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. yyyyyyyyyyyy(Rapporteur)

Sous la Direction de :

M.xxxxxxxxxxxx(Encadrant)

M.xxxxxxxx(Maitre de Stage)

année universitaire :2021-2022

Table des matières

Liste des tableaux

Table des figures

0.1 Résumé

Introduction Générale

Première partie

Présentation de la structure d'accueil et La définition des concepts et

Chapitre 1

Présentation de la structure d'accueil et la sécurité informatique

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

Direction de 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 systemes d'exploitation et les bases de données de l'ANSICE et en assurer les sauvegardes des régulières ;
- Assister les utilisateurs dans la maitrise 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

1.2 Les objectifs

- Concevoir et de mettre en œuvre les politiques de promotion de la cyber-sécurité 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 cyber-sécurité 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 cyber-sécurité et de la lutte contre la cybercriminalité ;

— Adopter un programme efficace de sensibilisation à la cyber-sécurité 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 ;

—

—

1.2.1 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 (ANSICE) ; 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**

1.3 Cadre du projet

1.3.1 context

1.3.2 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 ladite cible par étapes de manière stable.De disposer d'une solution commune à l'ensemble des Directions Métier 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 de pouvoir
- ❖ 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.
- ❖

1.3.3 Etude de l'existant

Les entreprises ont besoin d'un système IAM pour assurer la sécurité en ligne et augmenter la productivité de leurs collaborateurs.
Après une analyse de la situation nous avons remarqué que notre structure d'accueil ne dispose aucun système qui permet de gérer les identités et les accès des utilisateur. En termes de l'existant, notre structure d'accueil dispose d'un réseau local déployé permettant aux employés de se connecter sur le net.

1.3.4 Critique de l'existant

Les employés, des sous-traitants, des fournisseurs, des clients,ont besoin d'accéder aux systèmes et nécessitent donc leur identité 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

1.3.5 Proposition

Les investissements des entreprises dans des systèmes de sécurité de haute technologie, les mesures sophistiquées de sécurité de l'information pour garantir leurs identités,les utilisateurs existants peuvent ne pas être trompés par des pirates pour voler leurs informations d'accès :

- ❖ Identification des individues dans le système
- ❖ 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 le un certain degrés de privilège d'accès aux ressource système
- ❖ Gerer le privilège d'accès des utilisateur qui travail en télé travail
- ❖ Améliorer la productivité et les coûts récurrents de gestion et d'exploitation.
- ❖ créer et de gérer des identités dans une solution IAM au moyen de flux de travail simples en privilégiant l'automatisation de la gestion
- ❖ Etre capable, de désactiver l'ensemble des comptes et des accès d'un utilisateur qui vient de quitter la structure dans un temps court (inférieur à 24h).
- ❖ Intégrer les applications dans la solution IAM et définir le type de provisioning (manuel ou automatique) et d'authentification

Conclusion

Deuxième partie

Le système de gestion des identités et accès informatique

Chapitre 2

Le système de gestion des identités et accès informatique : définition, concepts et principes

Introduction

2.1 Le système de gestion des identités et accès

2.2 Les acteurs, les ressources et les processus impliqués

2.3 Les types et les niveaux d'identité et d'accès

2.4 Les concepts clés du système de gestion des identités et accès

2.5 Les principes fondamentaux du système de gestion des identités et accès

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

Conclusion

Chapitre 3

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

3.1 L'évaluation

3.1.1 Les critères et les indicateurs de l'évaluation du système de gestion des identités et accès

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

3.1.2 les impacts de l'évaluation du système de gestion des identités et accès

3.2 Les tendances et les évolutions du système de gestion des identités et accès

3.2.1 Les défis et les opportunités du système de gestion des identités et accès

3.2.2 Les recommandations et du système de gestion des identités et accès

Chapitre 4

La Gestion des identités et accés

Introduction

4.1 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

4.1.1 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

4.1.2 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.

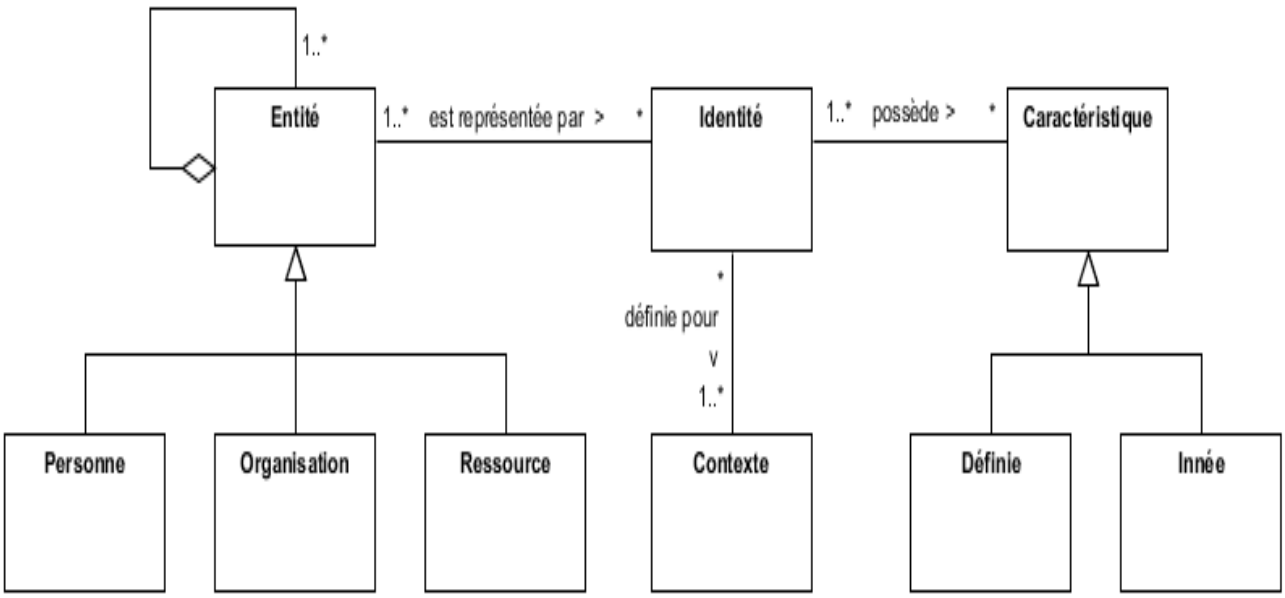

FIGURE 4.1 – Diagramme de classe du concept d'identité

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

4.1.3 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

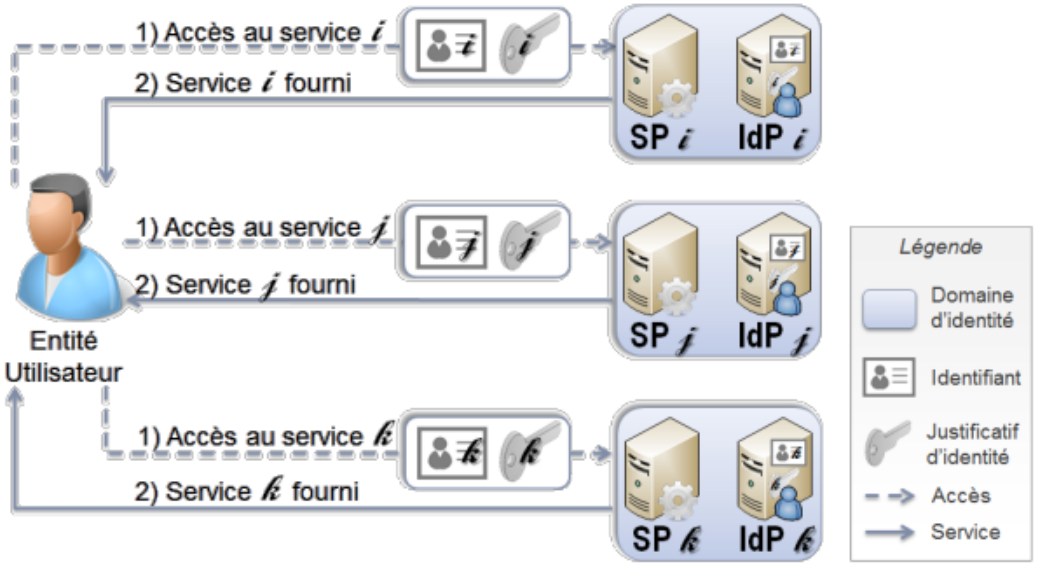

FIGURE 4.2 – Modèle de gestion d'identité isolée

4.1.4 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 un nom d'utilisateur et un mot de passe.

4.1.5 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.

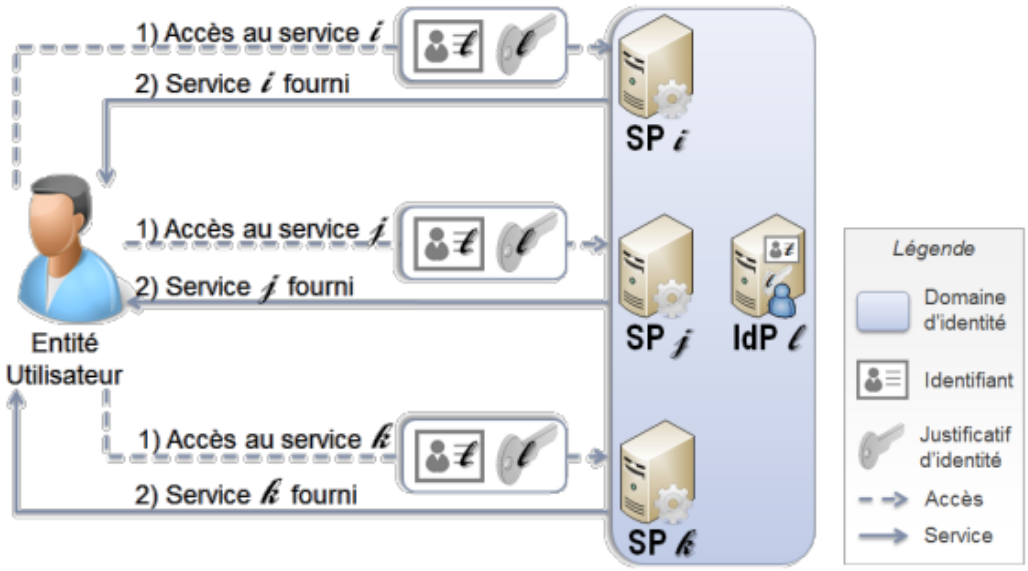

FIGURE 4.3 – Modèle de gestion d'identité isolée

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.

4.1.6 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.

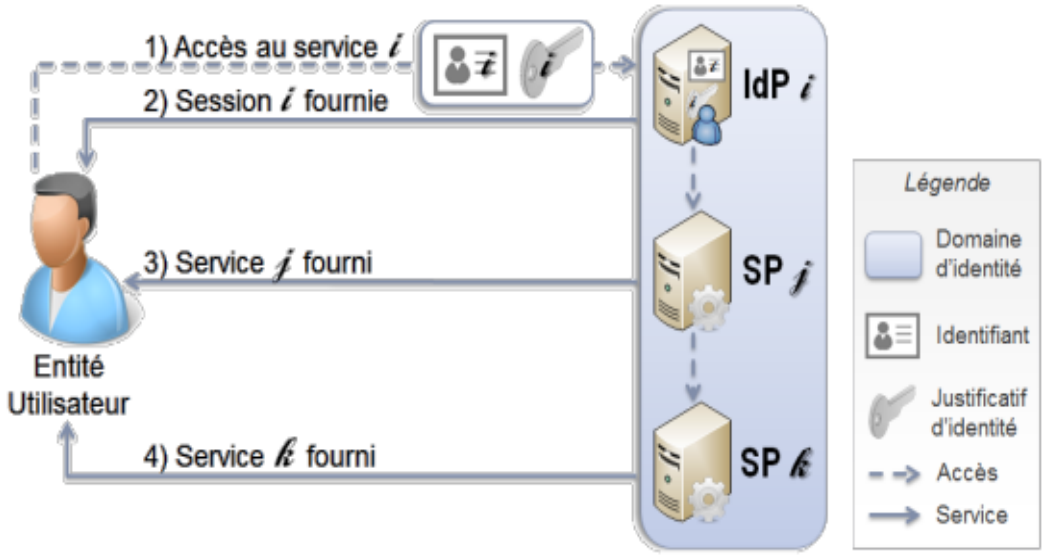

FIGURE 4.4 – Modèle de gestion d'identité :Single Sign-On

4.1.7 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.

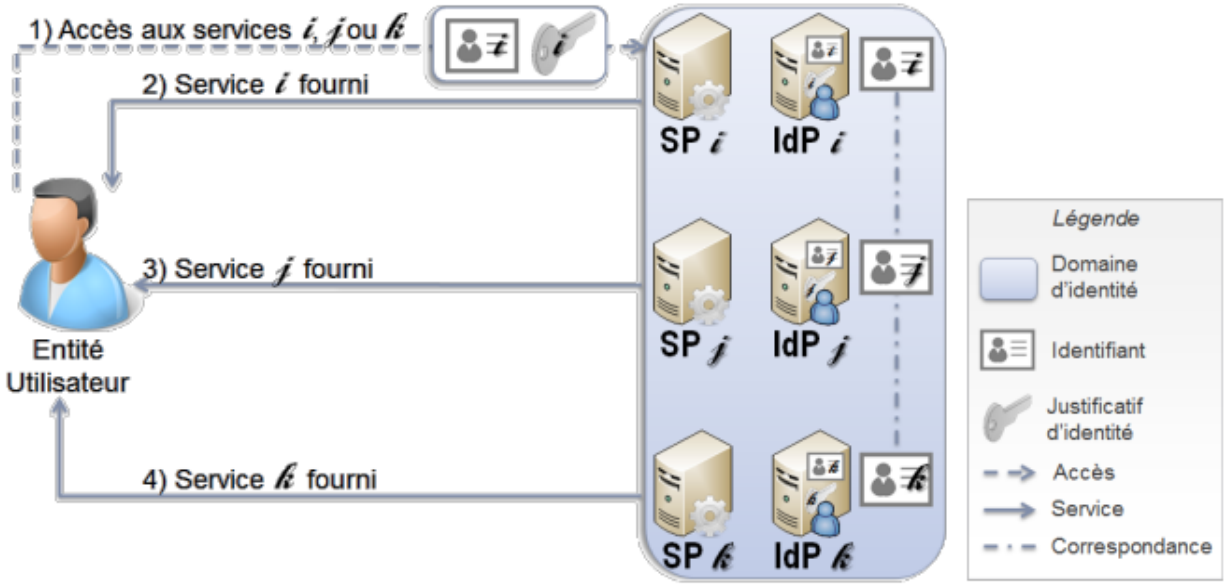

FIGURE 4.5 – Modèle de gestion d'identité fédéré

[1]

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

1. 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.

4.2 Gestion des accès

4.2.1 Définition

4.2.2 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.

4.2.3 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

4.2.4 Authentification et autorisation

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 reponse
    - 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

4.2.5 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

4.3 Les accés physiques et logiques

4.3.1 Les accés physiques

Conclusion

Troisième partie

Implémentation du système

Chapitre 5

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

Introduction

5.1 la politique de sécurité du système

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

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

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

5.5 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)**

5.6 Cartographie fonctionnelle

La phase de recueil des besoins a permis de mettre en évidence des besoins récurrents qui peuvent pris en charge facilement par les outils existants.la liste des besoins n'est pas exhaustive. Cependant, cela a permis d'entrevoir les priorités et ainsi d'établir le périmètre de la présente étude de faisabilité. Les cas d'utilisation sont répertoriés par catégorie d'utilisateur d'un système d'information de gestion des identités et des accès, puis par type de finalité.

Administrateur

1. Gérer les accès
   - Attribuer un rôle
   - Révoquer un rôle
2. Gérer les comptes
   - Créer un compte d'après une fiche agent non finalisée
   - Créer un compte temporaire
     - ☛ Définir une date de fin
     - ☛ Automatiser la désactivation
   - Réactiver un compte existant
   - Modifier les informations
   - Propager les modifications
   - Annuler les modifications
3. Gérer les rôles
   - Déléguer un rôle
   - Attribuer un rôle à un agent sur une période limitée
   - Attribuer un rôle à un agent sur une période limitée

Auditeur

1. Identifier les comptes génériques
2. Visualiser les modifications d'information
3. Identifier les comptes anonymes
4. Visualiser les journaux d'accès
5. Visualiser les activités

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$_{g}estion_{d}es_{i}dentites_{e}t_{d}es$