  def String run(service, registeredService, authentication, httpRequest, logger, ... other_args) {
    if( (int)registeredService.id in [10, 11, 12, 13] &&
        httpRequest.getRemoteAddr().startsWith("192.168.") && ... ) {
      return "mfa-esupotp"
    }
    return null
}
```



MFA sur un service Shibbolethisé

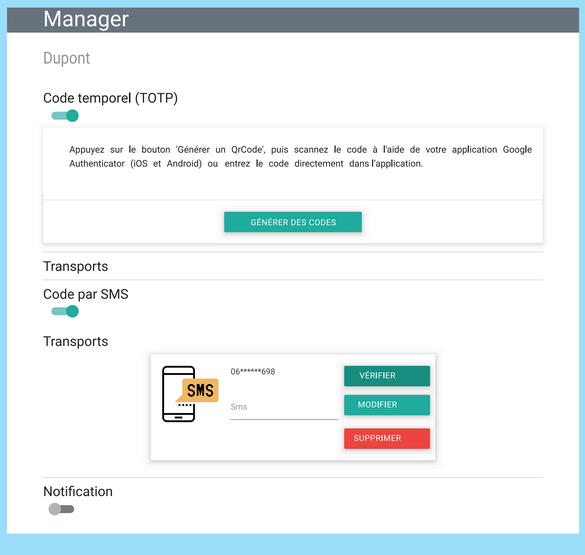
Théoriquement possibile sur le SP via le Profil MFA de REFEDS

MAIS { Actuellement le plus simple, pertinent, pragmatique, le faire côté IdP via Shib-cas-authn

```
shibcas.entityIdLocation=embed
```

et CAS {

```
@class" : "org.apereo.cas.services.RegexRegisteredService""
serviceId": "^http://idp\\.univ-ville\\.fr/idp/Authn/External\\?conversation=[a-z0-9]*
            &entityId=https://mon-sp-sensible\\.univ-ville\\.fr",...}
```



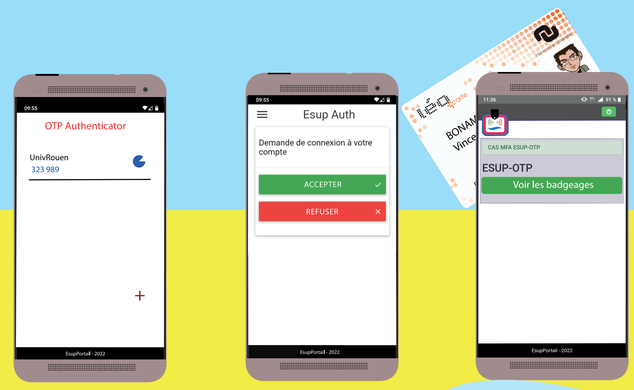
Retours d'expérience

Université Paris1 Panthéon-Sorbonne

Depuis 2017, ESUP-OTP avec chaînage de CAS.
2FA pour VPN, gestion OTP, gestion de groupes (Grouper).
Bientôt parapheur électronique (esup-signature) et webmail.
1200 utilisateurs ont activé la MFA.
En 5 ans, aucun dysfonctionnement majeur.

Université de Rouen Normandie

En 2022, l'URN est un utilisateur récent d'ESUP-OTP.
CAS 6.4, règles spécifiques d'activation via script groovy, Trusted Devices/Browsers ...
Via ESUP-OTP, l'URN tente de convaincre ses utilisateurs de participer à renforcer la sécurité des services numériques.



Nécessaire pour sécuriser au mieux nos SI, l'usage de la MFA reste long à faire accepter.

Les mécanismes souples d'ESUP-OTP allié à CAS facilitent l'adoption de la MFA.

C'est avec le soutien des utilisateurs que la généralisation de l'usage d'un tel outil peut avoir lieu.

esup-otp-cas / mire CAS

esup-otp-manager / vue utilisateur

Conception affiche : Yassamine Amiri

UNIVERSITÉ DE ROUEN NORMANDIE

https://www.esup-portail.org/wiki/display/esupotp

UNIVERSITÉ PARIS 1 PANTHÉON SORBONNE