Université de Lille

Journée Sécurité Min2Rien
décembre 2025

Projet MFA

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

Université de Lille

De quoi va-t-on parler ?

- De la problématique
- De notre démarche de recherche
- Des tests qu’on a pu effectuer
- Du calendrier de déploiement
- Un peu de technique mais très peu…

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

Université de Lille

Problématique

- On a sécurisé une grande partie des postes de travail (Près de 20000 postes et serveurs protégés via EDR/SOC externalisé 24x7) mais :
  - Le nombre de compromissions de comptes reste important (toutes les semaines)
  - Plus de 80% des attaques réussies trouvent leur origine dans une compromission de comptes (pas forcément avec des privilèges élevés).
  - Ca tombe dru pas loin de chez nous ou dans notre écosystème
- La législation évolue…
  - NIS2 bientôt qui va nous obliger à mettre en place une authentification sécurisée
- Bref… Le temps presse, après avoir traité les postes il faut maintenant s'attaquer à l'interface chaise-clavier.
  - Campagnes de sensibilisation au phishing
  - MFA !

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

C’est quoi le MFA ?

Selon Wikipedia :

La double authentification, authentification à deux facteurs (A2F), authentification à double facteur ou vérification en deux étapes ou à deux étapes (two-factor authentication en anglais, ou 2FA) est une méthode d'authentification forte par laquelle un utilisateur ne peut accéder à une ressource informatique (un ordinateur, un téléphone intelligent ou encore un site web) qu’après avoir présenté à un mécanisme d'authentification deux preuves d'identité distinctes. Un exemple de ce processus est l'accès à un compte bancaire grâce à un guichet automatique bancaire : seule la combinaison de la carte bancaire (que l'usager détient) et du numéro d'identification personnel (que l'usager connaît) permet de consulter le solde du compte et de retirer de l'argent.

L’authentification multiple, plus communément appelée authentification à facteurs multiples, authentification multi-facteurs ou authentification à étapes (multi-factor authentication en anglais, MFA) exige, quant à elle, plus de deux preuves d'identité.

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

Déroulement du projet – Phase 1 - Etude

- Cahier des charges
  - Utilisable dans le contexte Université de Lille (VPN, CAS…)
  - Simple d'utilisation (le plus possible)
  - Sécurisé (le plus possible)
  - Pas trop cher, voire gratuit
  - Multiplateforme
  - De préférence en mode SaaS (circulaire 6404/SG du 31 mai 2023)
  - Répondant aux préconisations (si possible avec le tampon ANSSI)
  - Ne demandant pas trop de ressources en interne (rien n'est gratuit)
  - ⚠ Ne nécessitant pas que l'usager possède un téléphone mobile, donc avec la possibilité d'installer sur sa machine un logiciel permettant de saisir un facteur complémentaire
  - Consultation d'autres universités pour se faire une idée (AMU, Orléans, Clermont, Toulon) et mieux connaître la solution TrustBuilder

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

Déroulement du projet – Phase 1 - Etude

- Solutions étudiées
  - EsupOTP
    - Pas de coût de licence
    - OnPremise
    - Consortium Esup assurant le développement
  - TrustBuilder
    - SAML2
    - Payant mais un coût raisonnable (au marché du Groupe Logiciels), pas de maintenance
    - Externalisé (mode SaaS), nécessite peu de ressources internes
    - **Souveraine, certifiée ANSSI**
    - Accompagnement de l'éditeur
    - Pilotable via des API

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

Université de Lille

Déroulement du projet – Phase 1 - Etude

- Notre choix
  - TrustBuilder
    - Excellent retour des universités consultées
    - Mise en place très rapide
    - Externalisé (mode SaaS), nécessite peu de ressources internes (peu ou pas de ressources disponibles pour intégration et maintenance)
    - Solution techniquement plus avancée que le TOTP classique
    - Pilotable via des API

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

Déroulement du projet – Phase 2 - Tests

- Travail avec le DPO (car fourniture des comptes mail à un sous-traitant) pour la déclaration de traitement
- Préparation d'une documentation pour les usagers
- Choix de la population test, périmètre choisi : VPN (OpenVPN)
- Réunion de présentation aux équipes support
- Création des comptes chez TrustBuilder, invitation par mail aux usagers à l'activer.
  - A la main pour commencer (novembre 2025)
  - Rappels (les invitations sont valables 21 jours)
- MFA forcé pour la population test le 15 avril 2025

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

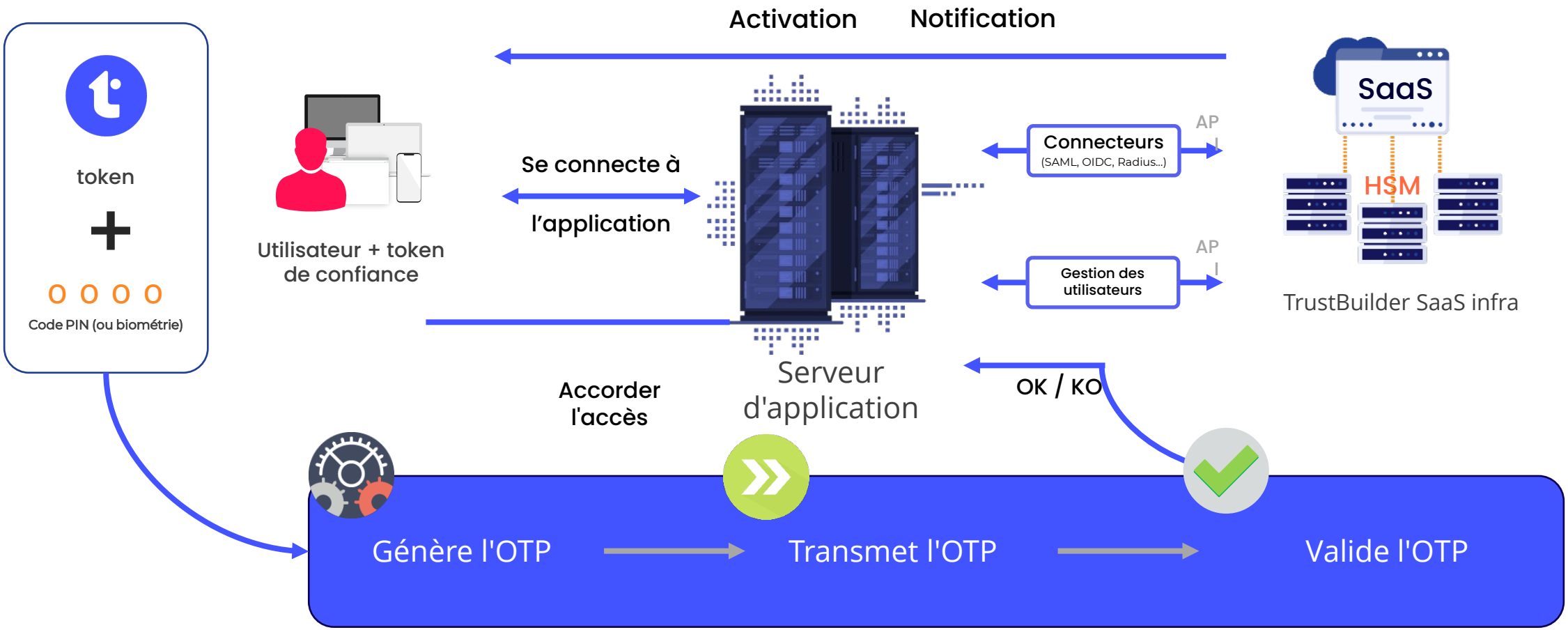
Où en est-on dans le déploiement ?

- ☑ 200 clients actifs, pour une connexion au VPN
- Développement en cours pour interfaçage avec l'identité numérique de l'Université.
  - Installation d'un serveur iWDS de synchronisation avec l'annuaire LDAP qui permet :
    - Gestion automatique des comptes au fil de l'eau
      - Arrivées
      - Départs
    - Possibilité d'activer ou désactiver les comptes
      - Avant le premier usage pour maîtriser les phases de déploiement par service ou entité
      - En cas de compromission
- Production de documentations, clips vidéo

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

3 - Solution SaaS

Architecture technique



Ce qui reste à faire

- Pilotage par l'API TrustBuilder des comptes usagers
- Généralisation à l'ensemble des usagers du VPN (y compris prestataires externes). Cible : 8000 postes d'ici à la fin de l'année 2026
- Généralisation à certaines applications sensibles via l'ENT pour les personnels, par vagues (populations)
  ou
  Généralisation à tout l'ENT (par vagues)
- Extension à la population étudiante
- …
- Intégration de l'outil d'authentification à l'application mobile étudiants, au master des postes de travail…

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

Retour d’expérience

- Principaux problèmes rencontrés
  - Entre la chaise et le clavier (comptes pas activés dans les temps, code PIN oublié, blocage suite à plusieurs tentatives erronées…)
  - Rien d’autre…
- Fonctionnement simple, ça marche…
- Coût acceptable à l’échelle d’un budget informatique, au regard du bénéfice apporté.
- Place au déploiement généralisé

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE

Université de Lille

…Des questions ?

DGDNUM / RSSI
Christophe MASSON, Thierry DELMEIRE