

ESUP-DAYS (38)

MENER UN PROJET MFA DANS L'ESR POUR DE VRAI !

Aymar ANLI -- Université Paris 1 Panthéon-Sorbonne

PLAN

◆ ESUP-OTP

- ◆ Genèse et objectifs du projet
- ◆ Principales fonctionnalités
- ◆ Architecture technique

◆ Mise en œuvre à Paris 1

- ◆ Démarche adoptée
- ◆ Dates marquantes
- ◆ Usages

◆ Conclusion & Perspectives

◆ Genèse

- ◆ Lors des premiers ateliers ESUP-Authentification (2013-2014)
- ◆ Identification du besoin de MFA
- ◆ Pas de solution sur les outils déployés dans l'ESR (CAS et Shibboleth)
- ◆ Solutions payantes et/ou cloud hors UE
- ◆ Chères et non open source

◆ Objectifs

- ◆ Solution utilisable avec CAS
- ◆ Open source
- ◆ Auto hébergée
- ◆ Self activation et choix de méthodes
- ◆ Interface de gestion pour l'assistance

PRINCIPALES FONCTIONNALITÉS

- ◆ Plusieurs méthodes OTP disponibles
- ◆ Choix des méthodes par l'utilisateur et/ou par l'administrateur
- ◆ Disponibilités des méthodes par profil
- ◆ Durée de validité de l'OTP par service (esup-otp-cas-server)

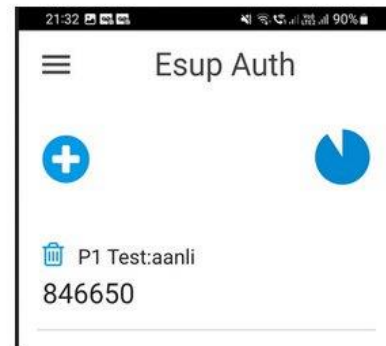
MÉTHODES DISPONIBLES



Codes à imprimer



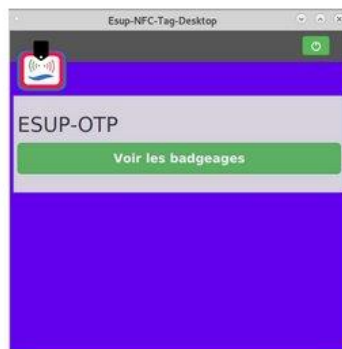
SMS/Mail



TOTP



Notification mobile

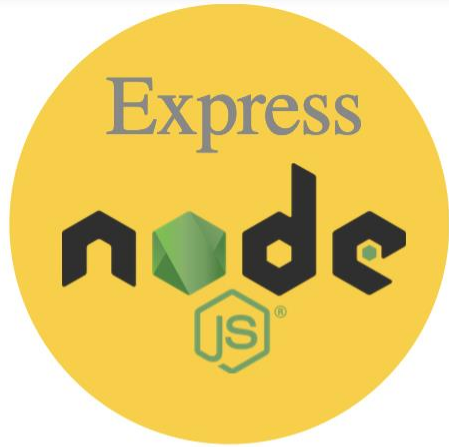


Badgeage NFC



WebAuthn

ARCHITECTURE TECHNIQUE



ESUP OTP MANAGER

CASsified web application

User preferences

User help/assistance

Administration UI

HTTPS
↔



ESUP OTP API

REST API

Code generation methods

Code transports

HTTPS
↔



ESUP OTP CAS

CAS module

esup-otp-cas-server



PANTHÉON SORBONNE
UNIVERSITÉ PARIS 1

MISE EN ŒUVRE À L'UNIVERSITÉ PARIS 1 PANTHÉON-SORBONNE

3 grands domaines

Sciences économiques et de gestion

Arts et sciences humaines

Sciences juridiques et science politique



+45 000
ÉTUDIANTS

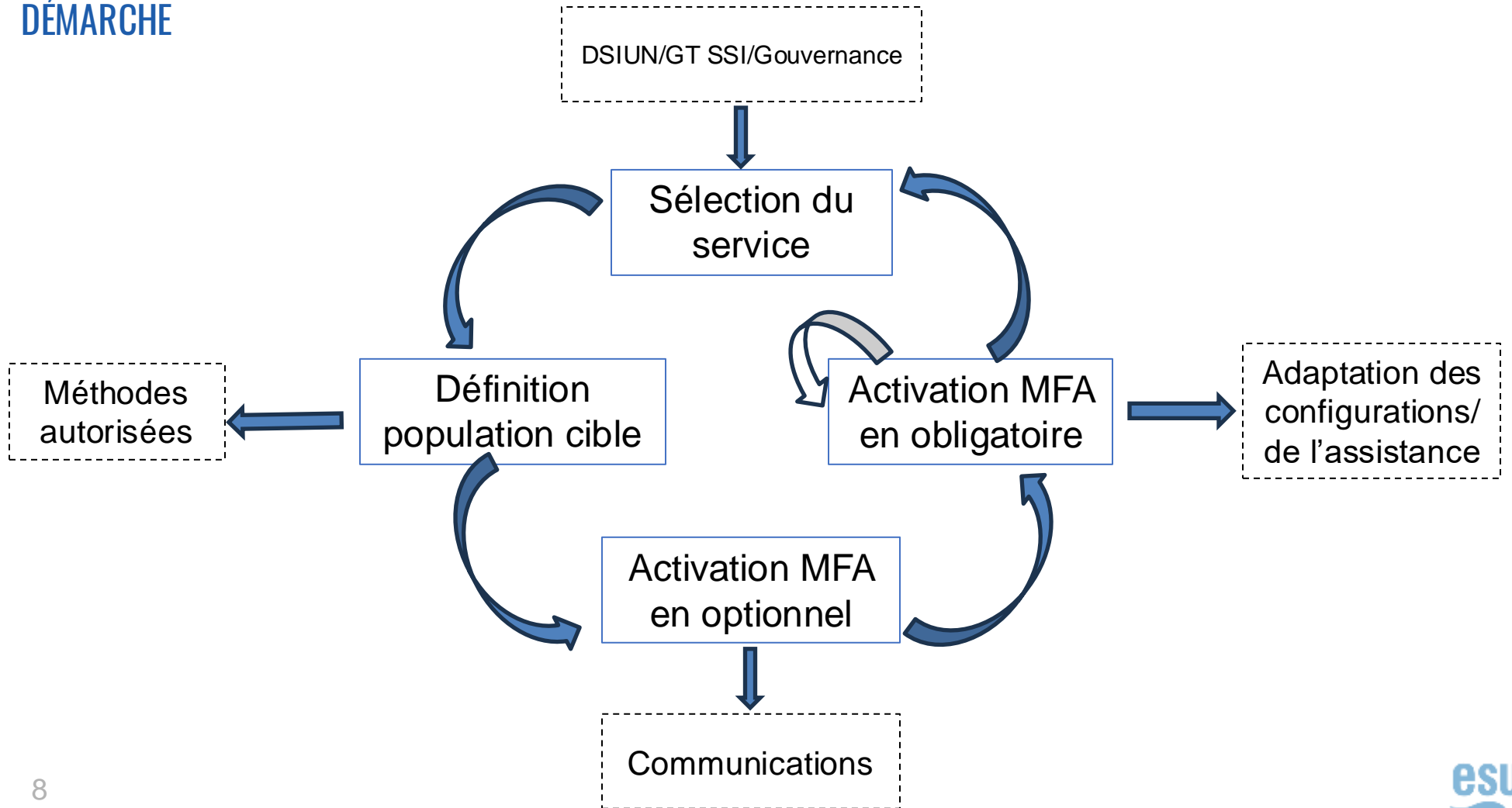


+1200
PERSONNELS ADMINISTRATIFS
ET DE BIBLIOTHÈQUES

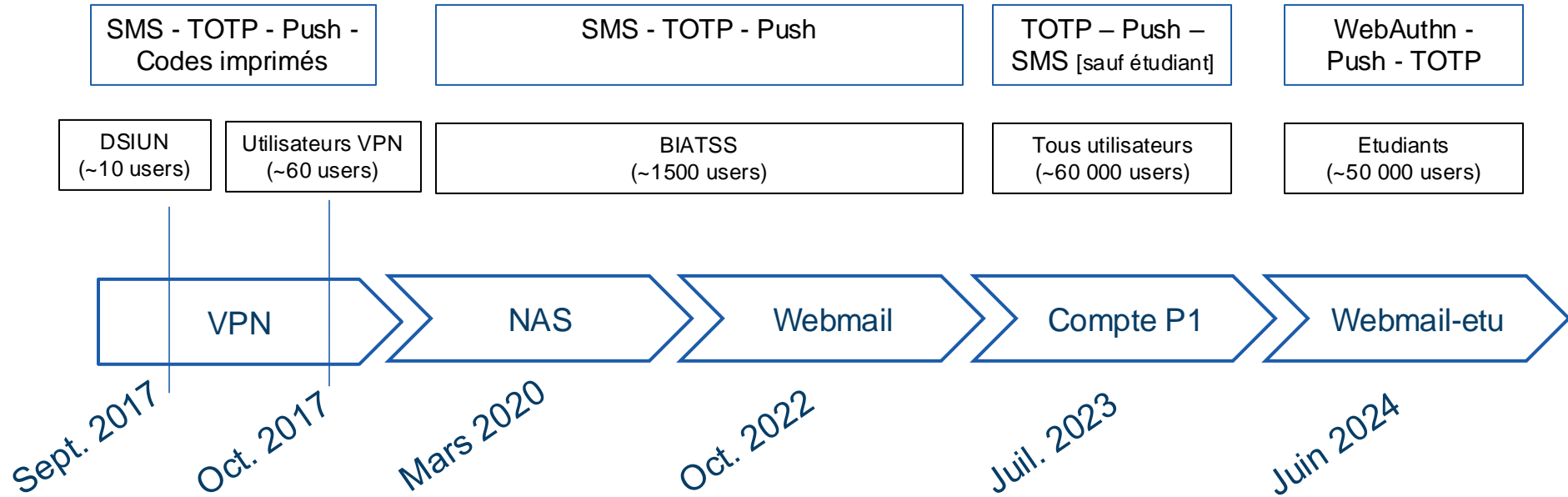


+1500
ENSEIGNANTS
ET ENSEIGNANTS CHERCHEURS

DÉMARCHE

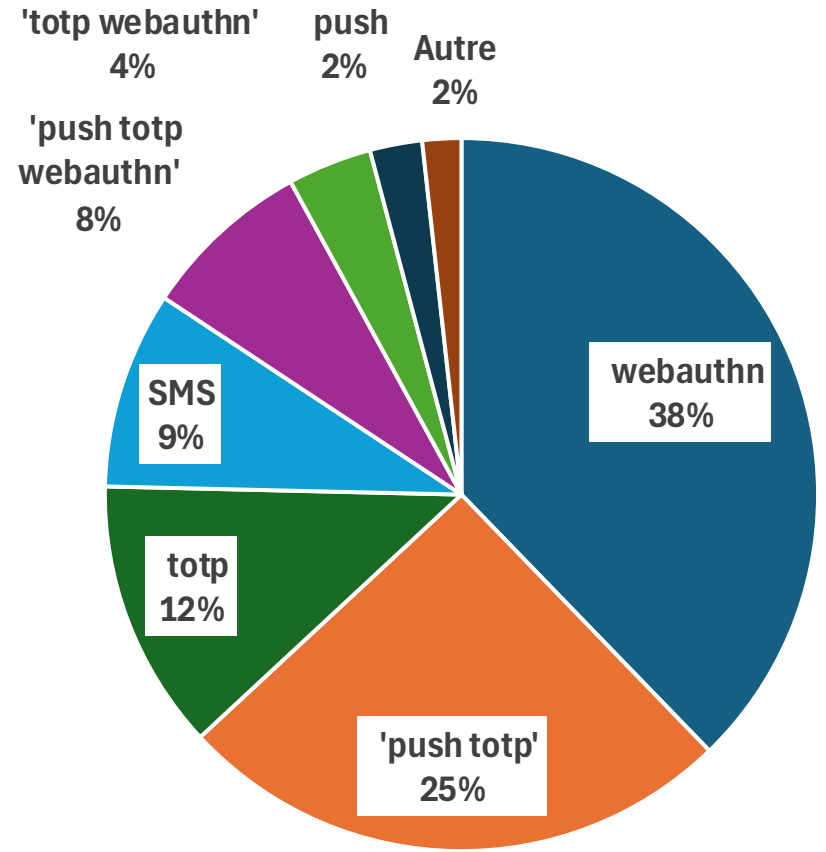
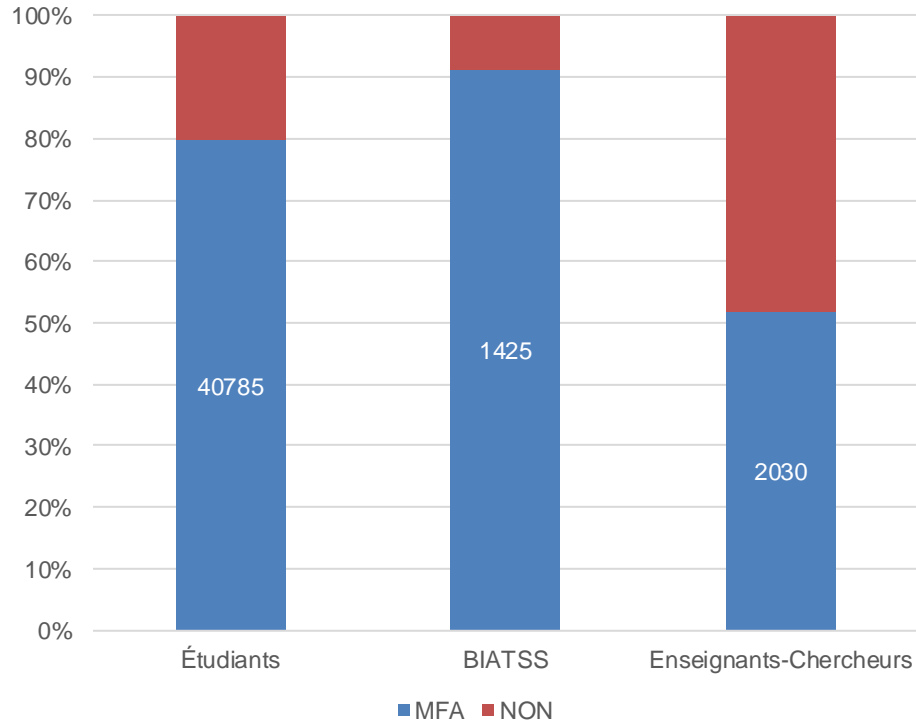


DATES MARQUANTES



USAGES

Activation MFA



Méthodes activées par les utilisateurs

CONCLUSION

- ◆ 78% de nos utilisateurs (étudiants, BIATSS, E-C) ont activé la MFA
- ◆ Les utilisateurs acceptent globalement la MFA
- ◆ Besoin de procédure de self réinitialisation de l'OTP
- ◆ Vers une généralisation à l'ensemble de nos services en ligne ?

ESUP-OTP : TRAVAUX EN COURS

- ◆ Authentification NFC via l'app Esup Auth (iOS & Android)
- ◆ Méthode des grilles de codes
- ◆ Module Shibboleth (avec Renater)
- ◆ Accessibilité (avec l'INRIA)



ESUP OTP Manager

Vous permet d'ajouter un deuxième niveau de protection à votre compte (authentification double facteur). Ainsi, il sera impossible d'accéder à votre compte même avec votre mot de passe.



Dans vos préférences, nous vous conseillons fortement de paramétrer au moins 2 méthodes afin de pouvoir assurer la continuité d'utilisation des services numériques.

Consultez la fiche d'aide du paramétrage

Vous pouvez définir :



Facteur physique d'authentification
WebAuthn (Smartphone, Windows Hello, TouchID, ...).



qu'une notification / push soit envoyée sur l'application Esup Auth (Android, iOS).



qu'un code (TOTP) soit généré dans une application (Esup Auth, Authenticator, Plugin OTP...).



qu'un code à usage unique vous soit envoyé par SMS.



une connexion en badgeant avec votre carte d'étudiant ou professionnelle.

ESUP-DAYS 38

CONTRIBUTEURS ESUP-OTP

FLORIAN NARI
MOUHAMED BASSIROU DEME
PASCAL RIGAUX
PENIEL GLORIEL MMEN
VINCENT BONAMY

MERCI !