ENASTIC
Ecole Nationale Supérieure des TIC

Logo-structure-d'accueil

**Projet de fin d'etudes**

En vue de l'obtention du Diplome de Licence en Informatique

**Option :**Cybersécurité

---

THÈME :

# La Gestion des Identités et Accès(IAM)

---


**Realisé et Présenté par :**

Hamid sougour ardane


**Jury :**

**M.** xxxxxxxxxxxxx(President)

**M.** yyyyyyyyyyy(Rapporteur)

**Sous la Direction de :**

M.xxxxxxxxxxxx(Encadrant)

M.xxxxxxxx(Maitre de Stage)

année universitaire :2021-2022

# Avant-propos

# Dédicace

Ce mémoire est dédié :
A mes très chers parents, pour leurs soutien et encouragement durant toutes mes années d'études

# Remerciement

# RÉSUMÉ

# ABSTRACT

# Table des matières

# Table des figures

# Liste des tableaux

# LISTE DES ACRONYMES

**IAM :** Identity and Access Management

**SGIA :** système de gestion des identités et accès

**GIA :** gestion des identités et des accès

**IoT :** l'Internet des objets

**IA :** L'intelligence artificielle

**SSI :** sécurité du système d'information

**SI :** système d'information

**ISP :** Internet Service Provider

**SSO :** Single Sign-on

**SGIA :**

**SGIA :**

**SGIA :**

**SGIA :**

**SGIA :**

# Introduction Générale

# Première partie

# la structure d'accueil

# Chapitre 1

# Présentation de la structure d'accueil

## Introduction

## 1.1 Présentation de l'organisme d'accueil.

Dans cette partie,nous allons d'abord décrire la structure qui nous a accueil pour ce modeste travail,ses missions et son structure de fonctionnement et sa création.Ensuite nous allons définir le cadre d notre projet et proposer une solution open source,le cas notre système de gestion des identités et des accès vue son nécessite au sein de l'organisme d'accueil

### 1.1.1 Création

L'Agence Nationale de Sécurité Informatique et de Certification Électronique est une institution créée par la Loi **No 006/PR/2015 du 10 février 2015** . Cet organisme a été créé dans un cadre juridique sur la cybercriminalité et la protection de données à caractère personnel permettant de régir le secteur de la cybersécurité au niveau national suite à la convention de l'UA relative à la cybersécurité et à la PDP de 2014.Au début de sa création, elle a été placée sous la tutelle de la primature. Pour des réformes institutionnelles, la primature a été supprimée et vu la Loi **No 23/PR/2019 du 26 Avril 2019** , portant ratification de l'ordonnance **No 02/PR/2019 du 1er Mars 2019** portant modification de la Loi **No 006/PR/2015 du 10 février 2015**,l'ANSICE a été placée sous la tutelle de Présidence de la République. Cette institution est un établissement public à caractère administratif, dotée de la personnalité morale et de l'autonomie financière est désormais placée sous la tutelle de la Présidence de la République. Le gouvernement a par le Décret **No 982/PR/PM/2017 du 14 Juillet 2017** défini le cadre de son organisation et fonctionnement, c'est ce qui a permis le démarrage effectif des activités de l'ANSICE en Janvier 2018. Elle a pour siège N'Djamena.

### 1.1.2 Missions

Avec l'évolution massive de la technologie de l'information et de la communication (TIC),le Tchad a une institution : L'Agence Nationale de Sécurité Informatique et de Certification Électronique par la Loi No 006/PR/2015 du 10 février 2015 pour sécuriser la cyberespace tchadienne .
Cet institution a pour mission

- Assurer la cyber-sécurité des infrastructures critiques de l'État ;
- Coordonner au niveau national la lutte contre la cybercriminalité ;
- Veiller sur la protection des données à caractères personnel des citoyens et personnes résidant au Tchad ainsi que sur les libertés dans le cyberespace ;
- Sécuriser les transactions électroniques sur l'ensemble du territoire national en veillant notamment à la bonne application de la Loi N°008/PR/2015 du 10 Février 2015 relative aux transactions électroniques

### 1.1.3 Les objectifs de l'ANSICE

- Concevoir et de mettre en œuvre les politiques de promotion de la cybersécurité et de lutte contre la cybercriminalité ;
- Protéger pour les comptes de l'État, la régulation, le contrôle et le suivi des systèmes d'information et des réseaux de communications électroniques ; de coordonner les actions en matière de cybersécurité au niveau national ;
- Veiller à la sécurité des systèmes gouvernementaux de l'information et des infrastructures essentielles de l'État ;
- Contrôler les activités de sécurité des réseaux de communications électroniques et des systèmes d'information ;
- Créer une plateforme nationale aux fins de coordonner l'assistance technique et les initiatives de formation au niveau international
- Émettre un avis consultatif sur les textes touchant au domaine de la cybersécurité et de la lutte contre la cybercriminalité ;
- Adopter un programme efficace de sensibilisation à la cybersécurité aux fins de promouvoir le partage d'information avec toutes les parties prenantes sur des questions s'y rapportant ;
- Émettre des alertes et des recommandations en matière de sécurité des réseaux de communications électroniques et de certification électronique ;

### 1.1.4 Organisation et fonctionnement

Décret **N°0848/PR/PM/2019 du 14 juillet 2019** , portant Organisation et Fonctionnement de l'Agence Nationale de Sécurité Informatique et de Certification Électronique (AN-

SICE) ; Elle est placée sous la tutelle de la Présidence de la République,Cet organisme a été créé dans un cadre juridique sur la cybercriminalité et la protection de données à caractère personnel :

- ➞ par le décret **N°1350/PR/2018** , portant organigramme de la Présidence de la République, du 06 juin 2018,
- ➞ Par la Loi **N°023/PR/2019 du 26 avril 2019** portant ratification de l'ordonnance **N°002/PR/2015** portant modification de la Loi création de l'ANSICE ;

Elle est administrée par un Conseil d'Administration composé de 11 membres, nommés par Décret **N°627/PR/PM/2018 du 30 mars 2018** ; Une Direction Générale composée de six directions techniques, nommée par Décrets **N°16/PR/PM/2018** du **10/01/2018** et **N°1392/PR/2018** du **11 juin 2018**

### 1.1.5 Présentation de la Direction d'accueil

**Service d'Exploitation et support Technique(SEST**

SEST est placé sous l'autorité d'un chef de service.Il est chargé de :

- Planifier,concevoir,déployer et optimiser les infrastructure des réseaux et système de communication de l'ANSICE ;
- Assurer la continuité et le bon fonctionnement,la sécurité,la disponibilité, et la performance de ces infrastructures ;
- Élaborer les termes de référence et les spécification techniques relatifs a ces infrastructures et aux équipements informatique l'ANSICE ;
- Effectuer une surveillance active des réseaux et systèmes déployés dans le Data-center de l'ANSICE et en assurer la sécurisation ;
- Assurer la maintenance et la sécurisation du parc informatique de l'ANSICE avec une gestion informatisée des incidents ;
- Administrer et optimiser les systèmes d'exploitation et les bases de données de l'ANSICE et en assurer les sauvegardes des régulières ;
- Assister les utilisateurs dans la maîtrise des outils informatiques et assurer leurs informations ;
- Prendre toutes autres actions relatives a la bonne exploitation des infrastructures réseaux et des systèmes de l'ANSICE

**Service d'Expertise et d'Innovation(SEI)**

est placé sous l'autorité d'un chef de service.Il est chargé de :

- définir et veiller a la mise en œuvre de la politique national en matière de la sécurité SI et des réseaux de communications électroniques de l'État ;

— élaborer les référentiels de sécurité du système d'information ;

— suivre les évolutions technologique en matière de sécurité du SI ;

— Participer a la consolidation de la formation et recyclage du personnel de l'État en matière de la cybersécurité ;

— Participer a l'élaboration des programmes des formations en matières de cybersécurité en collaboration avec des grandes écoles et des instituts nationaux de formation ;

— Établir les références et normes en matières de sécurité du SI et des réseaux de communications électroniques en assurant sa mise jours ;

— sensibiliser les structures nationales a la bonne utilisation des normes et standards en matières de sécurité informatique ;

— apporter un appui technique aux structures de l'État a utilisation des normes et standards en de sécurité su SI et ses réseaux ;

**Service d'Audit de Sécurité du Système d'Information(SASSI)**

est placé sous l'autorité d'un chef de service.Il est chargé de :

— définir le cahier de charge des auditeurs ;

— élaborer les référentiels de l'audit ;

— procéder a l'audit des administrations publiques ;

— promouvoir la fonction de l'audit de sécurité du système d'information ;

— procéder a la vérification sur le terrain de l'effectivité d'une mission d'audit après étude du rapport fourni ;

— veiller a la mis œuvre par la structure auditée des recommandations et des propositions mentionnées dans le rapport d'audit ;

— examiner la conformité des rapport des auditeurs externes suivant les procédures élaborées ;

## 1.2 Cadre du projet IAM de l'ANSICE

### 1.2.1 contexte

Ce projet de fin d'études entre dans le contexte de l'obtention de mon diplôme de Licence en informatique option cybersécurité.De ce fait, le projet IAM vise à mettre en place une infrastructure et des processus pour gérer de manière efficace et sécurisée les identités et les accès des utilisateurs dans un système informatique de cet institution.

### 1.2.2 les objectifs du projet

Les principaux objectifs de la gestion des identités et des accès sont de s'assurer que les parties légitimes ont le bon accès aux bonnes ressources au bon moment tout en gardant les parties non autorisées hors des systèmes.outre la définition d'une cible commune en matière de gestion des Identités et des Habilitations pour l'ensemble des Directions Métier de l'ANSICE, est la mise en œuvre des différentes exigences attendues et la définition d'une trajectoire à suivre permettant d'atteindre la cible par étapes de manière stable.De disposer d'une solution commune à l'ensemble des directions de travail pour gérer les habilitations des personnes accédant au SI de l'ANSICE en s'appuyant sur un référentiel global et centralisé.

- ❖ S'assurer de la fiabilité des données en synchronisant les informations entre les sources de données
- ❖ S'assurer de la conformité entre habilitations théoriques et habilitations pratiques par des réconciliations entre le référentiel central et les ressources applicatives cibles,
- ❖ Séparation du pouvoir des taches
- ❖ Réduction des habilitations en exception
- ❖ Processus de validation adaptés aux risques
- ❖ Identifier de manière unique un utilisateur sur le SI.
- ❖ Répondre aux évolutions technologiques à venir, notamment en termes de gestion des objets connectés, de virtualisation des identités, de blockchain et d'Intelligence Artificielle.

### 1.2.3 Etude de l'existant

Les entreprises ont besoin d'un système IAM pour assurer la sécurité en ligne et augmenter la productivité de leurs travail dans un environnement sécurisé.
Après une analyse de la situation nous avons remarqué que la structure d'accueil(ANSICE), dispose d'un réseau local déployé permettant aux employés,les personnels de se connecter sur l'internet.L'ANSICE dispose également d'une salle serveur gérer par les administrateurs réseau.Lors de notre stage au sein cet institution nous avons remarqué qu'il n'ya pas des systèmes permettant de gerer,de faire le suivis des utilisateurs,leurs activités en temps réel dans le système et leurs privilèges d'accès aux ressources confidentielles de cet institution

### 1.2.4 Critique de l'existant

Les employés, des sous-traitants, des fournisseurs, des clients,ont besoin d'accéder aux systèmes et nécessitent donc leurs identités et des droits d'accès qui leur sont attribués pendant le processus d'intégration aux système.
Nous avons remarque que lors de stage,la structure d'accueil ne dispose aucun mécanisme qui permet gérer les identités et des accès numérique

### 1.2.5 Proposition

Les investissements des entreprises ou organisation dans les systèmes de sécurité de haute technologie nécessite des mesures performants de sécurité de l'information,pour garantir leurs identités,les utilisateurs existants peuvent ne pas être trompés par des pirates.Ainsi nous proposons :

- l'Identification des individues dans le système IAM ;
- l'attribution des rôle des utilisateur(employés, des sous-traitants, des fournisseurs, des clients,des partenaires) dans le système ;
- Ajouter,supprimer et de mettre a jours des utilisateurs et leur rôle
- La création des groupes des utilisateurs avec un certain degrés de privilège d'accès aux ressource système ;
- Gérer le privilège d'accès des utilisateurs qui travail en télétravail
- Améliorer la productivité et les coûts récurrents de gestion et d'exploitation dans le système ;
- créer et de gérer des identités dans une solution IAM au moyen de flux de travail simples en privilégiant l'automatisation de la gestion ;
- Être capable, de désactiver l'ensemble des comptes et des accès d'un utilisateur qui vient de quitter la structure dans un temps court ;
- Définir le type de provisioning (manuel ou automatique) et d'authentification ;

# Conclusion

# Deuxième partie

# Le système de gestion et identification d'accès

# Chapitre 2

# Management des identités et accès

# Introduction

## 2.1 la sécurité informatique

La sécurité informatique est une discipline qui permet de protéger l'intégrité et la disponibilité des informations stockées dans un système informatique.
La sécurité permet de créer un espace numérique de confiance favorable a la dématérialisation,au partage et a l'échange de données de l'entreprise

### 2.1.1 Le système d'information

le Système d'information(SI) est un ensemble des moyens humains,techniques,organisationnels visant a assurer le traitement,le stockage et l'échange d'informations aux activités de l'entreprise

### les finalités de la sécurité du système d'information

les finalités de la sécurité du système est de lutter contre les risques auxquels est liés.ses risques sont entres autres :

- ➤ Défauts d'usage ;
- ➤ Défauts de conception
- ➤ Défauts d'implémentation
- ➤ Défauts de développement

### Limitation des impacts potentiel des risques

- ➤ Disposer des sauvegardes des données
- ➤ Avoir des procédures dégradées
- ➤ Tester les procédures de restaurations
- ➤ Avoir des secours de reprises,de continuité

### 2.1.2 Les notions fondamentales de la sécurité(DICP)

- ➤ Disponibilité(D) ;
- ➤ Intégrité(I) ;
- ➤ Confidentialité(C)
- ➤ Preuve(P)


FIGURE 2.1 – Exigence de la Sécurité Informatique

## Disponibilité(D)

La disponibilité du système d'information permet de garantir en permanence la communication et l'échange des données,sans défauts y compris les heures non ouvrées

## Intégrité(I)

L'intégrité est l'objectif d'exactitude et fiabilité des données et des traitements les systèmes d'informations doivent garantir que les informations sont identiques et inaltérables dans le temps

**une defaillance :** provoque des dysfonctionnement

## Confidentialité(C)

La confidentialité permet réserver l'accès aux seuls personnes autorisé dans un système informatiques.Les données confidentiels sont telles que les informations privées personnel,les informations protéger par l'organisation comme secret.

## Preuve(P)

La preuve permet l'investigation en cas de dysfonctionnement et d'incidents. Les systèmes d'information doivent pouvoir fournir la preuve d'un événement donné et permettre la vérification du bon déroulement des traitement des données informatique réalisé par les système ou des applications. Les mécanismes généralement employé sont la génération des traces informatique et un système d'imputabilité qui permet d'associer une action a son auteur

## 2.2 les incidents informatiques

### 2.2.1 Définition

Un incident de sécurité informatique est un imprévu indésirable qui a un impact sur la confidentialité,l'intégrité et la disponibilité de trafique des informations sur le réseau du système d'information. Ces incidents peuvent être causés par des erreurs humaines, des défaillances techniques, des attaques malveillantes ou d'autres facteurs externes.

### 2.2.2 les attaques

#### Deni de service

Déni de service/denial of service ou distributed(DOS/DDOS) est une attaque qui consiste a bombarder une machine avec un nombre des requêtes très important.Ainsi le serveur devient incapable d'assurer son service et commence a répondre aux services non autoriser

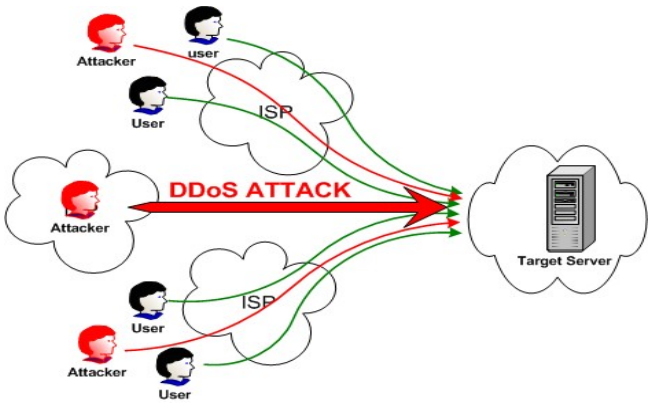


FIGURE 2.2 – DDoS1.jpg

[1]

#### attaque de l'homme du milieu

lorsqu'un pirate,prenant le contrôle d'un équipement du réseau,se place au milieu d'une communication,il peut écouter ou modifier des échanges des informations.Cet attaque est également appeler Man In The Middle(MITM).Se fait passer pour l'un avant d'obtenir le mot de passe de l'autre pour se retourner contre le premier.Les points sensible pour cet attaque sont DHCP,ARP,ICPM

[2]

1. sourc :images.search.yahoo.com/yhs/search ?p=attaque+par+d%C3%A9ni+de+servicefr=yhs-bc
2. sourc :https ://www.google.com/search ?q=attaque+par+l%27homme+du+milieuclient=ubuntu

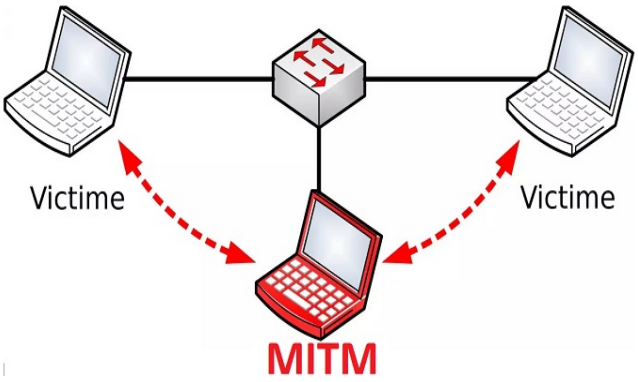


FIGURE 2.3 – Man in The Middle

### 2.2.3 Packer

un packer est un logiciel permettant de compresser,encoder ou chiffrer un binaire sans en altérer le fonctionnement.Il serve a encoder des fichiers afin de compliquer la détection des logiciels malveillant aux logiciels antivirus.ces logiciels sont entre autre :Armadillo,Aspack,Asprotect

#### Hijacker

est programme qui s'installe de manière invisible et qui modifie les paramétrages du navigateur et fonctions afin de le forcer a consulte d'autre pages que celles qui étaient définies auparavant.Les navigateurs internet hijacker utilisent souvent les failles de sécurité et les points faibles des systèmes pour s'y implanter profondément.Le but de ce type d'attaque d'augmenter le nombres des visiteurs de leur site malveillant.

## 2.3 Etude préliminaire

Afin d'atteindre nos objectifs, il est important avant tout de procéder à l'analyse des mécanismes existants qui vont nous permettre en place notre système.Pour cela nous allons étudier les différents système de gestion des identités et d'accès (sgia) existant et utilisant par grand entreprise prometteuse de la nouvelle technologie

### 2.3.1 Etat de lieu de l'existant

Il existe plusieurs systèmes IAM (Identity and Access Management) largement utilisés dans le monde.

- **Microsoft Azure Active Directory (Azure AD)** : est un service de gestion des identités et des accès basé sur le cloud,hybrides et sur site fourni par Microsoft. Il est couramment utilisé pour la gestion des identités et des accès dans les services Microsoft tels que Office 365 et Azure également utiliser pour les application intra et extranet d'une organisation.

■ **Ping Identity** :est une plateforme IAM complète qui prend en charge l'authentification, l'autorisation, la gestion des identités et des accès, ainsi que le SSO. Elle est utilisée pour sécuriser l'accès aux applications et aux données dans les environnements cloud, hybrides et sur site.PingFederate s'intègre aux solutions existantes de nombreux fournisseurs d'infrastructure IAM.La coexistence avec les solutions IAM existantes est rendue possible par un processus de traduction de jeton, permettant de nombreuses options d'authentification pendant la phase de migration.

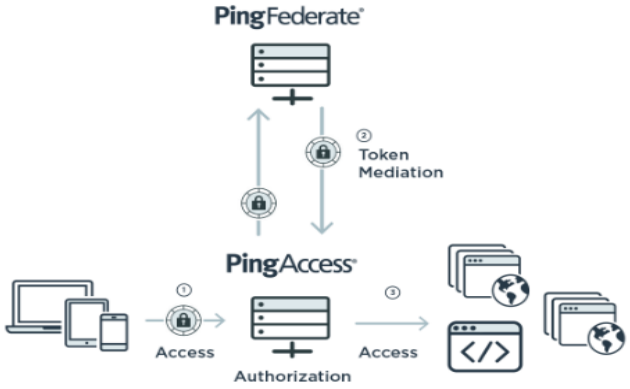


FIGURE 2.4 – Ping Identity federate

[3]

■ **IBM Security Identity Manager** : Il s'agit d'une solution IAM d'IBM qui permet la gestion centralisée des identités et des accès. Il offre des fonctionnalités de provisioning, de gestion des rôles, de workflow et de gouvernance des identités. [4]

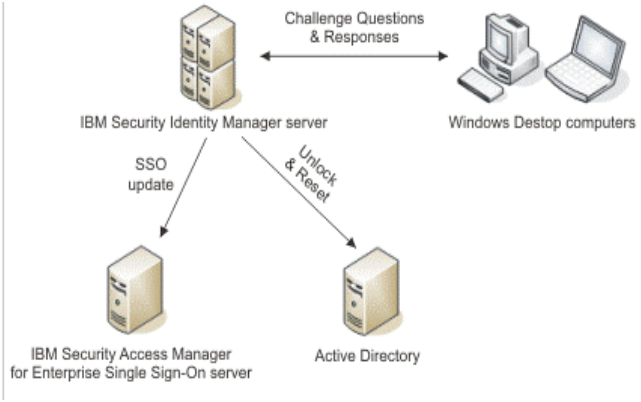


FIGURE 2.5 – IBM Security Access Manager

3. source : https ://www.pingidentity.com/de/platform/capabilities/extensibility.html
4. source :https ://entwickler.de/sharepoint/zutritt-nur-fur-mitglieder

IBM Security Access Manager, anciennement IBM Tivoli Access Manager, est un produit commercial d'IBM destiné à protéger contre l'accès des utilisateurs non autorisés aux applications Web. Comme le figure ci-dessus indique,le fonctionnement d'IBM Security Access Manager repose en grande partie sur ses composants , le serveur de connexion unique et un composant LDAP. IBM Security Access Manager prend en charge divers composants LDAP tels que l'Active Directory.

- **ForgeRock Identity Platform :**La ForgeRock Identity Platform est une suite IAM complète qui propose des fonctionnalités de gestion des identités, de l'authentification, de la gestion des accès et des privilèges, ainsi que du SSO. [5]

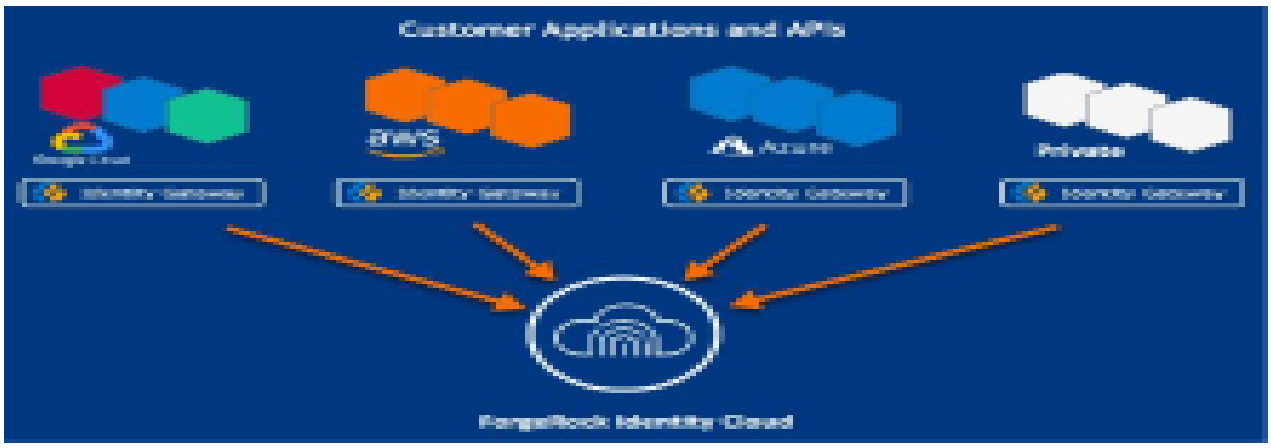


FIGURE 2.6 – ForgeRock Identity Platform

ForgeRock offre la seule plate-forme de bout en bout du secteur, basée sur l'IA, spécialement conçue pour toutes les identités et pour tous les environnements sur site, multi-cloud ou hybride.

- **Oracle Identity Management :**Oracle propose une suite de produits IAM qui comprend Oracle Identity Manager, Oracle Access Management et Oracle Identity Governance.

  [6] Oracle Identity Manager (OIM) est un produit Stack qui gère l'approvisionnement des utilisateurs,la création/suppression/gestion des privilèges d'accès des utilisateurs,la réconciliation et le traitement des demandes (à l'aide du workflow).

5. source :https ://www.google.com/search ?client=ubuntu-chrhs=50vsxsrf=AB5stBjQ5EU8IvtqOOPiRqNz$_7$*eb*8*Kbz*−*Q*

6. source :https ://onlineappsdba.com/index.php/2010/06/29/oracle-identity-manager-thor-xellerate-architecture/

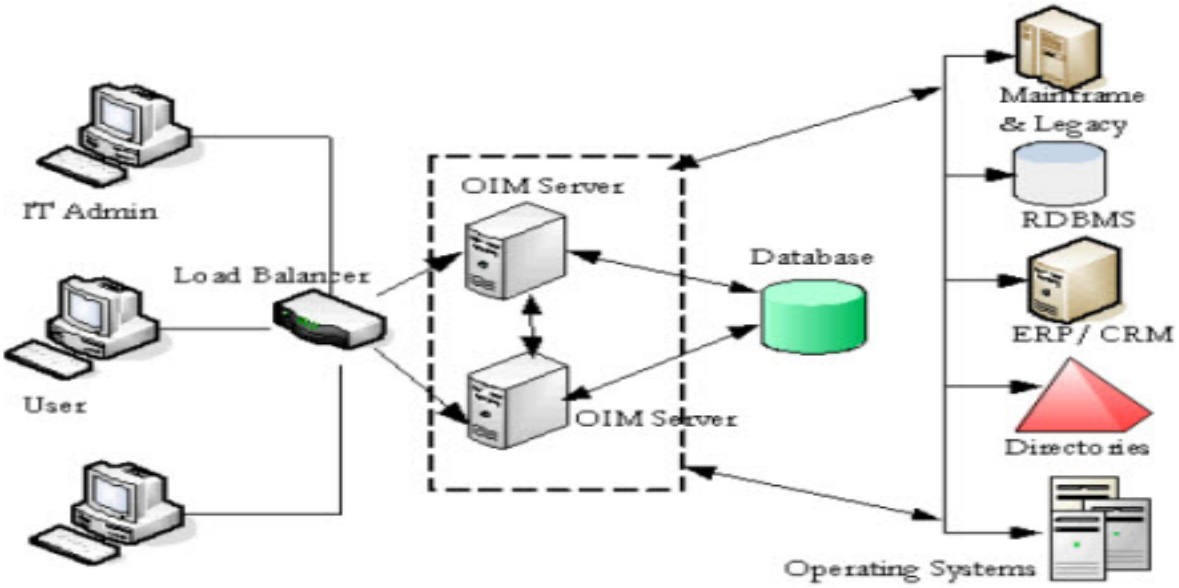


FIGURE 2.7 – Architecture Oracle Identity Manager

■ **SailPoint IdentityIQ :** SailPoint IdentityIQ est une solution IAM qui offre des fonctionnalités de gestion des identités, de la gouvernance des accès et de la conformité. Elle permet aux organisations de gérer les identités des utilisateurs, de contrôler les accès

### 2.3.2 Justification du projet IAM

Comme nous avons vus dans l'étude de l'existant que l'ANSICE ne dispose pas le système IAM,gérer des nombreux problèmes a savoir :

1. la perde de productivité du système ;
2. la charge et le travail des administrateurs
3. impossible de faire la traçabilité pertinence des actions des administrateurs pour assurer la cohérence et la
4. difficile de faire l'audit des ressources du système
5. non-respect des contraintes ou la réglementation

## 2.4 Les acteurs, les ressources et les processus impliqués

Le système de gestion des identités et des accès (IAM) implique différents acteurs, ressources et processus pour assurer la sécurité et la gestion des identités et des accès au sein d'une organisation. Voici les principaux éléments impliqués dans le système de Gestion des identités et d'accès :

### 2.4.1 Les acteurs

Les acteurs du système de gestion des identités et d'accès sont personnes responsables de la gestion,de maintenance du système du IAM

1. Utilisateurs finaux : Ce sont les personnes ou des entités ayant une identité numérique qui utilisent les applications,les services,et un certain nombre d'accès a son niveau au sein de l'organisation. Ils ont des identités uniques et des droits d'accès qui leur permettent d'interagir avec les ressource.
2. Administrateurs IAM :se sont personnes qui sont responsables de la création,de gestion,de suivie et supprimer des identités d'utilisateur, de définir des politiques d'accès,les bonnes pratiques pour garantir la sécurité et la disponibilités et de veiller également à ce que les bonnes personnes aient les bons niveaux d'accès.
3. Propriétaires de ressources : Ce sont les individus et les équipes qui sont pondéré des différentes ressources, telles que les applications,les bases de données ou les fichiers. Ils définissent les politiques d'accès à leurs ressources et collaborent avec les administrateurs IAM pour les mettre en œuvre.
4. Fournisseurs de services d'identité :Il s'agit d'organisations ou tout entité externes qui donnent des services d'authentification et d'autorisation, tels que l'intégration avec des fournisseurs d'identité tiers

### 2.4.2 les ressources

1. Identités d'utilisateur :dans le système IAM Chaque utilisateur final doit possède une identité unique dans le système IAM. Cela peut inclure des informations telles que le nom, l'adresse e-mail,reconnaissance faciale tout autre politique utiliser pour accéder au système
2. Groupes :les utilisateurs du système peuvent êtres regroupés dans les référentielle centrale en groupe statique ou dynamiques.Les groupes simplifient la gestion des autorisations,car les politiques d'accès peuvent être appliquées à un groupe plutôt qu'à des utilisateurs individuels.
3. Rôles : Les rôles sont des ensembles permission ou de privilèges et de droits d'accès prédéfinis qui sont assignés aux utilisateurs ou aux groupes. Les rôles définissent les autorisations spécifiques pour accéder à certaines ressources ou effectuer certaines actions.

### 2.4.3 les processus impliqués

Une processus est définie comme étant des taches effectués par les acteurs,identifier a l'aide des différents outils,démarche orienter sur les modélisation des étapes a réaliser en vue d'obtenir un résultat.

#### Authentification

Il s'agit du processus permettant de vérifier l'identité numérique d'un utilisateur.Cela peut impliquer les différents manière d'authentification telles que l'authentification multi facteurs facteurs(2FA),reconnaissance faciale ou d'utilisation d'empreinte digital.

#### Autorisation

Autorisation détermine les ressources auxquelles l'utilisateur a accès en fonction de son rôle,de ses privilèges et de politique d'accès définie par le système.

#### Gestion des identités

Cela regroupe les processus de création,de mise a jour et des suppression des identités des utilisateurs.Implique également la gestion des comptes des utilisateurs,la récupération de mot de passe des comptes perdu et la gestion des d'accès.
ON definie trois types sous processus dans la gestion des identité

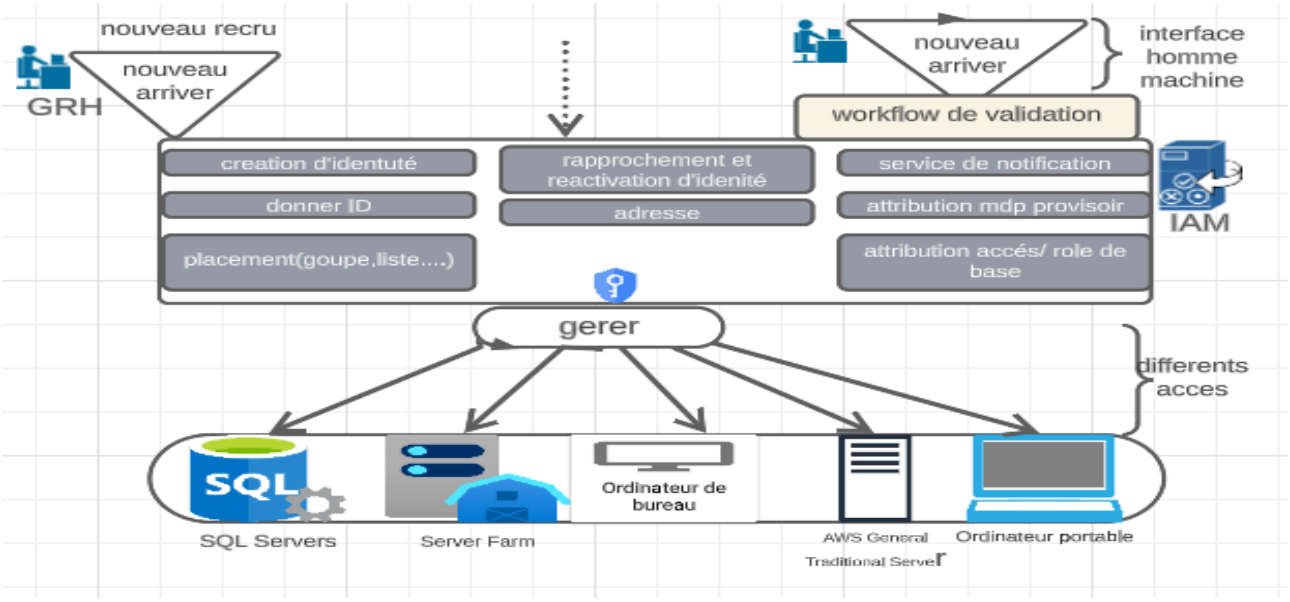


FIGURE 2.8 – processus de la gestion des identité d'un nouveau arrivé

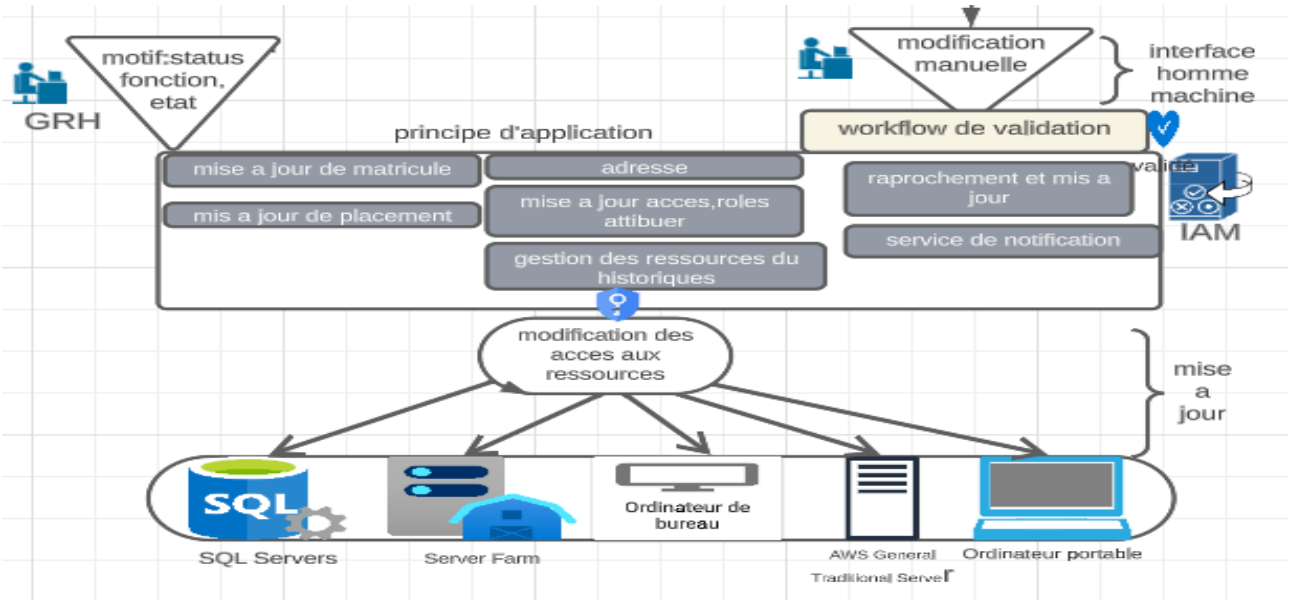


FIGURE 2.9 – processus de la gestion des identité du cycle de vie d'utilisateur

## processus de gestion des accès

Demande d'accès

Demande de suppression d'accès

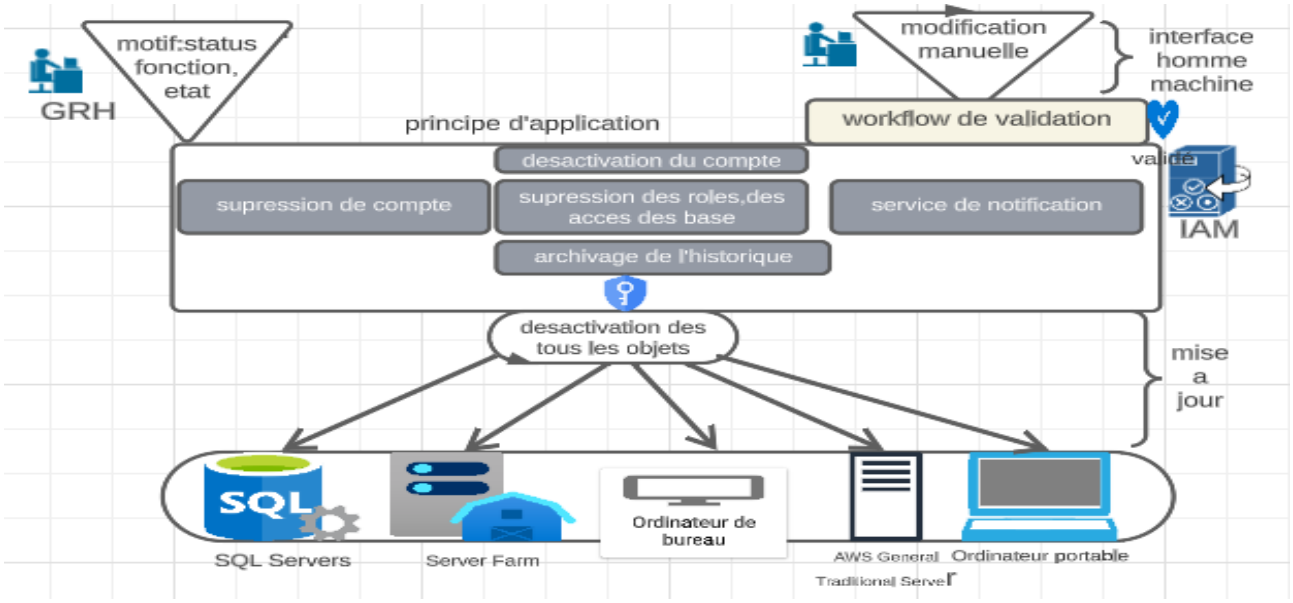


FIGURE 2.10 – processus de la gestion des identité d'un nouveau depart

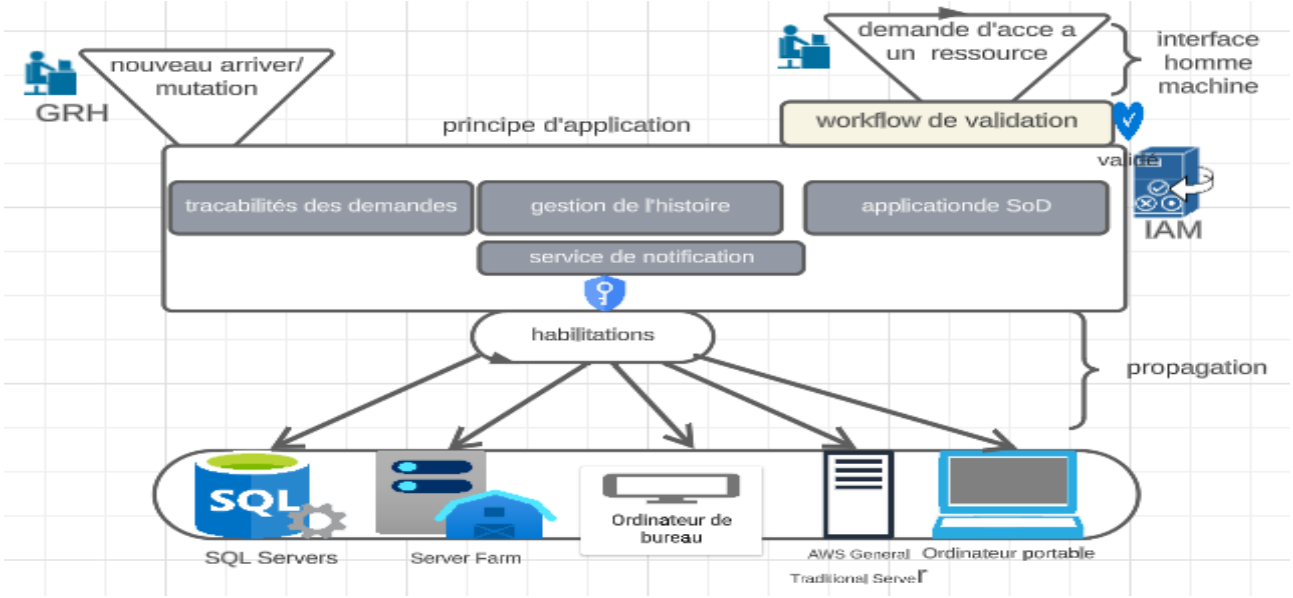


FIGURE 2.11 – processus de la demande des accès

## processus de la gestion de conformité

tous les processus utlisee dans le systeme de gestion des identités et d'accès se résument dans le schema ci-dessous

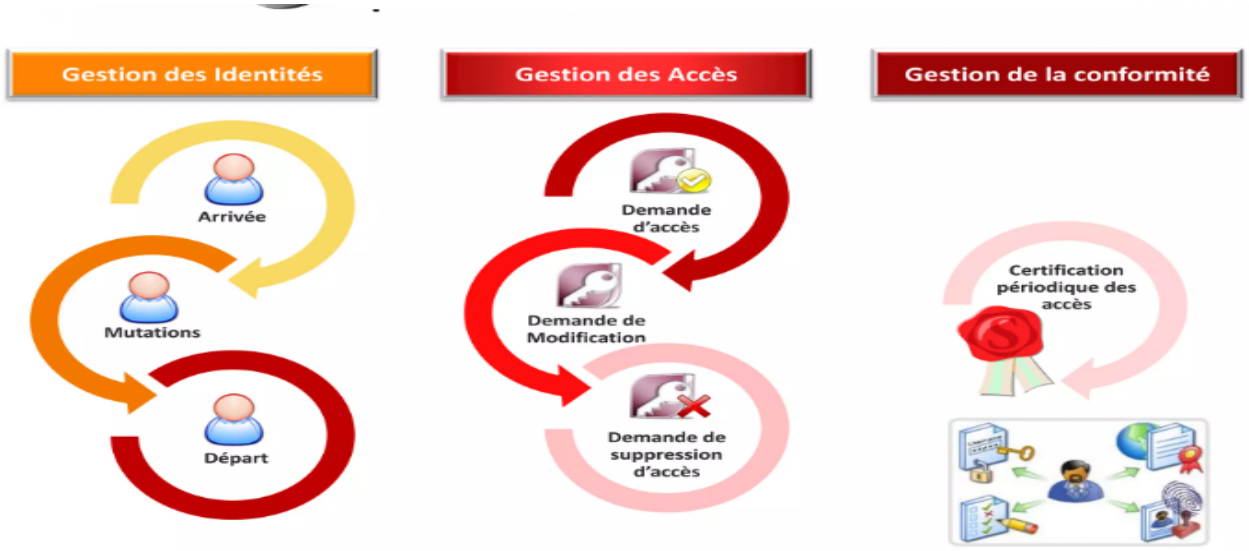


FIGURE 2.12 – processus de la demande de suppression d'accès

## 2.5 Les types et les niveaux d'identité et d'accès

les principaux types et niveaux d'identité et d'accès couramment utilisés dans les systèmes IAM.

1. **Types d'identité :**
   - **Identité utilisateur individuelle :** Il s'agit d'une identité unique attribuée à un utilisateur individuel.
   - **Identité de groupe :** Une identité de groupe regroupe plusieurs utilisateurs en fonction de critères communs. Elle simplifie la gestion des autorisations en appliquant les mêmes privilèges à tous les utilisateurs du groupe.
   - **Identité de service :** l s'agit d'une identité utilisée par des applications ou des services plutôt que par des utilisateurs. Les identités de service permettent aux applications d'accéder à d'autres ressources et services de manière sécurisée.
2. **Niveaux d'accès :**
   - Accès au système ;
   - Accès physique ;
   - Accès aux données ;
   - Accès aux applications ;
   - Accès aux fonctionnalités ;

## 2.6 Les principes fondamentaux du système de gestion des identités et d'accès

Le système de gestion des identités et d'accès (IAM) repose sur certains principes fondamentaux pour assurer une gestion efficace et sécurisée des identités et des accès au sein d'une

organisation.

- ➤ Intégration et interopérabilité ;
- ➤ Audit et suivi ;
- ➤ Ségrégation des tâches ;
- ➤ Gestion des privilèges ;
- ➤ Autorisation ;
- ➤ Identification ;
- ➤ Gestion du cycle de vie des identités ;

Au niveau du cycle d'un utilisateur,il y'a plusieurs processus a suivre :L'inscription,L'octroi des accès,La modification des accès,a révision et la surveillance des accès,Le désapprovisionnement

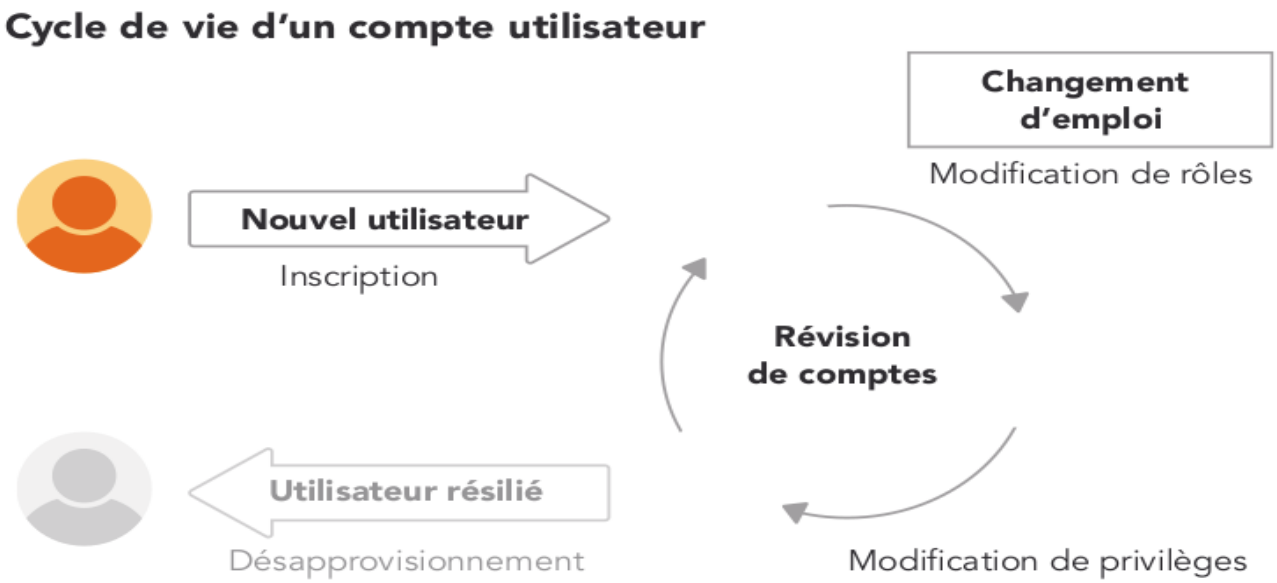


FIGURE 2.13 – le cycle de vie d'un utilisateur

## 2.7 Les avantages et les inconvénients du système de gestion des identités et accès

### 2.7.1 Les avantages

Le système de gestion des gestion des identités et accès est une technologie utilisée pour centraliser les activités des utilisateurs permettant de détecter les individues non autoriser dans le système et de faire suivies des utilisateurs durée le temps actif.Dans le cas de l'ANSICE l'IAM joue un role centraliser très important pour sa bonne gestion pour s'assurer la confidentialité,la disponibilité et la non répudiation .

— l'amélioration de l'expérience utilisateur, en réduisant le nombre d'identifiants à retenir pour l'accès aux actifs informationnels ;

— une réduction de la surcharge administrative concernant la gestion de comptes, grâce à des outils et des processus automatisés d'autorisation, d'approbation, de modification et de révocation des accès ;

— l'optimisation de la sécurité de comptes et des actifs informationnels, avec l'implantation de mécanismes d'authentification multi-facteur et de politiques appliquées en fonction de risques lié a ce système ;

— l'uniformisation des profils d'accès qui respectent les meilleures pratiques, tels le principe du moindre privilège, le besoin de savoir et la séparation de tâches incompatibles ;

— des mécanismes simplifiés, offerts aux responsables des actifs informationnels, pour la révision périodique des accès avec une procédures,dégrader ;

— des mécanismes d'alertes et de surveillance permettant la détection et le traitement des accès non autorisés.

### 2.7.2 les inconvénients

le système de gestion des identités et des accès (IAM) présente de nombreux inconvénients.

1. Le risque de sécurité lié à l'authentification repose sur un point central qui est le fournisseur d'identité qui devient un point de vulnérabilité.
2. Dépendance à un système centralisé : Si le système IAM centralisé rencontre des problèmes de performance ou est inaccessible, cela peut entraîner une interruption de l'accès aux ressources pour les utilisateurs.
3. Vulnérabilités de sécurité : Bien que l'IAM soit conçu pour renforcer la sécurité des identités et des accès, un mauvais déploiement ou une configuration incorrecte peuvent entraîner des vulnérabilités de sécurité.
4. Gestion des identités obsolètes : Les systèmes IAM doivent être constamment mis à jour pour refléter les changements dans l'organisation, tels que les mouvements du personnel, les changements de rôles ou les départs.

5. Coût : La mise en place d'un système IAM peut entraîner des coûts élevés, notamment en termes d'investissement initial, de développement personnalisé, de formation des utilisateurs et de maintenance continue.
6. Complexité : La mise en place d'un système IAM peut être complexe, en particulier pour les grandes organisations avec des infrastructures informatiques complexes et dispersées.

## 2.8 L'évaluation et Les perspectives du système de gestion des identités et accès

### 2.8.1 L'évaluation

L'évaluation du système de gestion des identités et des accès peut avoir plusieurs niveau sur l'organisation.
L'évaluation du système permet d'énumérer les vulnérabilités dans la gestion des identités et des accès. Cela peut inclure des défauts de configuration, des privilèges excessifs, des politiques d'accès inappropriées ou des oublis dans les contrôles de sécurité. L'évaluation du système IAM aide à s'assurer que l'organisation est conforme aux réglementations et aux normes de sécurité pertinentes. Cela inclut des réglementations telles que le RGPD (Règlement général sur la protection des données) et des normes de sécurité telles que ISO 27001.système IAM permet d'améliorer le contrôle et la gouvernance des identités et des accès,d'identifier les problèmes et les contraintes que les utilisateurs peuvent avoir lors de l'authentification et de l'accès aux ressources.

### 2.8.2 Les perspectives

Le système de gestion des identités et des accès (IAM) a ses perspectives prometteuses pour l'avenir de la technologie. L'IAM joue un rôle primordiale dans la gestion sécurisée des identités et des accès aux ressources cloud.Les perspectives d'avenir incluent une intégration plus étroite de l'IAM avec les services cloud, une gestion centralisée des identités multi-cloud et des mécanismes d'authentification et d'autorisation adaptés aux environnements cloud. L'intelligence artificielle (IA) et l'apprentissage automatique (machine learning) peuvent être intégrés dans l'IAM pour détecter les comportements anormaux, identifier les tentatives d'accès frauduleuses et améliorer la détection des menaces. Les perspectives futures incluent une adoption accrue de l'IAMaaS, permettant aux organisations de se concentrer davantage sur leur cœur de métier tout en bénéficiant d'une gestion des identités sécurisée et évolutive. l'IAM est appelé également à jouer un rôle important dans la gestion sécurisée des identités et des accès aux objets IoT,l'utilisation de technologies biométriques telles que la reconnaissance faciale, l'empreinte digitale ou la reconnaissance vocale,

### 2.8.3 Les méthodes et les techniques de l'évaluation du système de gestion des identités et accès

L'évaluation du système de gestion des identités et des accès (IAM) peut être réalisée en utilisant différentes méthodes et techniques pour collecter des informations et évaluer la performance, la sécurité et l'efficacité du système. La méthode revue documentaire implique le teste approfondi de la documentation liée à l'IAM, tels que les politiques, les procédures, les directives, les contrats de niveau de service et les preuves d'Audit. Les entretiens avec les parties prenantes clés, tels que les administrateurs système, les gestionnaires d'identités, les responsables de la sécurité et les utilisateurs finaux, permettent de recueillir des informations sur l'utilisation, la satisfaction et les défis liés au système Les tests de pénétration, également connus sous le nom de tests d'intrusion, permettent d'évaluer la résistance du système IAM aux attaques et aux tentatives de violation de la sécurité. L'évaluation des performances implique la collecte de mesures quantitatives, telles que les temps de réponse, les taux de disponibilité et les capacités de traitement, pour évaluer l'efficacité et la fiabilité du système,également cette évaluation consiste à justifier si le système est conforme aux réglementations et aux normes de sécurité applicables dans l'organisation

## 2.9 La Gestion des identités

Pour toute entreprise axée sur les données, les solutions d'identité numérique devraient constituer un élément principale. Il est impératif d'assurer une sécurité robuste des données à tous les niveaux, car toute forme de compromission peut rendre l'entreprise vulnérable.Alors l'identité est définie comme un ensemble des éléments caractéristiques propres par lesquelles une personne ou une organisation est connue ou reconnue. Ces éléments peuvent être définis,comme le nom, l'adresse courriel, la nationalité, ou peuvent être des caractéristique naturel comme les empruntes digitales,reconnaissance faciale. Pour l'identité d'une organisation, les caractéristiques sont acquises.De ce fait,nous allons étudier en détail les différents types des identités,leur mode de fonctionnement dans le système

### 2.9.1 Importance de gestion des identités

En ce qui concerne l'importance de gestion des identité,est très primordial dans l'évolution massive de la science technologie de l'information et de la communication (TIC) avec la numérisation du monde de jours. La gestion des identités(IDM) garantit que uniquement les utilisateurs autorisés, ont accès aux ressources technologiques dont ils ont besoin pour accomplir leur travail.S'appuie également sur des règles et des technologies qui déploient un processus à l'échelle de l'entreprise pour identifier des personnes, des groupes de personnes ou des applications logicielles, les authentifier et leur accorder des autorisations, comme il convient, via des attributs, en fonction de leur identité, qu'il s'agisse de leur accorder des droits d'accès utilisateur ou de limiter leurs accès. Un système de gestion des identités empêche tout accès non autorisé aux systèmes et aux ressources, empêche l'exfiltration de données d'entreprise ou protégées, et déclenche des alertes et des alarmes lors de tentatives d'accès par des personnes ou des programmes non autorisés

### 2.9.2 Modèles de gestion des identités

Une identité peut être utilisée dans plusieurs contextes. Conjointement, dans un même domaine, une entité peut être incarnée par plusieurs identités. De plus, plusieurs identités d'une même entité peuvent partager les mêmes caractéristiques, ce qui implique que les identités peuvent ne pas être uniques dans un même contexte.

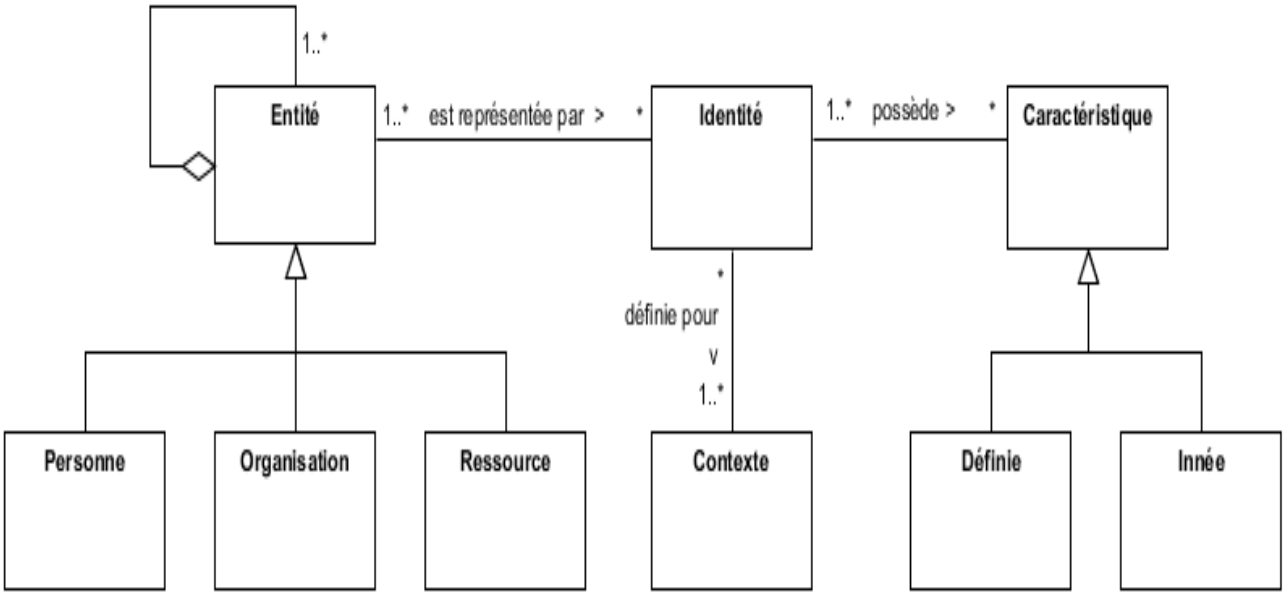


FIGURE 2.14 – Diagramme de classe du concept d'identité

Dans un domaine d'identité, le partage des attributs utilisés par les mécanismes d'identification (association de l'identifiant et d'un justificatif d'identité ; l'identification est souvent réalisée conjointement à l'authentification) implique pour les fournisseurs de service de partager les risques en cas de corruption d'une identité. Les différents modèles de gestion des données permettent donc de déporter les risques et les charges d'administration à différents niveaux. Différents modèles de gestion des identités peuvent cohabiter au sein de la même organisation

### 2.9.3 Identités isolées

Dans ce modèle, chaque fournisseur de service utilise son propre domaine d'identité.Un utilisateur doit utiliser un identifiant et un justificatif d'identité différents pour s'authentifier auprès de chacun des domaines. Du point de vue de chacun des fournisseurs d'identité, la gestion des identités est plus simple. De plus, en cas d'usurpation d'identité dans l'un de domaine d'identité, les autres fournisseurs de service ne sont pas impactés. Ce modèle a également l'avantage de permettre de définir un niveau de sécurité différent pour les justificatifs d'identités. Cette approche peut devenir complexe pour les utilisateurs du système,ce dernier doit répéter les étapes d'authentification et d'identification auprès de chacun des domaines d'identité rattachés aux fournisseurs de services.Dans ce modèle l'utilisateur doit gérer plusieurs information pour s'authentifier a chaque système,cela peut entraîner le risque d'oublie ou la confusion des identifiant

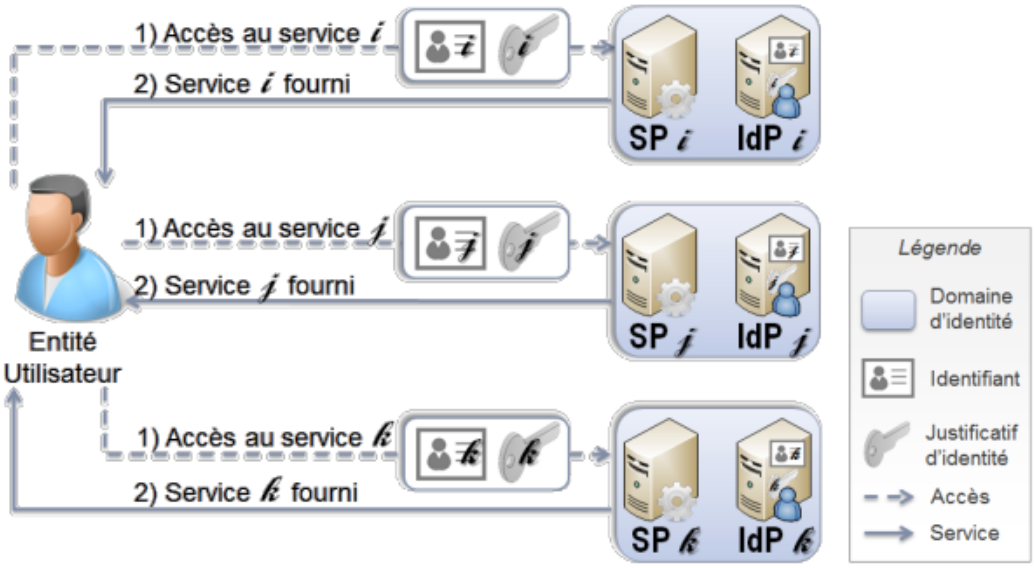


FIGURE 2.15 – Modèle de gestion d'identité isolée

### 2.9.4 Identités centralisées

la gestion centralisée des identités, les utilisateurs peuvent accéder à toutes leurs applications, à leurs sites web et autres systèmes avec les mêmes identifiants. Ceci améliore l'expérience utilisateur car il suffit de saisir les identifiant de l'entité associer.Sont entre autre :

- ❖ Identité commune

❖ Single Sign-On (SSO)

### Identité commune

Dans ce modèle, une entité unique agit en tant que fournisseur d'identité pour l'ensemble des fournisseurs de service. Le mode de fonctionnement est à mi-chemin entre le modèle d'identité isolée et le modèle d'identité fédérée du point de vue de l'utilisateur.

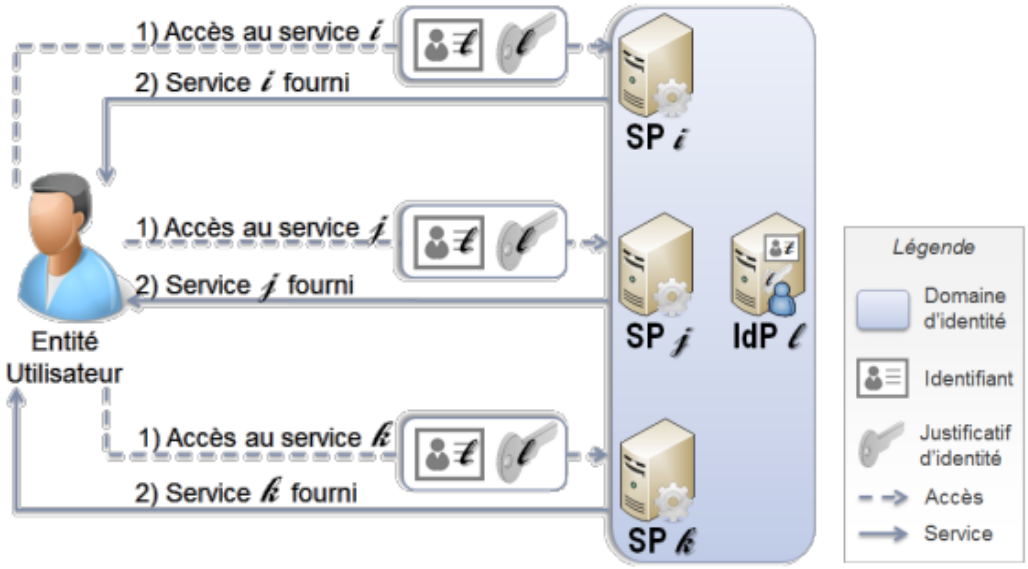


FIGURE 2.16 – Modèle de gestion d'identité isolée

Le fournisseur d'identité unique,le point point centrale de plusieurs fournisseur de service. en cas de défaillance ou de modification au niveau du domaine d'identité, toutes les entités dépendantes sont impactées.

### Single Sign-On (SSO)

L'approche Single Sign-On est similaire à une fédération d'identité,il n'existe qu'un seul fournisseur d'identité.Dans cet architecture l'utilisateur a besoin de s'authentifier qu'une seul fois.Le modèle Single Sign-On est un modèle permettant une authentification unique inter-domaine.
ce modèle d'identité permet aux utilisateurs d'utiliser un unique couple identifiant-justificatif d'identité quel que soit le service demandé au sein du domaine d'identité.

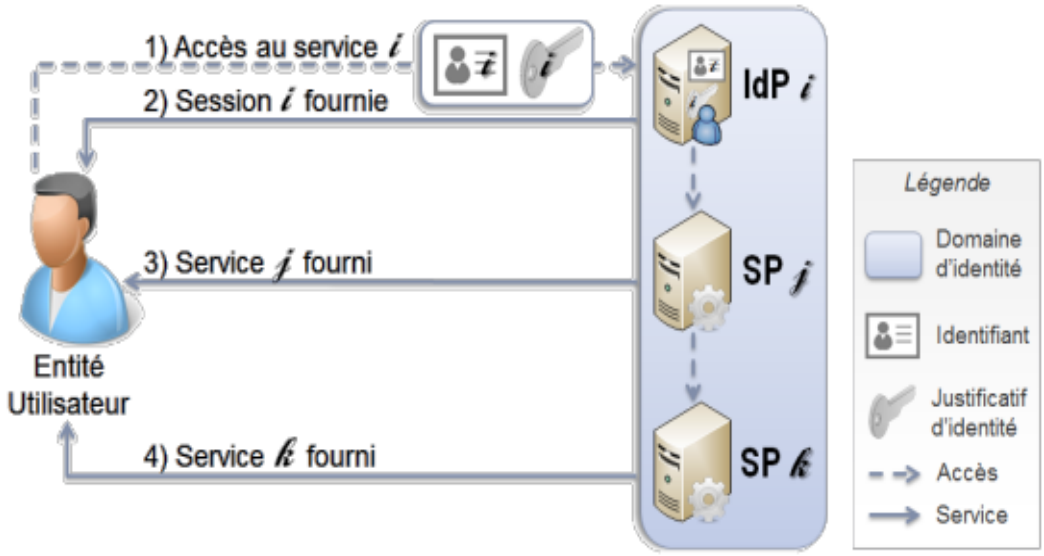


FIGURE 2.17 – Modèle de gestion d'identité :Single Sign-On

### 2.9.5 Fédération d'identités

a fédération d'identité est un ensemble d'accords, standards et technologies permettant à un groupe de fournisseurs de service de reconnaître les identifiants provenant d'autres fournisseurs de services appartenant à la fédération. La fédération donne aux utilisateurs l'illusion de n'utiliser qu'un seul et unique identifiant alors qu'il continue à en présenter un différent à chaque fournisseur de service. Dans ce genre d'architecture,chaque fournisseur de service utilise son propre fournisseur d'identité,mais est capable d'accepter les identités provenant d'autres fournisseurs. [7]

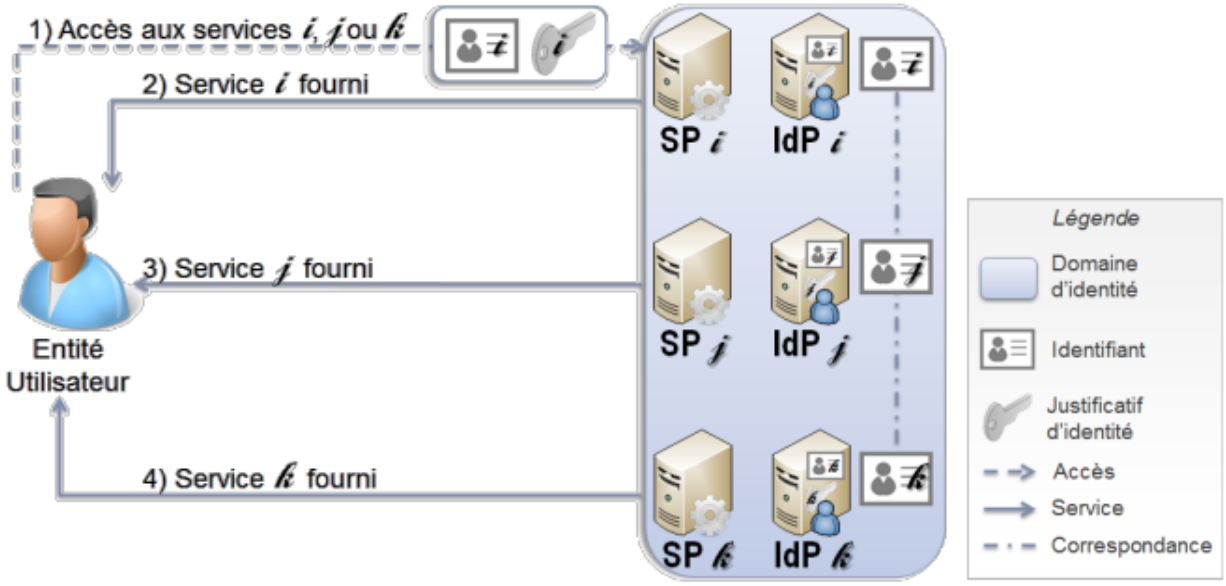


FIGURE 2.18 – Modèle de gestion d'identité fédéré

Le ci-dessus illustre les avantages de la fédération des identités des utilisateurs par apport

7. source :https ://www.b2b-infos.com/12694/ess-caracteristiques-economie-sociale-et-solidaire/

au modèle précédent.Dans ce modèle,les informations nécessaires des utilisateur aux processus d'authentification,d'identification et autorisation sont tous les mêmes.Ce qui permet d'éviter les oublies ou confusion.

## 2.10 Gestion des accès

### 2.10.1 Définition

### 2.10.2 Ressources et gestion des accès

La gestion des ressources permet d'autoriser les utilisateurs qui ont définie leur identités dans le système de donné l'accès aux ressource dont ils ont besoins pour y accéder. Par la politique de gestion des accès, les accès aux ressources sont limités par des contraintes établies par l'organisation dont les définitions sont développées ci-dessous :

— Mode d'authentification et contrôle d'accès ;

— Périmètre d'accès ;

— Rôles, profils et groupes autorisés.

### 2.10.3 Habilitations

une habilitation comme un droit d'effectuer une action sur une ressource. Elle est associée à un périmètre qui limite quand et comment cette ressource peut être utilisée par une entité.Dans une organisation,les habilitations sont attribues en fonction des besoins nécessaires

### 2.10.4 Identification,Authentification et autorisation

#### Identification

**identifiant** :C'est une chaîne de caractère qui sert d'index dans la base de donnée de l'application.L'identité informatique peut être liée a un objet ou a individue.

#### Les types d'identifiants

➤ Identifiant physique :Nom,Prénom,Date de naissance ;

➤ Identifiant d'accès réseau :téléphone,internet,mobile

➤ Code d'accès aux ressources réseau et système d'une entreprise

➤ Certificat numérique

➤ Identifiant auprès de services a accès réservés :banque

➤ Numéro de cartes bancaires

#### Authentification

l'authentification est le processus qui permet de vérifier que l'identité donnée par une entité est légitime. Elle est basée sur un ou plusieurs mécanismes de reconnaissance :

— un mot de passe ou un numéro personnel d'identification (code PIN) ;

— une carte ou une clé ;

— une empreinte digitale ou rétinienne.

L'authentification est plus sûre si plusieurs techniques sont utilisées. En effet, un mot de passe peut être deviné et une reconnaissance faciale peut être faussée. Aussi, l'utilisation d'une technique ne fournit pas un niveau de sécurité suffisant. Il faut en utiliser plusieurs pour diminuer les risques de falsification. Le mode d'authentification peut être déterminé en fonction du rôle associé aux comptes utilisateurs ou de la ressource utilisée.

**les 3 niveaux authentification**

1. Authentification faible a une passe
   - envoi simple de mot de passe
   - possibilité de génération automatique de mot passe
   - compromission a détecter
2. authentification forte a une passe
   - mot de passe dynamique
   - nécessite une bonne synchronisation pour le contrôle
3. Authentification forte a deux facteurs
   - une procédure challenge réponse
   - le vérificateur pose une question au prouveur
   - question différente a chaque fois et prédictible
   - la réponse varie a chaque session,permettant d'éviter le rejet
   - la réponse de prouveur dépend de :la question et l'élément secret qui caractérise le prouveur

### 2.10.5 autorisation

L'autorisation est un concept clé en sécurité informatique qui contrôle l'accès aux ressources, aux données et aux fonctionnalités d'un système informatique. Elle vise à garantir que seules les personnes ou les entités autorisées peuvent accéder et utiliser les ressources appropriées.

— accéder au système

— Entrer dans la salle

— lire/écrire des données

— acheter

## 2.11 Contrôle d'accès physique et contrôle d'accès logique

### 2.11.1 Contrôle d'accès physique

L'accès physique concerne l'entrée physique à un emplacement ou à un équipement informatique. Cela concerne la possibilité de toucher, d'interagir physiquement ou de manipuler le matériel informatique.
l'accès à un centre de données, aux serveurs, aux ordinateurs, aux périphériques de stockage ou à d'autres équipements matériels. La sécurité physique vise à protéger ces ressources contre l'accès non autorisé, le vol ou la manipulation physique.

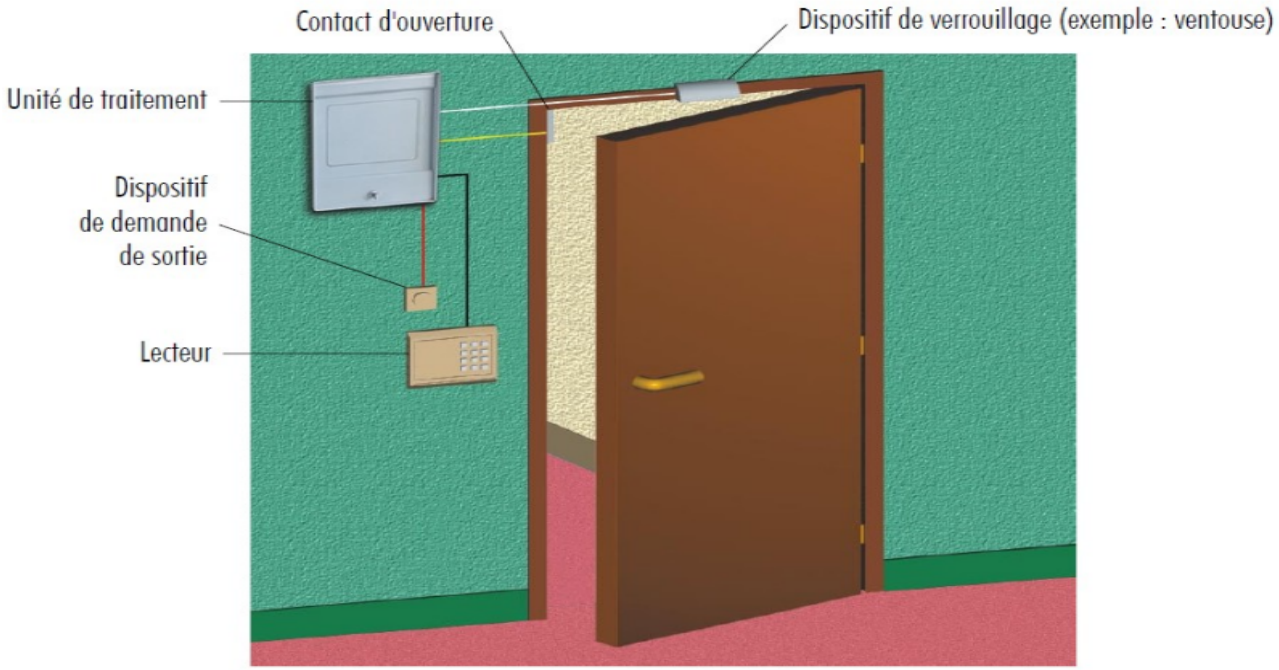


FIGURE 2.19 – le contrôle d'accès physique

8

### 2.11.2 contrôle d'accès logique

L'accès logique concerne la possibilité d'interagir avec les systèmes informatiques, les applications, les réseaux ou les données par le biais d'identifiants de connexion et de mécanismes de contrôle d'accès électroniques.
La sécurité de l'accès logique implique la mise en place de politiques et de mécanismes de contrôle d'accès pour vérifier l'identité des utilisateurs et leur attribuer des autorisations appropriées. Cela peut inclure :

➤ l'authentification basée sur des mots de passe

8. source :https ://www.google.com/search ?client=operasxsrf=AB5stBhAdgQzySH3y4WLJNc6UPseAgs2pA :168895163

- des certificats numériques ;
- des clés d'authentification à deux facteurs ;
- des contrôles d'autorisation et des journaux d'audit ;
- Les pare-feu, les systèmes de détection d'intrusion ;
- les systèmes de prévention des intrusions ;

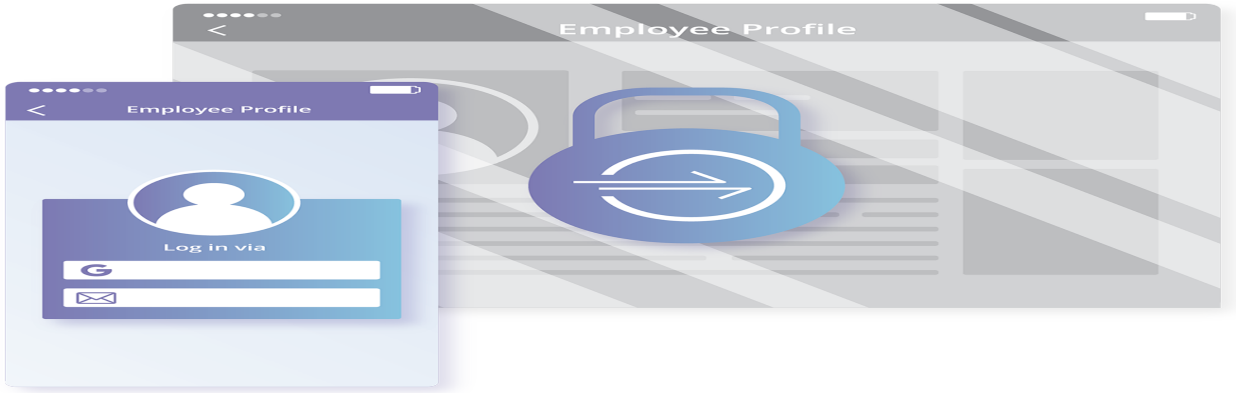


FIGURE 2.20 – le contrôle d'accès logique

9

d'autres mesures de sécurité sont également utilisés pour protéger les systèmes contre les accès logiques non autorisés, les attaques ou les violations de sécurité.

9. source :https ://www.google.com/searchclient=operasxsrf=AB5stBhAdgQzySH3y4WLJNc6UPseAgs2pA :1688951639

# Conclusion

# Troisième partie

# Mise en œuvre

# Chapitre 3

# Mise en place d'un système de gestion des identités et des accès

## Introduction

## 3.1 Les étapes et les méthodes de la mise en œuvre du système de gestion des identités et accès

## 3.2 Les outils, les normes et les bonnes pratiques du système de gestion des identités et accès

## 3.3 Les facteurs de succès et les risques du système de gestion des identités et accès

## 3.4 le cahier de charge

pour élaborer notre cahier de charge(CDC),nous avons pris le cas de deux directions de l'ANSICE que nous avons étudié lors de notre stage au sein de l'institution :

- **la directions de la sécurité du système d'information(DSSI)** :Elle a pour mission de veiller a la sécurité des réseaux des communications électroniques et du système d'informations de l'État.Cette direction gèrent trois(3) autres sous directions qui sont :
  - **direction de service l'audit de sécurité du système d'information(SASSI)** :gère l'audit physique et logique du système d'information au sein l'ANSICE pour assurer la technologique
  - **Direction des service d'exploitation et de support technique(SEST)** :élaborer les planning des gestions et organisation des l'audit,les rapports de travail

- **la direction de service d'expertise et innovation(SEI)** :mis en oeuvre de la veille technologique du système d'information

— **gestion des ressources humaines(DRH)**

## 3.5 la politique de sécurité du système

Pour établir une politique de sécurité notre système,nous devons prendre le cas d'une gestion des identités et accès centraliser qui est tres efficaces avec l'évolution de la technologie qui lui même est devenu non seulement un moyen de la traçabilité,de preuve,de suivis de trafique des toutes informations qui circulent mais plutot aussi un systeme de protection avec l'évolution de la science technologie(comme intelligence artificielle,machine learning d'autres language de développement ),le block chaine.

## 3.6 Estimation budgétaire de la mise en place IAM

## Conclusion

la Bibliographie les references

# Bibliographie


[1] https ://www.onelogin.com/fr-fr/learn/iam

[2] https ://identitymanagementinstitute.org/identity-and-access-management-purpose-and-objectives/ ? gclid=CjwKCAjwp6CkBhB$_{E}iwAlQVyxcPVwyrVCicg_{V}5JyTnDjPZAf8CJ90tcJJL$ $s1OwwUmUgdUNs_{XSkBoC7rAQAvD_{B}wEhttps://www.netwrix.fr/data_{s}ecurity_{p}olicy_{t}emplate.html}$

[3] https ://www.vmware.com/fr/topics/glossary/content/identity-management.html

[4] https ://hal.science/file/index/docid/879556/filename/IAM$_{g}estion_{d}es_{i}dentites_{e}t_{d}es$ $https://www.sailpoint.com/fr/identity-library/identity-and-access-management/$

[5] https ://www.appvizer.fr/magazine/services-informatiques/gestion-acces/gestion-des-acces

[6] https ://fr.slideshare.net/danjelba2men/les-systemes-de-gestion-des-identites-et-des-acces-mise-en-uvre-et-apport-pour-la-securite-dune-organisation

[7] https ://docplayer.fr/1980347-M2-miage-gestion-des-identites-et-des-acces.html

[8] https ://www.academia.edu/9128109/S%C3%A9curit%C3%A9$_{i}nformatique_{P}rincipes_{e}t_{m}$%C3%A9$thode$ $titlehttps://fr.slideshare.net/MarcRousselet/les-processus-iam$

[9] https ://www.ibm.com/fr-fr/topics/identity-access-management

[10] https ://learn.microsoft.com/fr-fr/security-updates/security/20141615

[11] https ://docplayer.fr/1980347-M2-miage-gestion-des-identites-et-des-acces.html

[12] https ://www.pingidentity.com/de/platform/capabilities/extensibility.html

[13] https ://www.infosectrain.com/blog/why-choose-sailpoint-over-some-other-tool/

[14] https ://harmonie-technologie.com/cyberark-okta-pam/

[15] https ://www.oracle.com/security/identity-management/what-is-iam/ : :text=Oracle