ELYSIUM
SECURITY

Conférence CYBER

MFA et 2FA, de l’attaque à la défense

Connaître les risques pour mieux protéger son environnement

Sommaire

1. Contexte
2. Risques et attaques
3. Démonstration
4. Recommandations
5. Questions

Elysium Security

Intervenant

Yoan ISSARTEL

- Associé Elysium Security / Root-Me PRO
- Expert en sécurité défensive
- Spécialités :
  - ✓ Architecture sécurisée
  - ✓ Supervision de sécurité
  - ✓ Réponse à incident et gestion de crise

INDÉPENDANCE

L'autofinancement de nos activités vous garantit un conseil fiable et des produits réellement adaptés à vos problématiques.

EXPERTISE

Chez Elysium, la compétence est reine. L'expérience cumulée de nos experts permet de bénéficier d'une couverture globale de vos besoins.

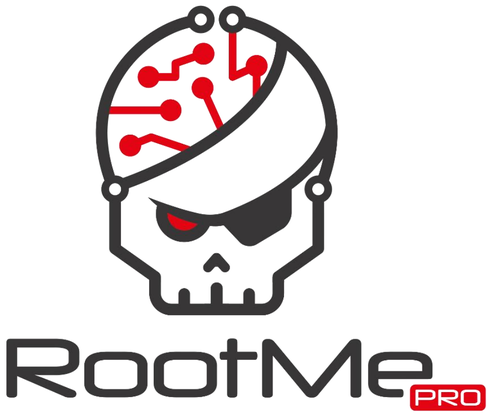
PROXIMITÉ

Notre mission implique confiance et réactivité. Nos clients peuvent compter sur un contact étroit avec nos équipes et partenaires.

TRANSPARENCE

Nous ne promettons jamais l'impossible et faisons toujours le maximum pour apporter une protection optimale à chaque contexte.

Nos actions dans le secteur de la santé

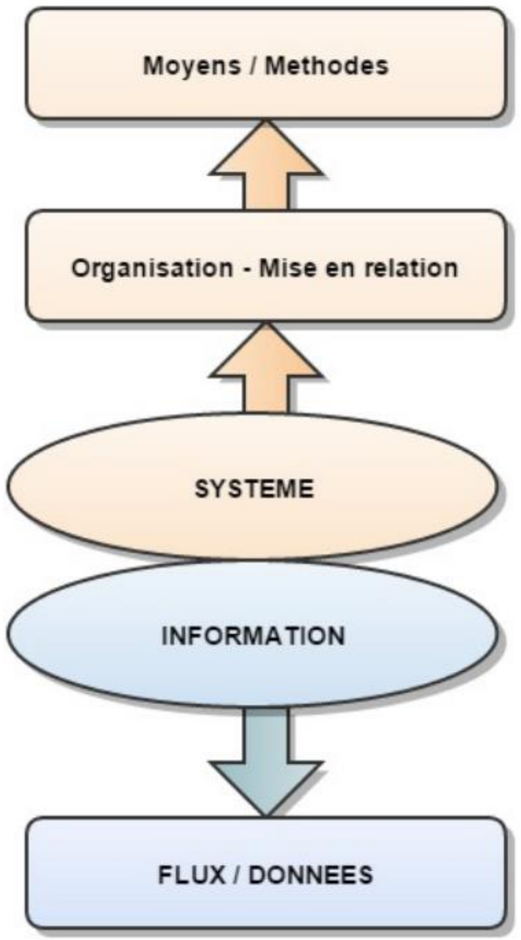


Identifier	▪ Audits de sécurité (tests d'intrusion, audit d'architecture, …), ▪ Cartographies et inventaires (puits de logs, sondes, …), …
Protéger	▪ Gestion des identités et des accès (IAM, SSO, MFA, PAM, …), ▪ Formations et sensibilisations, …
Détecter	▪ Intégration de solutions de détection (EDR, sondes, SIEM, …), ▪ Supervision de sécurité (SOC), …
Réagir	▪ Intégration de solutions de réponse à incident, ▪ Réponse à incident et gestion de crise, …
Se remettre	▪ Intégration de solutions de continuité/reprise d'activité, ▪ Mise à disposition de solutions de crise, …

1.

Contexte

Système d'information



Patrimoine informationnel

Information

« **l'information** est ce qui donne une forme à l'esprit […] donner forme à ». L'information est aussi une « indication, renseignement que l'on donne ou que l'on obtient sur quelqu'un ou quelque chose ». D'un point de vue informatique « il s'agit d'un élément de connaissance susceptible d'être représenté à l'aide de convention pour être conservé, traité ou communiqué » src: Larousse

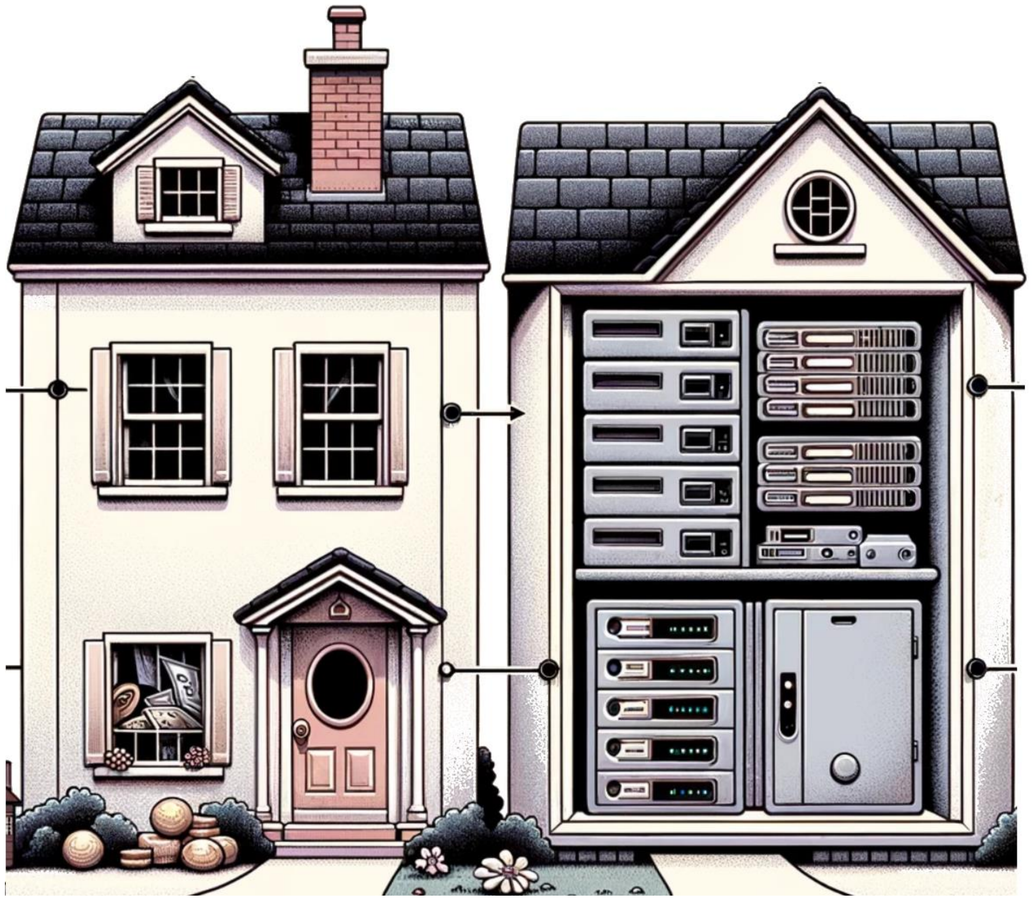
Formats — Stockage / Traitement / Flux — Données

Système d'information (SI)

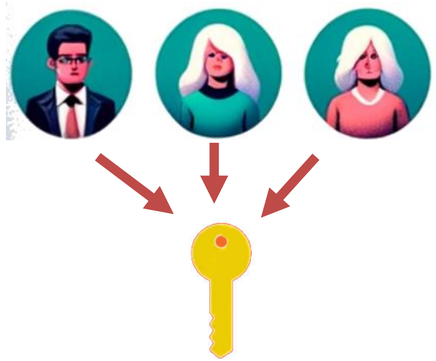
- **Un SI est un ensemble organisé de ressources (humaines, matérielles, immatérielles) qui permet de gérer, traiter, stocker et diffuser (flux) de l'information (données).**
- Parmi ces moyens et méthodes qui permettent d'organiser et de mettre en relation ces éléments ressortent deux grands piliers complémentaires: la **gouvernance du SI** et **l'architecture du SI.**

Analogie entre Maison et SI

Actifs
Bijoux, argent, souvenirs, voitures, papiers, etc.



Actifs
Données (brevet, CB, personnelles)
Applications, services, etc.



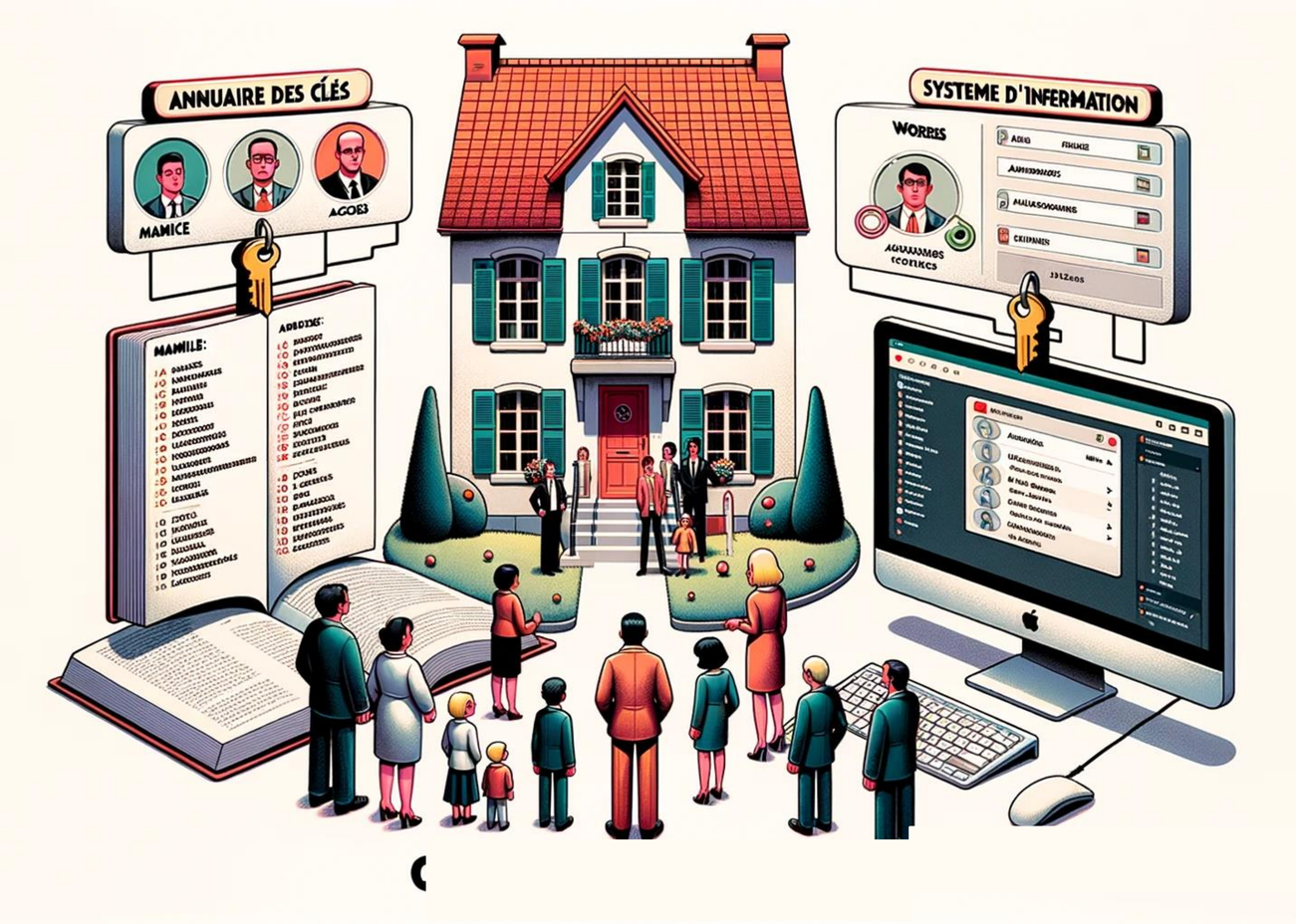
Clé physique

Voie publique

Internet

Mots de passe

Analogie entre Maison et SI – Annuaire



Active Directory

- **Référentiel central** qui stocke tous les objets d'une entreprise et leurs attributs respectifs (utilisateurs, serveurs, domaines, stratégies de sécurité, …).
- Permet aux utilisateurs de trouver et d'accéder aux ressources connues de l'annuaire en fournissant des **mécanismes d'identification, d'authentification et d'autorisation**.
- Principes de « **moindre privilège** », de modèle de **gestion des accès privilégiés** et de **cloisonnement** du SI (Tier).
- Différents services :
  - ✓ ADDS - Active Directory Domain Services
  - ✓ ADCS - Active Directory Certificate Services
  - ✓ ADFS - Active Directory Federation Services
  - ✓ ADRMS - Active Directory Rights Management Services
  - ✓ ADLDS - Active Directory Lightweight Directory Services

Active Directory – Fonctionnement

Source : ANSSI

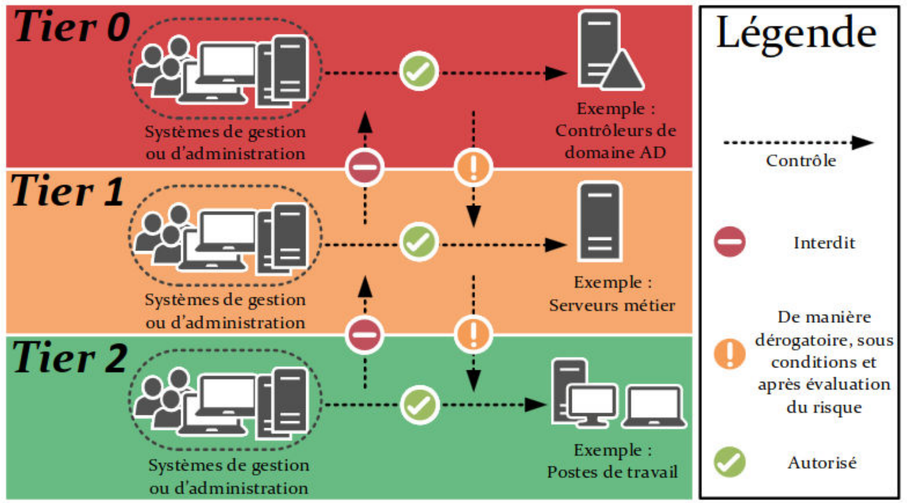
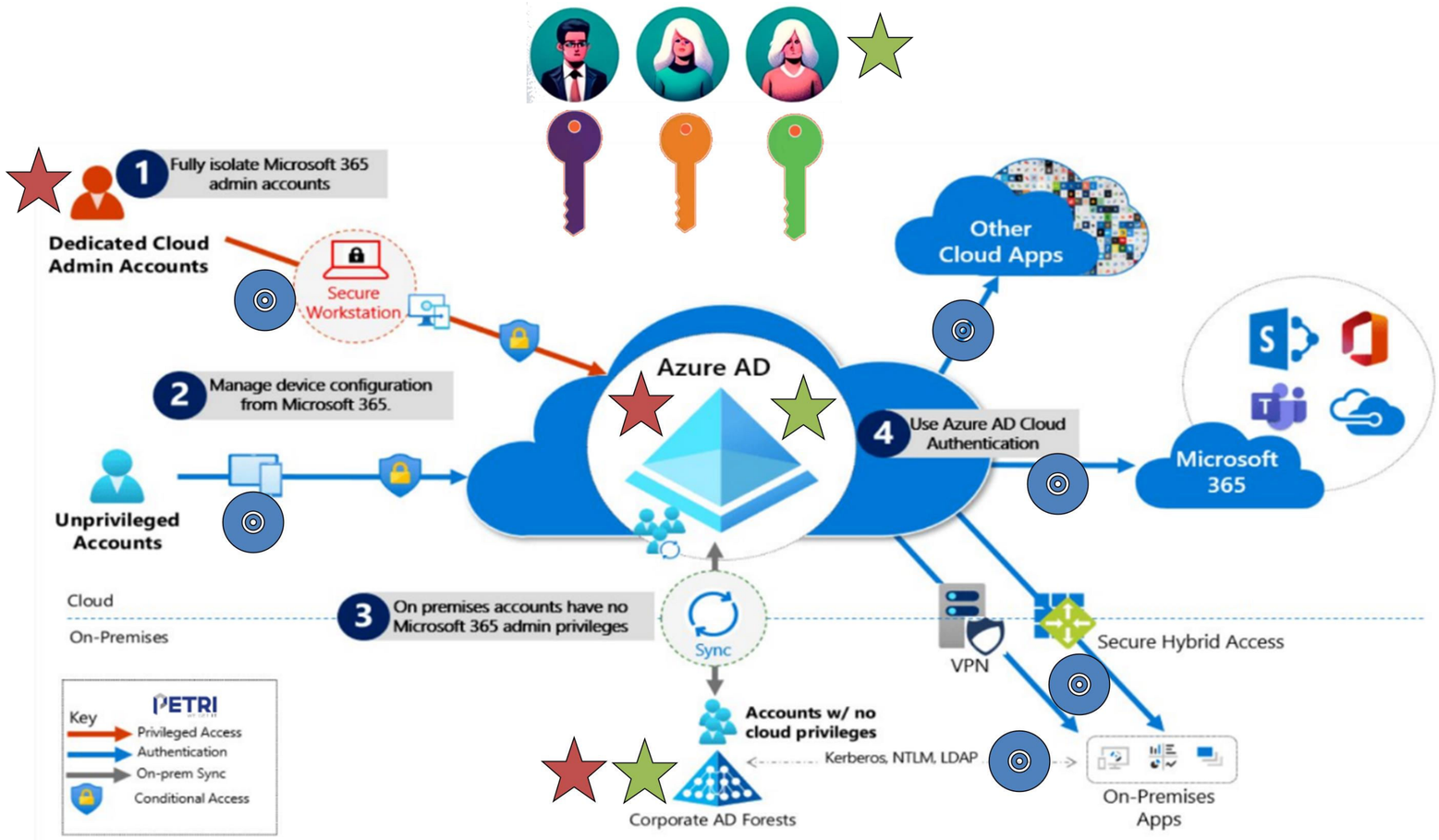
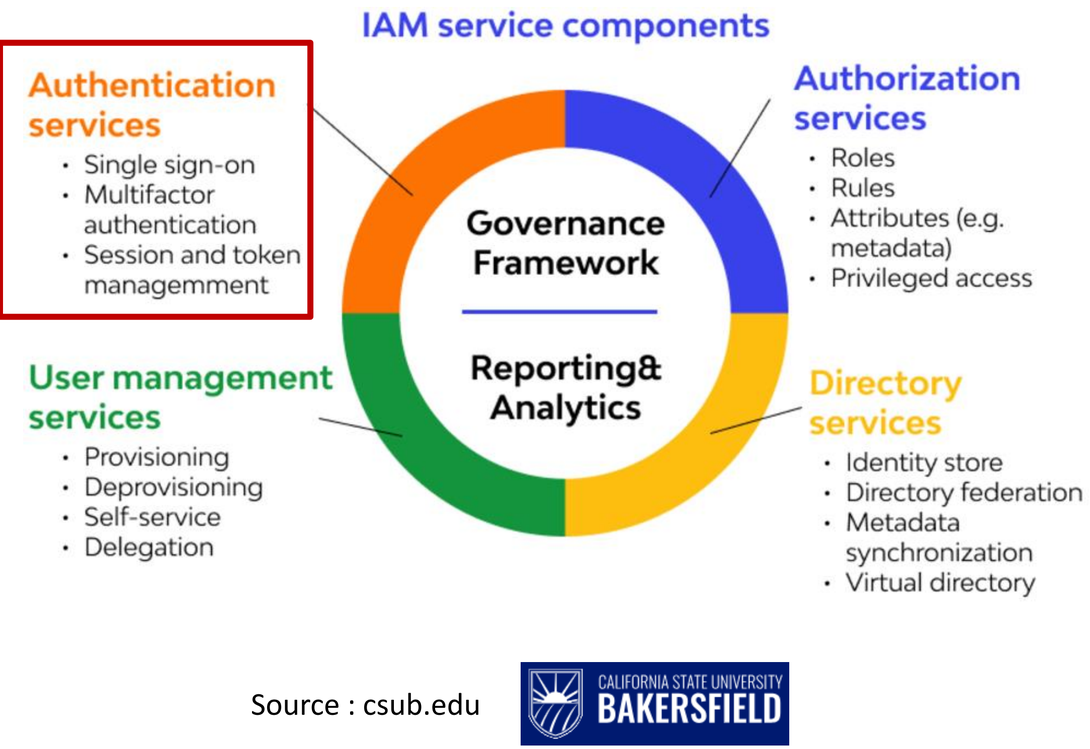


FIGURE 2 – Illustration du principe de cloisonnement des *Tiers*.

- Ressources
- Comptes utilisateurs
- Comptes Administrateurs



Gestion des identités et des accès



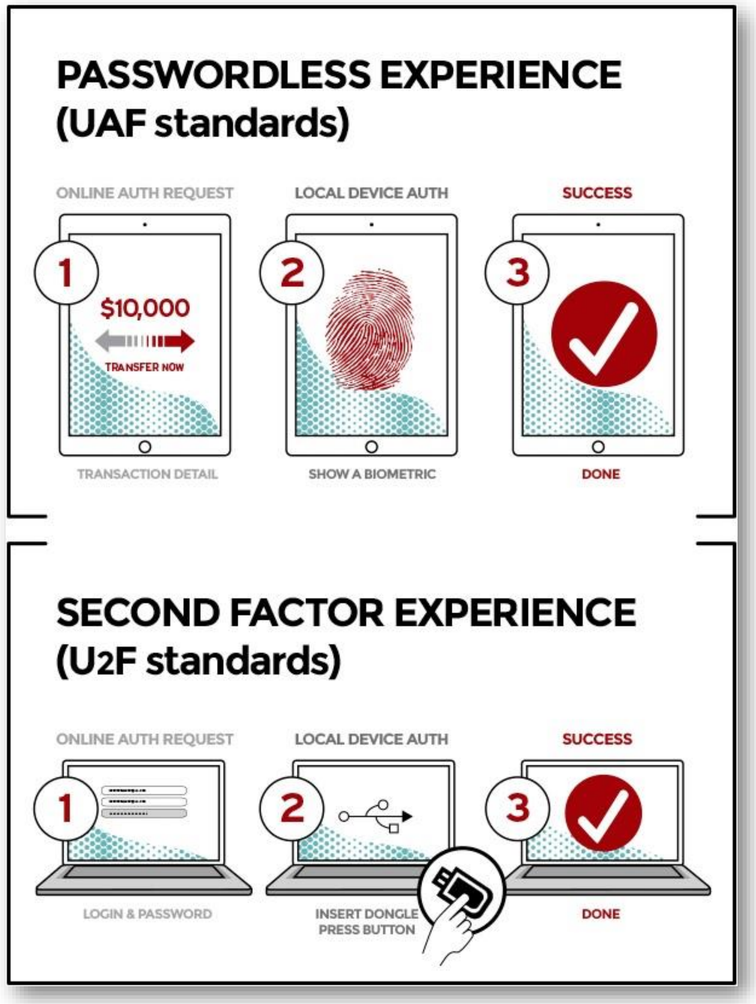
Source : csub.edu

IAM

Selon Gartner l'IAM (Identity and Access Management) peut se résumer de la manière suivante :

- *Identity and access management (IAM) is the* ***discipline that enables the right individuals to access the right resources at the right times for the right reasons****.*
- ***IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments****, and to meet increasingly rigorous compliance requirements. IAM is a crucial undertaking for any enterprise. It is increasingly business-aligned, and* ***it requires business skills, not just technical expertise.***
- *Enterprises that develop mature IAM capabilities can* ***reduce their identity management costs*** *and, more importantly, become significantly* ***more agile in supporting new business initiatives.***

Authentification (1/3)



Source : https://fidoalliance.org

2FA/MFA

- L'authentification multifacteur (MFA) est un **contrôle de sécurité** qui **oblige les utilisateurs à vérifier leur identité en fournissant plusieurs éléments de preuve** avant d'accéder à un appareil ou à une application.
- Pour l'utilisateur, il existe 3 manières de prouver qu'il est bien celui qu'il prétend être :
  - ✓ **Connaissance (ce que je sais)** : mot de passe, code PIN, …
  - ✓ **Possession (ce que je possède)** : smartphone, clé de sécurité (YubiKey), …
  - ✓ **Inhérence (ce que je suis)** : empreinte digitale, scan de la rétine, ...
- **La différence entre MFA et 2FA est simple**.
  - ✓ L'authentification à deux facteurs (2FA) utilise toujours deux de ces facteurs pour vérifier l'identité de l'utilisateur.
  - ✓ L'authentification multi-facteur (MFA) peut impliquer deux des facteurs ou les trois. "Multifacteur" signifie simplement un nombre de facteurs supérieur à un.
- L'Alliance **« Fast Identity Online » (FIDO)** est un consortium de grandes entreprises technologiques, d'agences gouvernementales, de fournisseurs de services, d'institutions financières, de processeurs de paiement et d'autres industries qui a été lancé en 2013 pour **éliminer l'utilisation de mots de passe sur les sites web, les applications et autres dispositifs.**

Authentification (2/3)

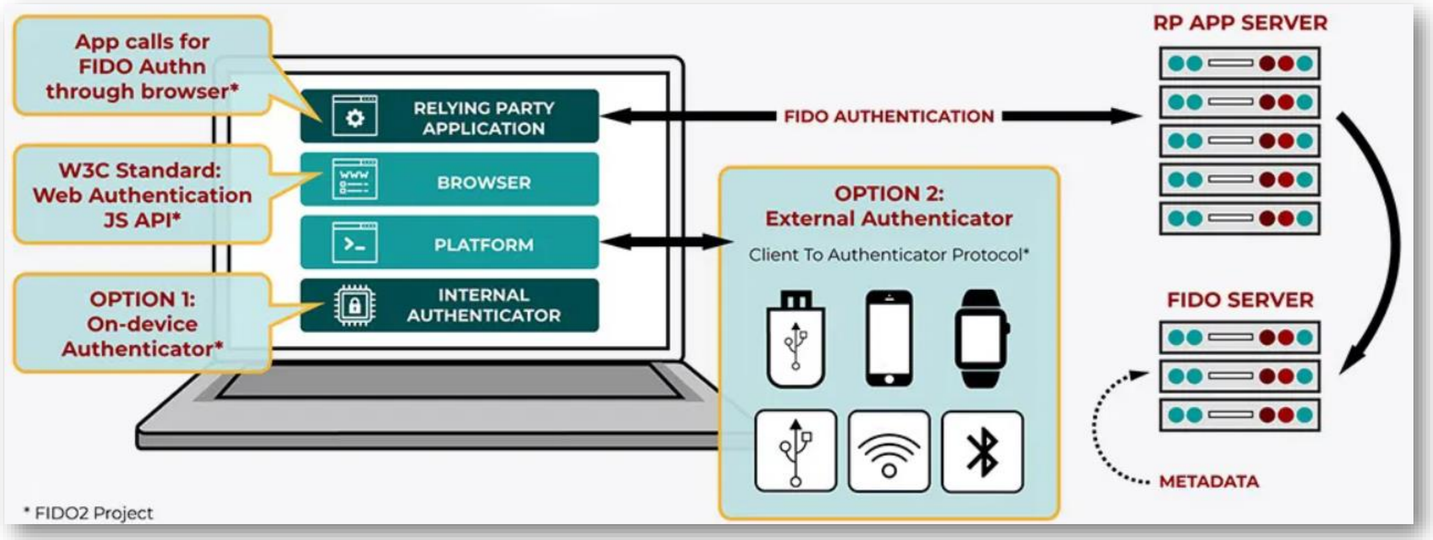
Authentification « forte »

- **L'authentification mutificateur ne garantie pas qu'une authentification soit « forte ».**
- Les facteurs, pris indépendamment ou ensemble, ne sont pas forcément considérés comme étant forts (par exemple, un mot de passe associé à un code temporaire reçu par SMS).
- **Une authentification forte** (reposant généralement sur un facteur unique) est une authentification qui s'appuie sur un **mécanisme cryptographique** dont les paramètres et la sécurité sont jugés robustes (l'élément secret est alors généralement une clé cryptographique).
- Le client prouve son identité au vérifieur en démontrant indirectement la possession d'une clé cryptographique qui doit rester secrète.
- Exemples **d'authentification forte reposant sur un facteur de possession** :
  - ✓ Authentification par certificat (stocké dans des cartes à puce) ;
  - ✓ Protocoles FIDO2 et FIDO U2F ;
  - ✓ Protocoles d'OTP : HOTP (HMAC-based OTP), TOTP (Timebased OTP) ou OCRA (OATH Challenge-Response Algorithm).
- Exemples **d'authentification forte reposant sur un facteur de connaissance** :
  - ✓ Protocole Kerberos ;
  - ✓ Protocoles de type PAKE (Password-Authenticated Key Agreement) comme SPAKE2.

Authentification (3/3)

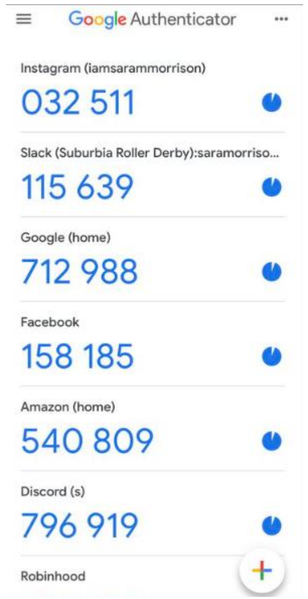
FIDO2

- Après FIDO Universal Second Factor (FIDO U2F) et FIDO Universal Authentication Framework (FIDO UAF), **FIDO2 devient la dernière spécification de la FIDO Alliance.**
- FIDO2 est composé de **CTAP (Client to authenticator Protocol)** et **WebAuthn (standard W3C).**
- **Cela permet aux utilisateurs de s'authentifier via des moyens d'authentification cryptographiques** (codes PIN, biométrie) **ou des moyens externes** (clé type Yubikey, téléphones, PCs).



Src : https://fidoalliance.org

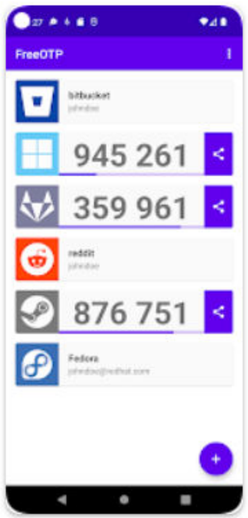
MFA – Méthodes (1/2)



Les méthodes

- **SMS :**
  - ✓ **Avantages** : facile à utiliser et à comprendre + aucun matériel supplémentaire n'est nécessaire.
  - ✓ **Inconvénients** : vulnérable aux attaques de détournement de SMS (SIM swapping) et AITM + non fiable si le réseau de téléphonie mobile n'est pas disponible.
- **Application d'authentification (Google/Microsoft Authenticator, FreeOTP, etc.) :**
  - ✓ **Avantages** : plus sécurisé que les SMS + fonctionne même sans connexion de données mobiles.
  - ✓ **Inconvénients** : nécessite un smartphone + peut être un défi pour les utilisateurs moins technophiles.
- **Token matériel (Clé U2F, RSA SecurID, etc.) :**
  - ✓ **Avantages** : très sécurisé, car le token est physique et unique + aucune dépendance au réseau ou au service de téléphonie.
  - ✓ **Inconvénients** : coût supplémentaire pour l'achat de tokens + peut être perdu ou volé.
- **Cartes à puce et cartes d'accès :**
  - ✓ **Avantages** : combinaison d'une possession physique et d'une connaissance (code PIN) + peut être intégré avec des badges d'identification existants.
  - ✓ **Inconvénients** : nécessite un lecteur de carte + coût de mise en place initial plus élevé.

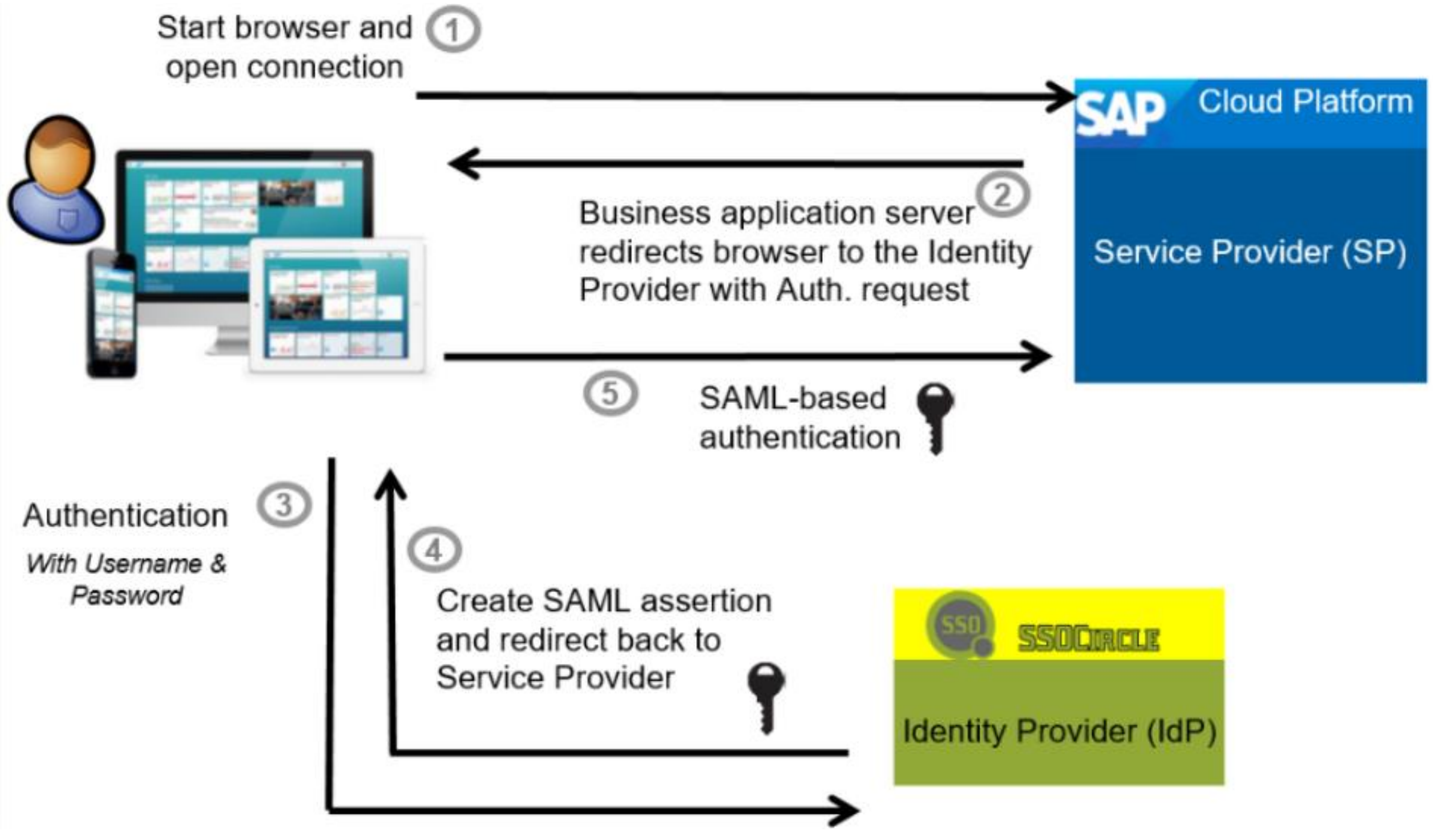
MFA – Méthodes (2/2)



Les méthodes (suite)

- **Biométrie (empreintes digitales, reconnaissance faciale, iris) :**
  - ✓ **Avantages** : très difficile à falsifier en fonction de l'élément de contrôle + pratique et rapide pour l'utilisateur.
  - ✓ **Inconvénients** : coût élevé de mise en œuvre + confidentialité et de stockage des données biométriques
- **Certificat numérique et clé USB :**
  - ✓ **Avantages** : sécurité élevée grâce à la cryptographie + peut être utilisé sur différents appareils.
  - ✓ **Inconvénients** : nécessite une gestion et une infrastructure de clés + peut être complexe à configurer et à maintenir.
- **Code jetable ou passcode (OTP - one time password) :**
  - ✓ **Avantages** : généré dynamiquement, donc très sécurisé + peut être reçu par différentes méthodes (SMS, e-mail, app).
  - ✓ **Inconvénients** : dépendant de la méthode de livraison (réseau, appareil) + vulnérable aux attaques de type AITM (peut être sujet à des attaques de phishing).

Single Sign-On (1/2)



Src : https://sap.com

Concepts

- **Méthode permettant à un utilisateur d'accéder à plusieurs applications informatiques (ou sites web sécurisés) en ne procédant qu'à une seule authentification.**
- Dans un service SSO web de base, un module agent sur le serveur d'application récupère les informations d'authentification spécifiques d'un utilisateur individuel à partir d'un serveur de politiques SSO dédié, tout en authentifiant l'utilisateur par rapport à un référentiel utilisateur tel qu'un répertoire LDAP (Lightweight Directory Access Protocol)**.**
- **Le service authentifie l'utilisateur final pour toutes les applications auxquelles l'utilisateur a reçu des droits et élimine les demandes de mot de passe futures** pour des applications individuelles au cours de la même session.

Single Sign-On (2/2)

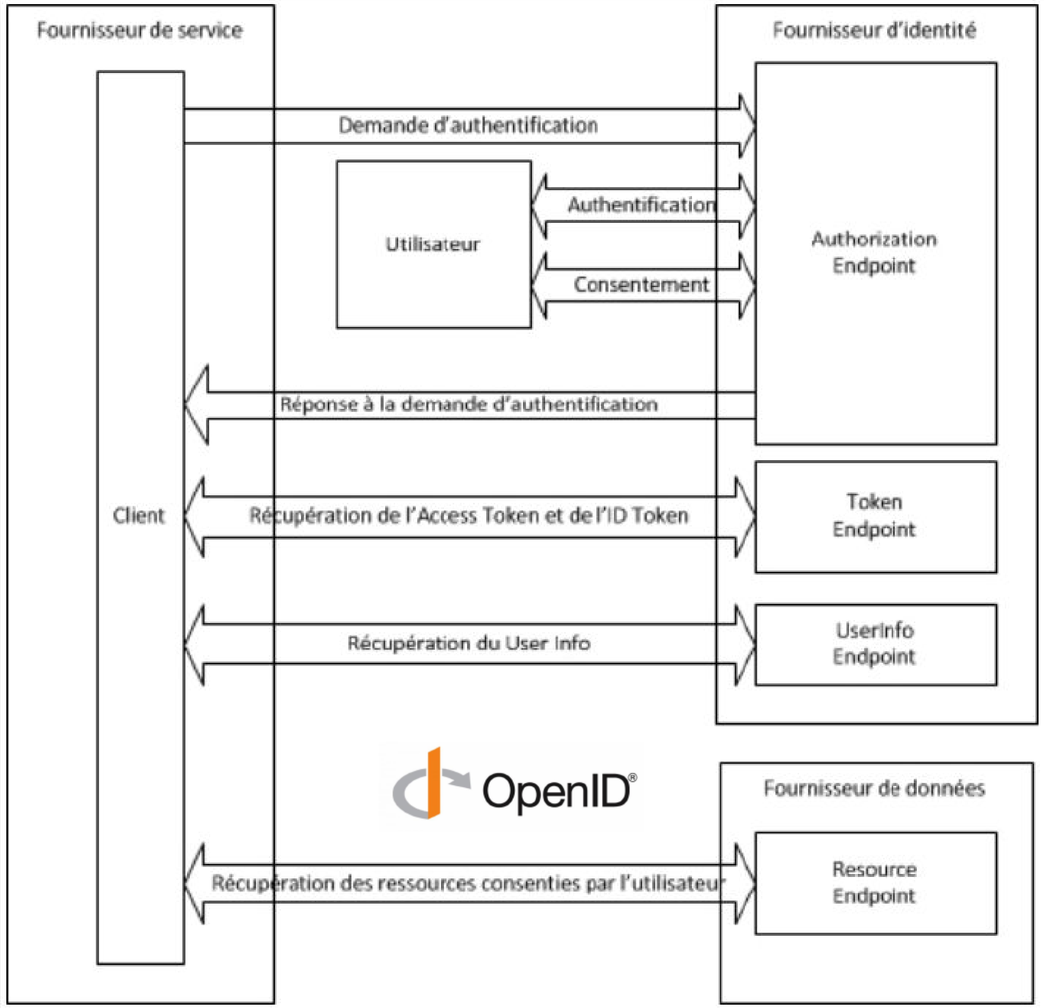
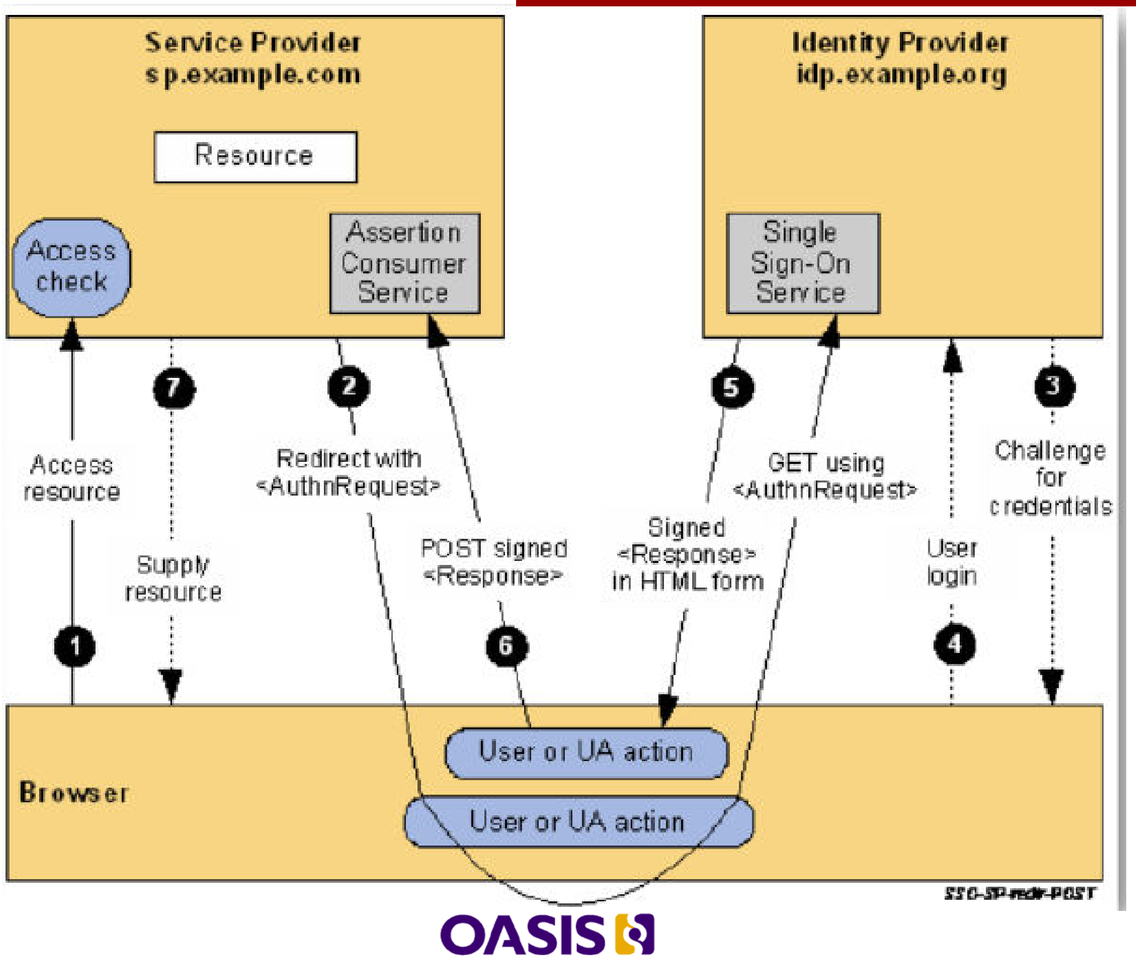


FIGURE 2.1 – Schéma simplifié des échanges entre les différents acteurs

Src : ANSSI

OpenID Connect / SAML



OASIS

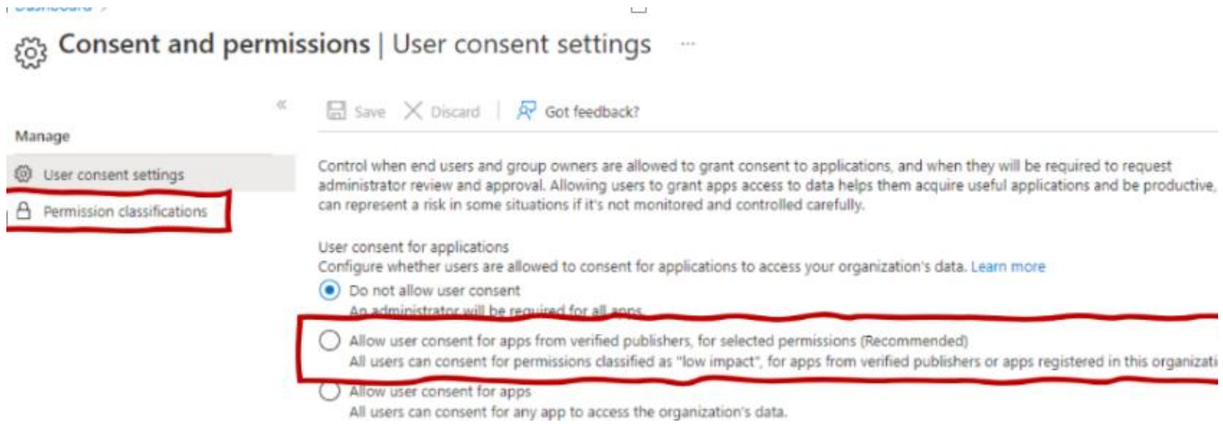
2.

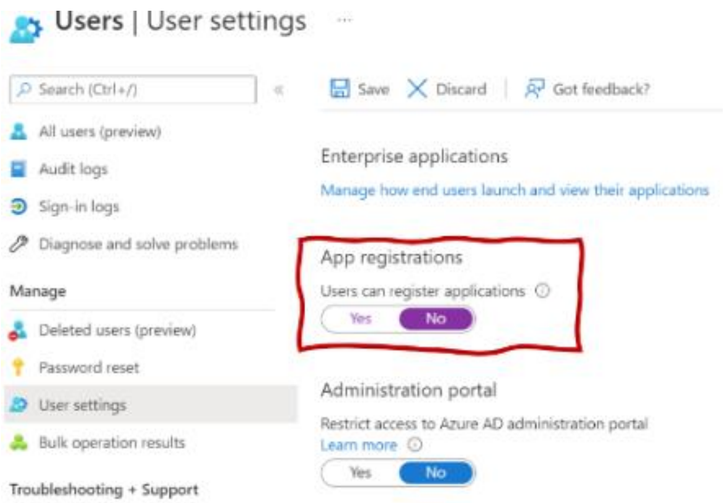
Risques et attaques

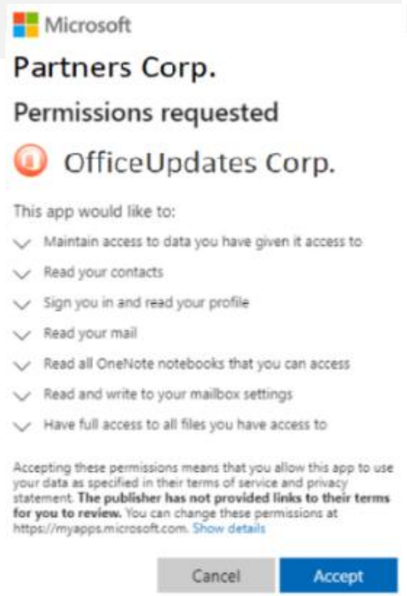
Scénarios d’attaque (1/3)

Abus de consentement – Accès à des ressources internes

- Le consentement est le processus par lequel un utilisateur accorde à une application l'autorisation d'accéder à des ressources protégées en son nom.
- Déroulement :
  1. L'attaquant crée une application multi-tenant dans son propre tenant ;
  2. Il configure l'application pour qu'elle se voit accorder un accès délégué ;
  3. Il trompe l'utilisateur pour que ce dernier se connecte à l'application (hameçonnage) ;
  4. Si l'utilisateur accepte, l'attaquant peut alors accéder à ses ressources.



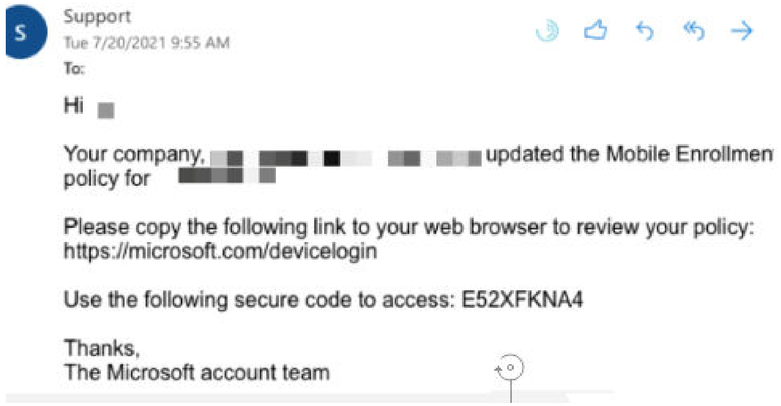


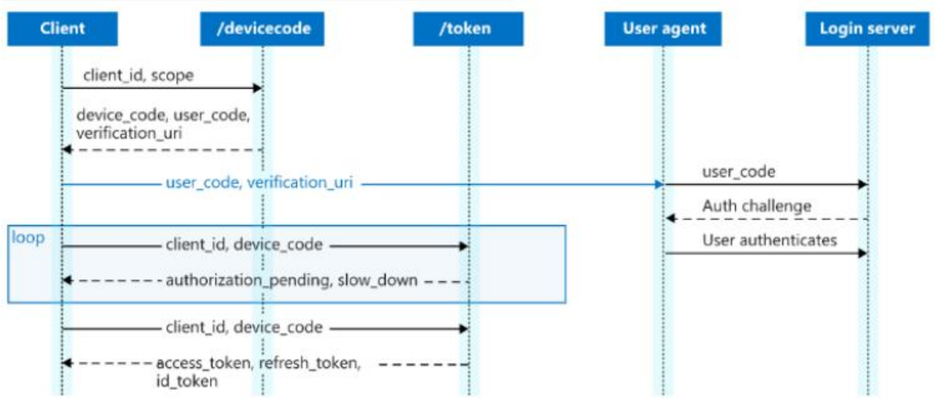


Scénarios d’attaque (2/3)

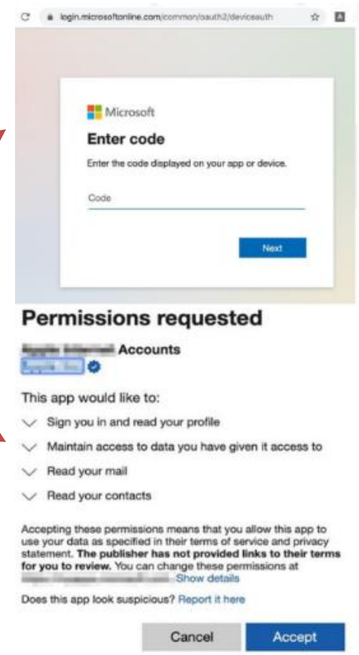
Abus de consentement – Flux d’autorisation d’appareil (Oauth Device Code Flow)

- *“The Microsoft identity platform supports the device authorization grant, which allows users to sign in to input-constrained devices such as a smart TV, IoT device, or a printer.*
- *To enable this flow, the device has the user visit a webpage in a browser on another device to sign in. Once the user signs in, the device is able to get access tokens and refresh tokens as needed.”*





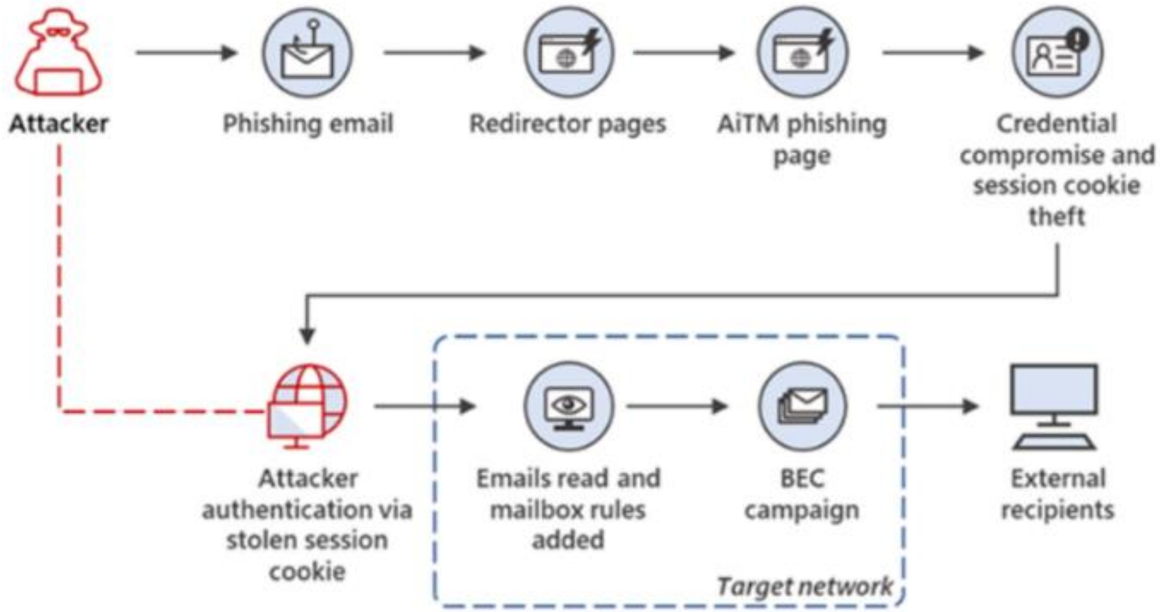

```
$ python3 pis.py -e user@example.com -p '<victim_phone>' \
                 -P'<from_phone>' -s '<twilio_sid>' \
                 -t '<twilio_token>' -c '<client_id>' --get-data


[INFO] [user@example.com] Code successfully retrieved.
[INFO] [user@example.com] Message: To sign in, use a web browser to open
the page https://microsoft.com/devicelogin and enter the code E2XZV7VLV to
authenticate.
[INFO] [user@example.com] Text message successfully sent.
[INFO] [user@example.com] Polling for user authentication...
[INFO] [user@example.com] Polling for user authentication...
[INFO] [user@example.com] Polling for user authentication...
[INFO] [user@example.com] Polling for user authentication...
[INFO] [user@example.com] Polling for user authentication...
[INFO] [user@example.com] Token info saved to user@example.com.tokeninfo.json
[INFO] [user@example.com] Azure Graph API results for 'profile' saved to
user@example.com.profile.json
```

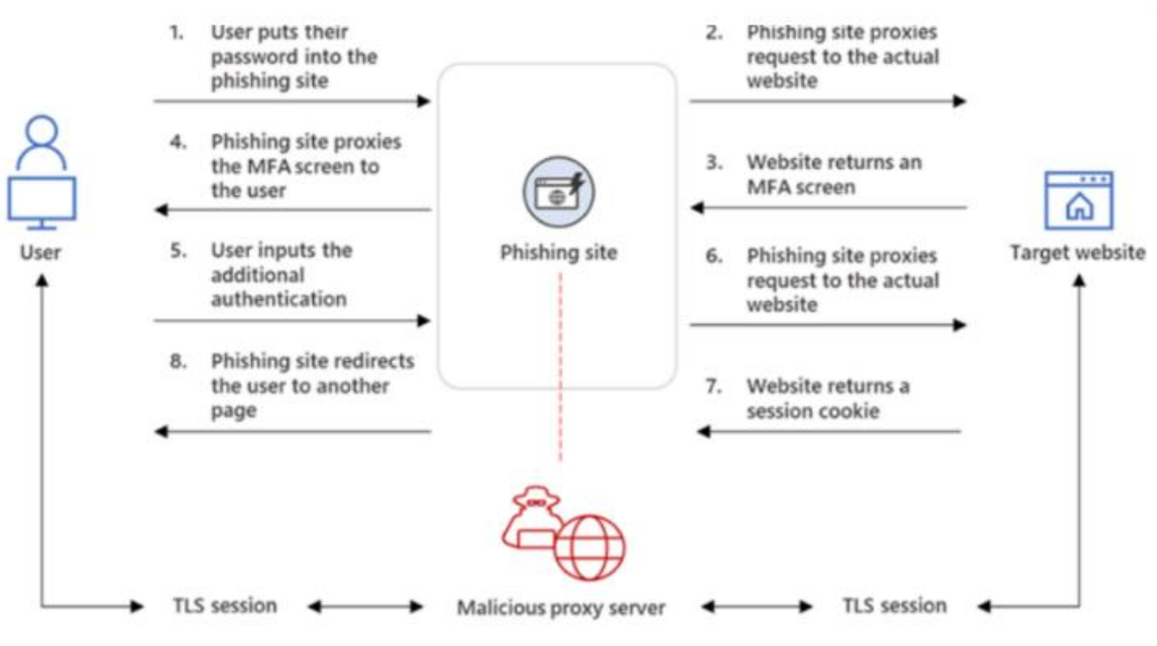


Scénarios d’attaque (3/3)

Adversary-in-the-middle (AiTM)

- **Principe** : l’attaquant déploie un serveur proxy entre un utilisateur cible et le site web auquel l'utilisateur souhaite accéder.
- Une telle configuration permet à l'attaquant **de voler et d'intercepter le mot de passe de la cible** et le cookie de session qui prouve que sa session en cours est authentifiée avec le site Web.

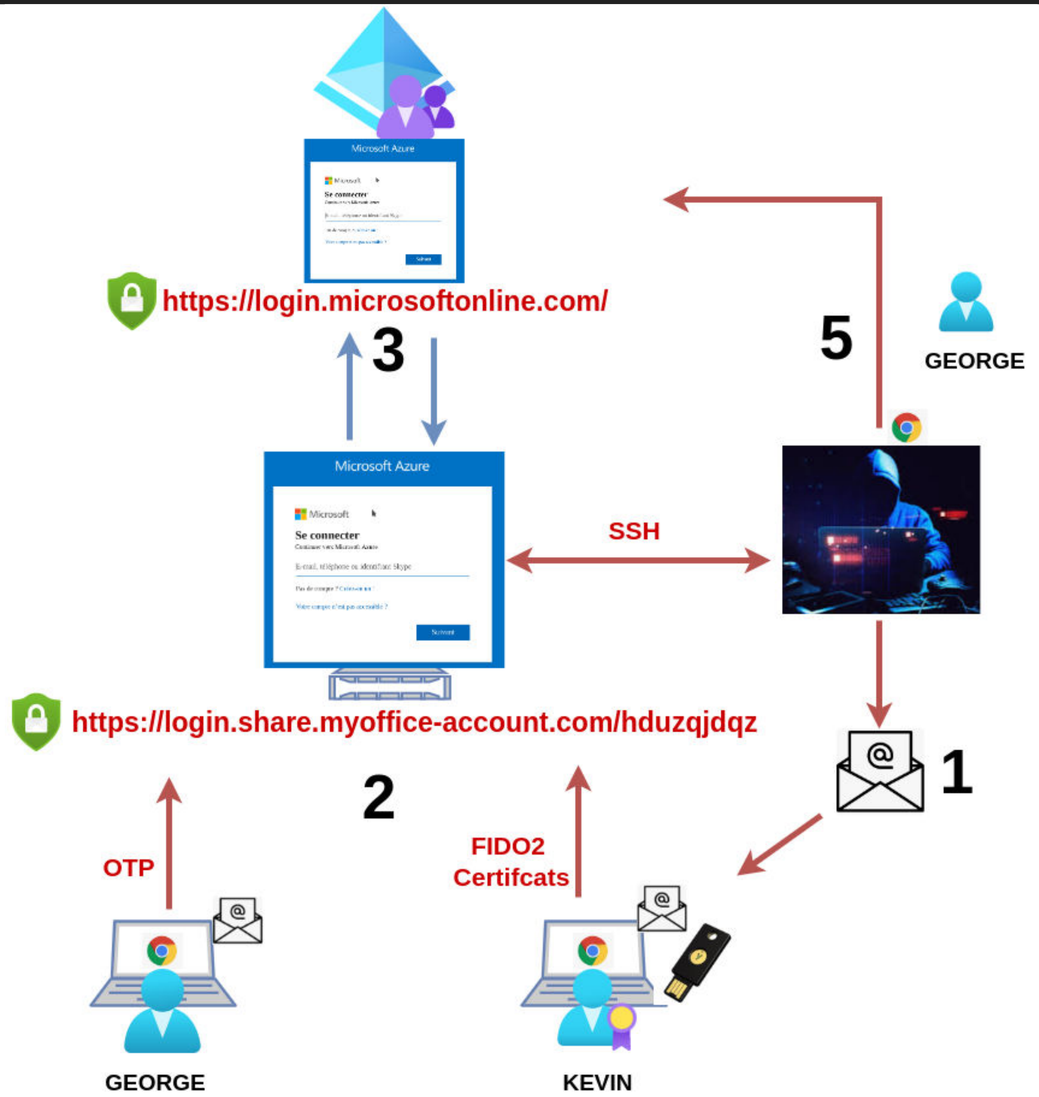




3.

Démonstration

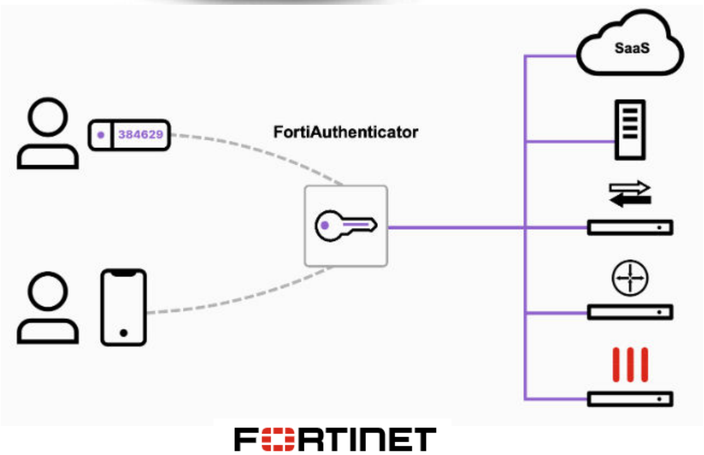
Démonstration – Adversary-in-the-middle (AiTM)



4.

Recommandations

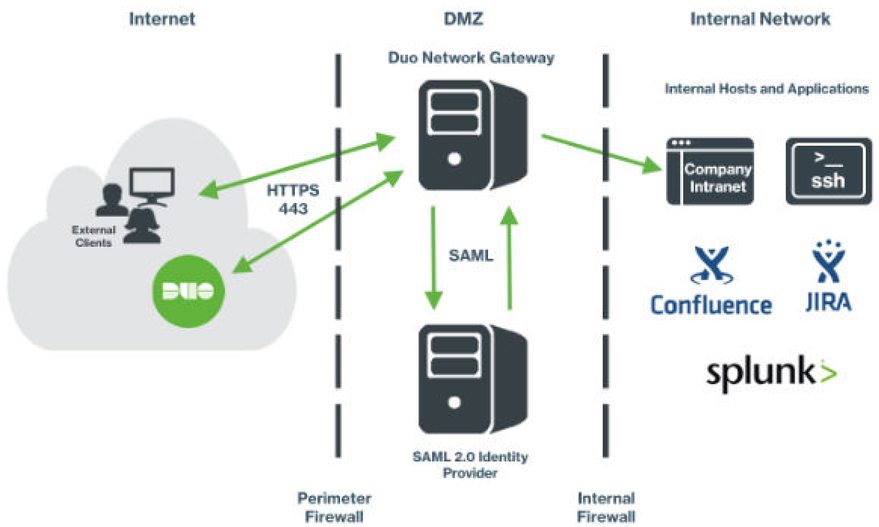
Implémentation du MFA

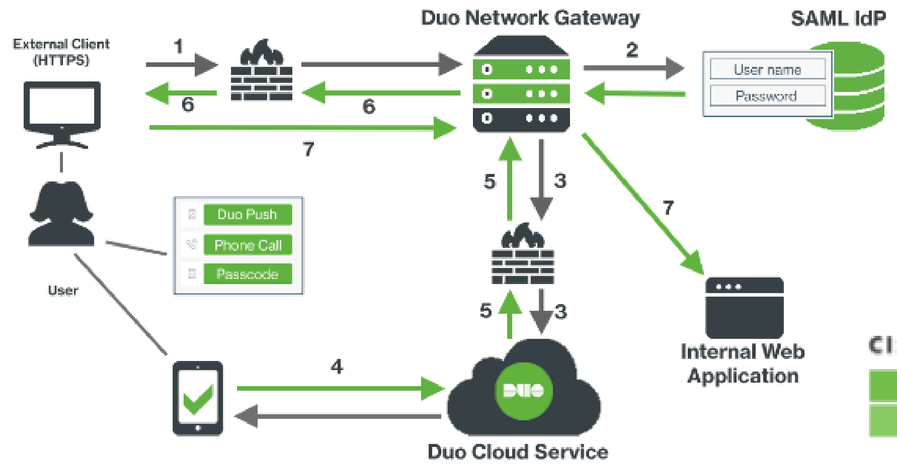


Méthodologie

1. **Risques** : évaluer les menaces potentielles et les vulnérabilités.
2. **Exigences de sécurité** : identifier quelles données nécessitent une protection renforcée et quelles sont les réglementations à respecter.
3. **Utilisateurs et ressources** : déterminer quels utilisateurs auront besoin du MFA et pour quelles applications, services ou données.
4. **Infrastructure actuelle** : examiner les systèmes d'authentification existants et leur compatibilité avec les solutions MFA.
5. **Ressources et budget** : estimer les coûts de mise en œuvre, y compris le matériel, les logiciels, la formation et l'assistance technique.
6. **Planification de la mise en œuvre** : définir un calendrier pour le déploiement et la formation des utilisateurs.
7. **Formation et sensibilisation** : former les utilisateurs finaux et les sensibiliser à l'importance du MFA.
8. **Surveillance et révision** : surveiller le fonctionnement du système MFA et effectuer des révisions régulières pour assurer son efficacité.

POC MFA (1/2)





Les avantages du POC

Réaliser un POC de différentes solutions présente plusieurs avantages :

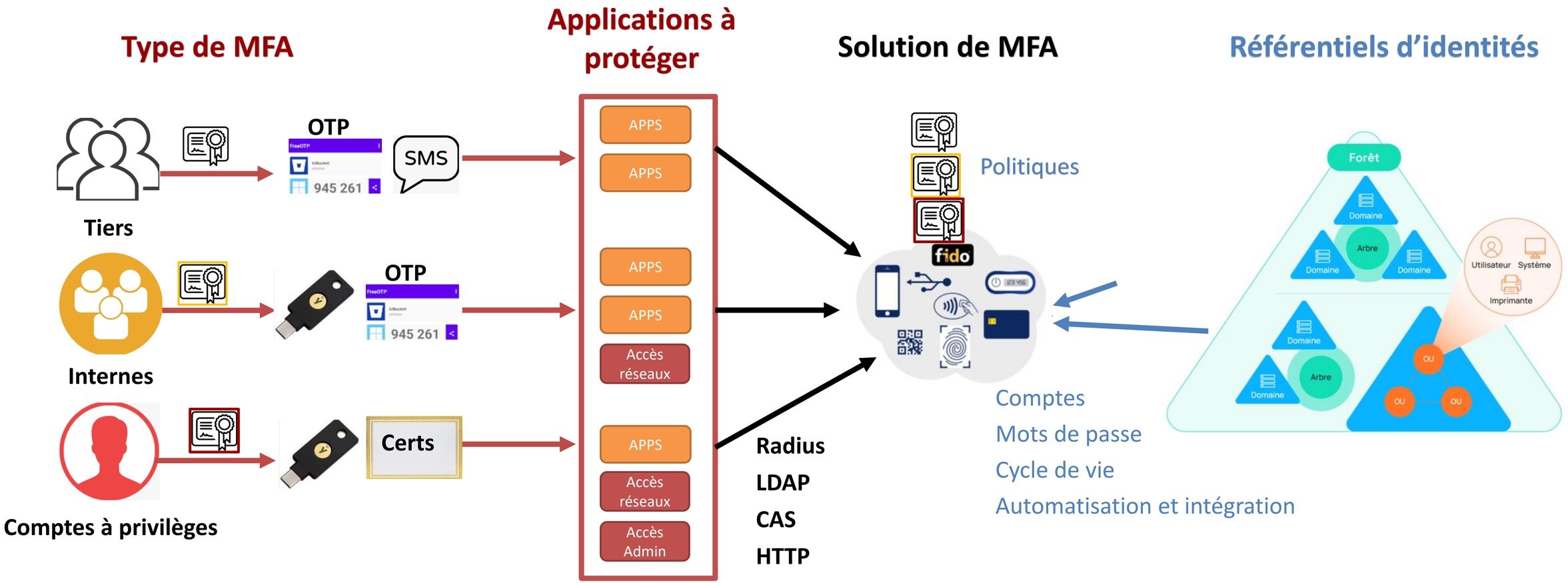
1. **Comparaison directe** : performances, fonctionnalités, usabilité, coûts, etc. Cela permet d'avoir une vision globale et détaillée des différences entre les solutions et les compétences des prestataires.
2. **Evaluation de la diversité des fonctionnalités** : déterminer celles qui répondent au mieux au contexte et contraintes d'utilisation ainsi qu'aux besoins.
3. **Réduction des risques** : identifier les points forts et les faiblesses de chaque solution.
4. **Flexibilité dans le choix final** : sélectionner la solution qui offre le meilleur équilibre entre performances, coûts (d'intégration, de MCO/MCS) et adaptation à l'existant.

POC MFA (2/2)

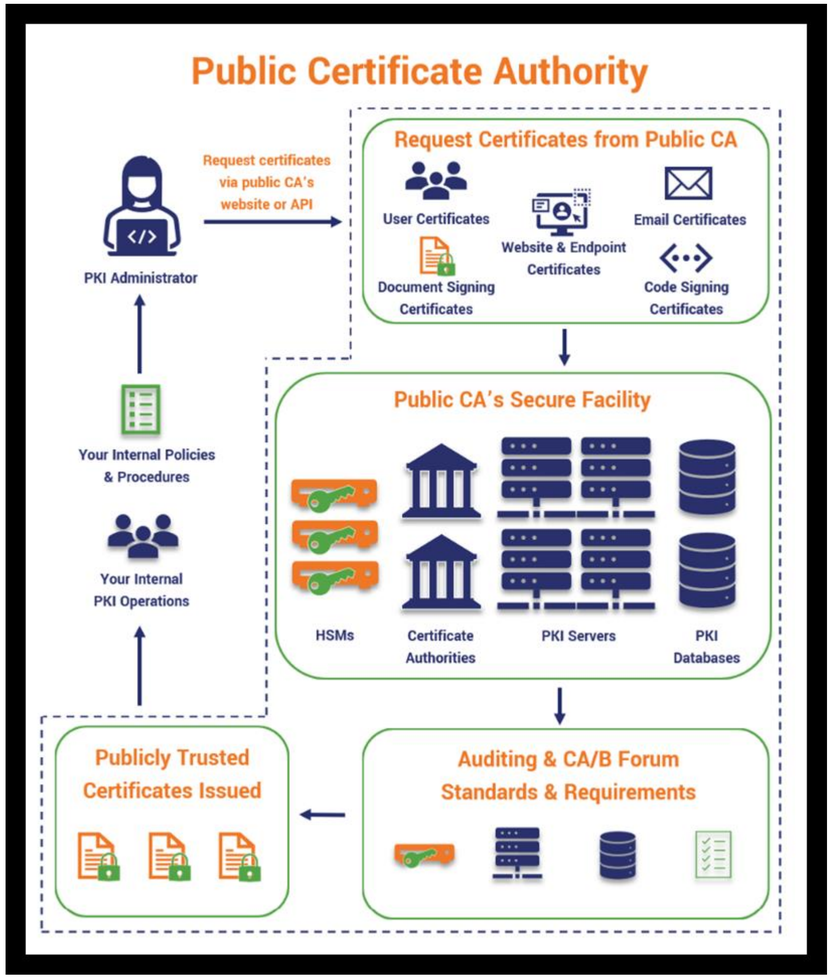
Les étapes du POC

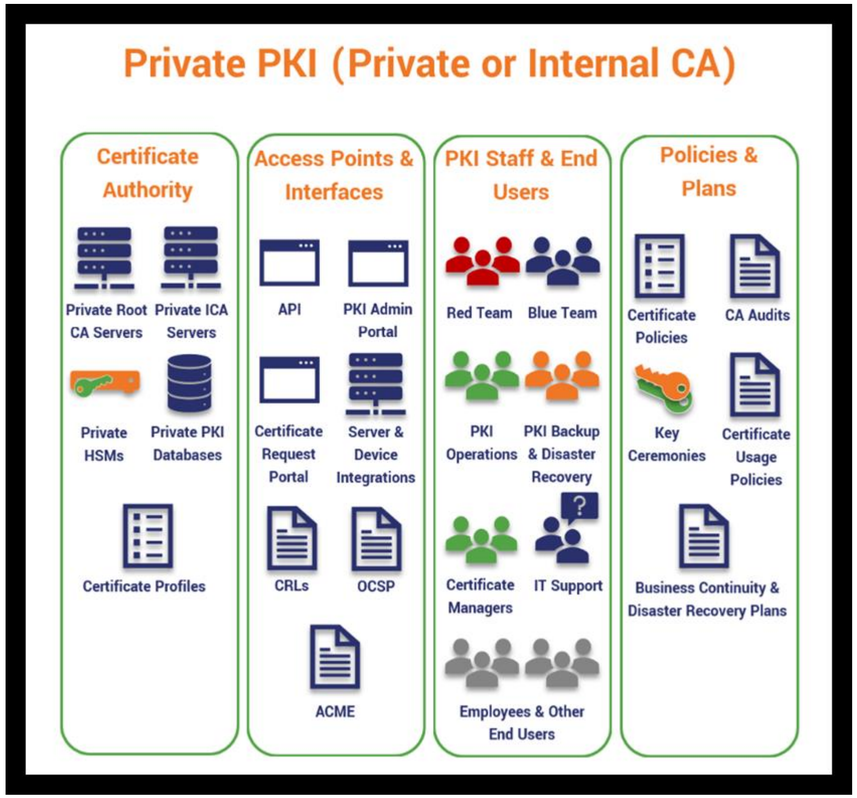
1. **Définition des objectifs du POC** : type de MFA, type de sujets, politiques, exceptions, périmètre.
2. **Sélection des prestataires MFA** : évaluer les capacités et compétences des intégrateurs.
3. **Configuration de l'environnement de test** : déployer un environnement de test simulant les applications concernées et les différents types d'authentification.
4. **Intégration des solutions MFA** : intégrer chaque solution dans l'environnement de test, en tenant compte des protocoles d'authentification utilisés (LDAP, CAS, SAML, OpenID, local, Radius).
5. **Définition des scénarios de test** : définir des scénarios de test pertinents dans le contexte pour évaluer les fonctionnalités et les performances de chaque solution, en tenant compte des différents types d'authentification et des diverses interactions utilisateur.
6. **Collecte des données et évaluation des résultats** : formaliser une matrice d'évaluation des solutions basée sur les scénarios de test et les objectifs du POC.
7. **Rapport de synthèse et recommandations** : prise en compte du retour d'expérience des différentes parties prenantes et définition de la cible (solution, intégrateurs, budgets, charges, …).
8. **Implémentation pilote** : mise en œuvre de la première phase d'intégration de la solution retenue sur l'environnement de production.

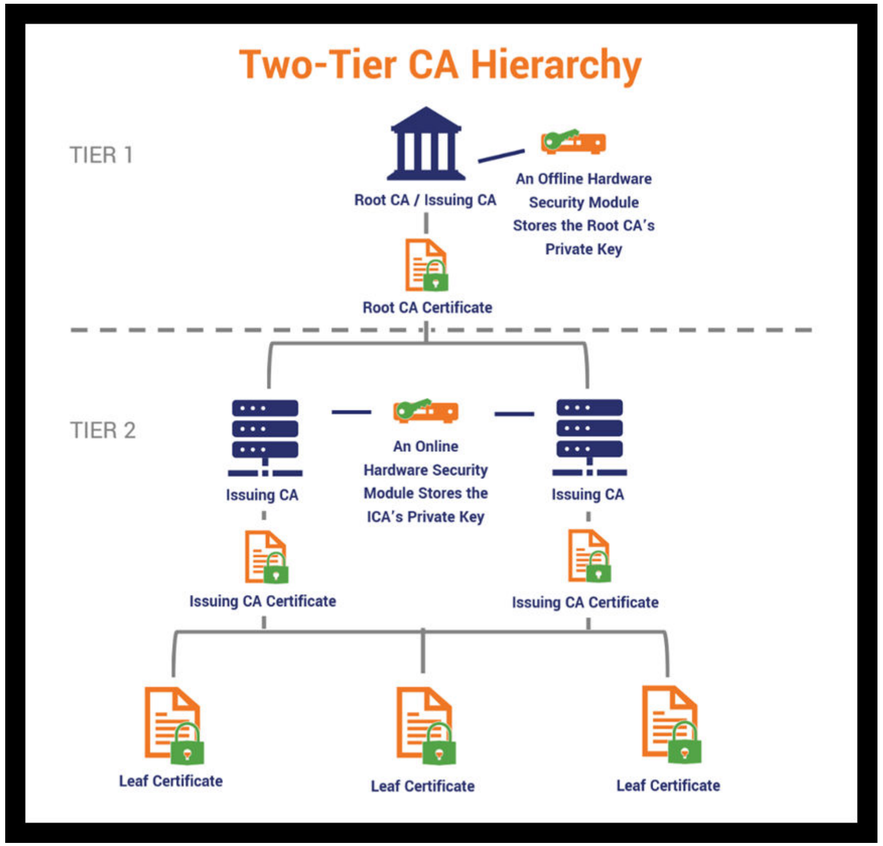
Intégration



Architecture d’une PKI

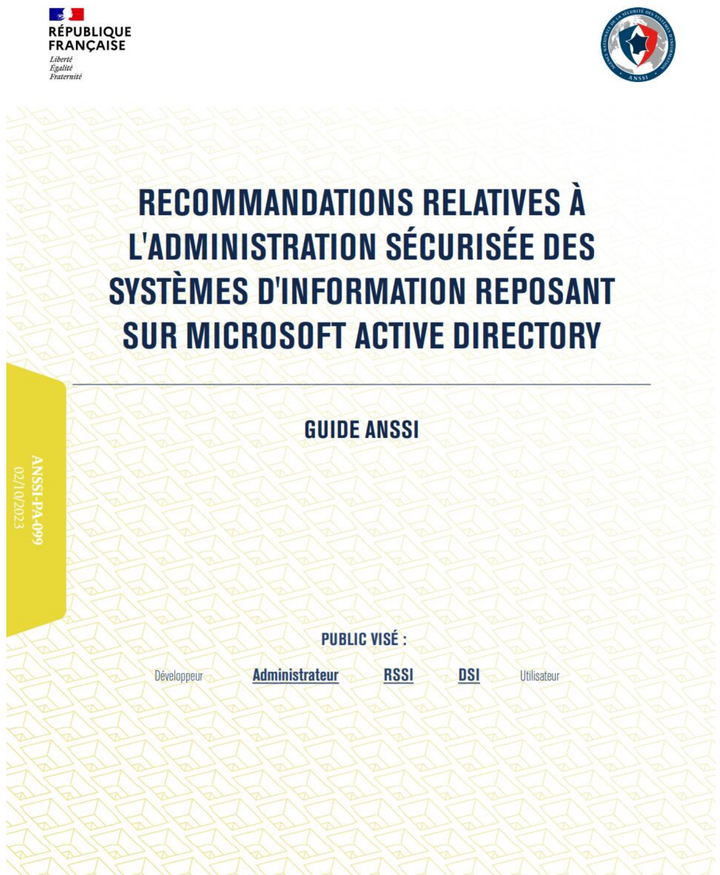






Source : https://www.thesslstore.com

Autres recommandations



Durcissement AD

- **Point de situation : Quel est mon niveau de sécurité ? Que dois je faire ?**
  - ✓ Audit de l'existant (TIE, TII, test du stagiaire)
  - ✓ Audit d'architecture technique et des configurations
- **Les actions : Comment améliorer mon niveau de sécurité ?**
  - ✓ Cible d'architecture technique de défense en profondeur
  - ✓ Durcissement des configurations
  - ✓ Journalisation
  - ✓ Supervision de sécurité
  - ✓ Agent de protection (EDR/HIDS/Defender for identity)
  - ✓ Supervision des flux réseaux (NIDPS).
  - ✓ Gestions des secrets et des comptes à privilèges
  - ✓ Gestions des correctifs
  - ✓ MFA / PKI

5.

Questions

CONTACTEZ-NOUS

ELYSIUM SECURITY

29 bis chemin de Grave

69450 Saint-Cyr-au-Mont-d'Or

+33 (0)4 28 29 63 37

commerce@elysium-security.com

https://elysium-security.com