Institut National des Sciences Appliquées Toulouse

Département de Génie Électrique et Informatique

Projet de Fin d'études

Spécialité : **Informatique-Réseaux**
Filière : **Sécurité des Systèmes d'Information**

Gestion des identités et des accès

Auteur :
ANSER - Omar

Entreprise :
Digital Security

Référent INSA :
Alata - Eric

Responsable du stage :
GONDOUIN - Hicham

Année 2019-2020

Résumé

Ce document restitue mes missions professionnelles effectuées au sein de l'agence Occitanie à Labège (Toulouse – 31) de la société Digital Security. Ce stage s'est déroulé du 15 Mars 2020 au 15 Septembre 2020. Vu la situation sanitaire qu'a traversé le monde durant cette période, le stage a été effectué en grande partie en télétravail. Plus de détails sur le déroulement du stage sont donnés dans le chapitre Introduction.

Digital Security est une société crée en 2015 et née de la fusion du CERT « Digital Security » et de la société Cyber Security issue du regroupement des sociétés Altasys et Clesys. Digital Security développe deux grands types d'activités :

— L'évaluation sécurité et la labellisation des objets connectés pour des industriels et des start-ups.

— L'évaluation et la mise en œuvre de politiques de sécurité au sein des entreprises.

L'agence Occitanie créée en 2018 est en phase de développement sur la région. Cette phase s'accompagne d'une part par des recrutements et d'autre part par l'établissement d'offres autour de la cybersécurité.
Le présent document est composé de quatre chapitres :

— Un chapitre d'introduction générale sur le sujet du stage et une présentation générale du rapport.

— Un chapitre sur le cadre et les objectifs du stage.

— Un chapitre réalisation qui contiendra plusieurs sous chapitres et qui traitera de la réalisation de mes missions professionnelles au sein de Digital Security et des points que j'ai approfondis en rapport avec le sujet du stage.

— Une Conclusion

Mots-clés : Identité numérique, CIAM, IDaaS, biométrie, DCP, réglementation, architecture sécurisée, produits IAM, reconnaissance faciale, usurpation d'identité, Blockchain, DLT.

Remerciements

Je tiens tout d'abord à remercier Eric Alata pour l'intérêt qu'il a porté à mon projet ainsi que les conseils qu'il m'a prodigués pour l'organisation et l'écriture de ce rapport. Je tiens à remercier l'équipe Digital Security de l'agence Occitanie pour la contribution à la réalisation de mon stage qui constitue mon projet de fin d'études.

Ce stage vient finaliser ma cinquième année à l'INSA de Toulouse (période septembre 2019-septembre 2020), dans la spécialité « Sécurité des Systèmes d'Information ». L'enseignement théorique et pratique sur la sécurité informatique m'ont permis d'élargir et approfondir mes connaissances et compétences dans ce domaine. C'était mon souhait de m'orienter à la fin de mes études vers un domaine d'avenir pour de nombreuses entreprises impliquées dans la transformation digitale de leur processus.

Le stage m'a permis de me focaliser sur un aspect particulier de la sécurité : la gestion des identités et des accès. Au fil des pages de ce rapport seront développés des aspects théoriques, techniques, fonctionnels, les enjeux de la gestion des identités et des accès ; le tout illustré par des cas d'entreprises.

Je tiens à remercier les personnes sans qui ce stage n'aurait pas été possible :

— Hicham GONDOUIN responsable de l'agence Occitanie en tant que tuteur pour ses conseils et sa bienveillance surtout en début de stage durant la période compliquée qu'a connu le monde.

— Thibault FEQUENT consultant sécurité de Digital Security Occitanie pour sa formation technique sur le sujet et son aide durant mes missions.

— Eric Alata en tant que tuteur INSA pour son aide et ses retours.

— Thibault, Faïçal, Anass, Elodie, Patrice et tous ceux que je n'ai pas cités, mais qui ont concouru à un moment donné au bon déroulement et à l'avancement du stage.

Je remercie également :

— La promotion 2019-2020 INSA Toulouse pour la bonne ambiance et la dynamique de groupe.

Table des matières

Acronyme	Signification	Acronyme	Signification
API	Application Programming Interface	SAAS	Software as a Service
ARA	Auvergne Rhone Alpes	SAML	Security Assertion Markup Language
ANSSI	Agence Nationale de la sécurité des SI	SI	Système d'Information
AWS	Amazone Web Services	SP	Service Provider
B2B	Business to Business	SSI	Sécurité Système d'information
B2C	Business to Customer	SSO	Single Sign-On
BATX	Baidu, Alibaba, Tencent et Xiaomi	STS	Security Token Service
BYOD	Bring Your Own Device	URI	Uniform Resource Identifier
CIAM	Customer Access Identity Management	URL	Uniform Resource Locator
CLUSIF	Club de la sécurité de l'information Francais	WS	Web-services
CRM	Customer Relationship Management	XML	Extensible Markup Language
CXM	Customer Experience Management		
DCP	Données à caractère personnel		
DL	Deep Learning		
DNS	Domain Name Service		
DS	Digital Security		
GAFA	Google, Apple, Facebook et Amazone		
GED	Gestion électronique des documents		
GIA	Gestion des identités et des accés		
GRC	Governance, Risk management and Compliance		
HTTP	HyperText Transfer Protocol		
IA	Intelligence Artificielle		
IAaS	Infrastructure As a service		
IAM	Identity ans access management		
IDAAS	Identity as a service		
IDP	Identity Provider		
IETF	Internet Engineering Task Force		
IGA	Identity Governance and Administration		
IOE	Internet of Everything		
IOT	Internet of Things		
MCD	Modèle Conceptuel des Données		
MDM	Mobile Device Management		
MFA	Multi Facteurs Authentification		
ML	Machine Learning		
OTP	One Time Password		
PAAS	Plateform as a Service		
PAM	Privileged Access Management		
POC	Proof of Concept		
RPA	Robotic Process Automatisation		
RSSI	Responsable de la sécurité des systèmes d'information		
RT	Responsable de Traitement		

Chapitre 1

Introduction

1.1 Déroulement du stage

Etant donné la situation sanitaire dans laquelle se trouvait la France en début du mois de Mars 2020, le gouvernement français avait imposé un confinement total obligatoire et strict. Les nouvelles règles exigeaient de mettre en œuvre le télétravail pour toute entreprise voulant continuer son activité durant cette période. C'est ce qui a été appliqué par l'agence Digital Security de Toulouse. Ainsi, pendant la période de confinement du 17 mars 2020 au 11 mai 2020, mon stage s'est déroulé entièrement en télétravail. Digital Security a choisi de prolonger cette méthode de travail jusqu'au 11 Juin, jour à partir duquel a commencé un déconfinement progressif .

Mon premier jour de stage devait se dérouler à Paris afin de faire connaissance avec l'équipe RH et récupérer un PC Portable de travail configuré pour la réalisation de mes missions. Ce déplacement a été annulé à la dernière minute et j'ai dû effectuer cette procédure à distance. J'ai reçu mon PC portable par voie postale une semaine après la date du début de mon stage. J'ai fait connaissance avec mes collègues via la plateforme collaborative de Microsoft Teams. L'agence de la région Occitanie est jeune et est constituée essentiellement de consultants Sécurité. L'ambiance sur Teams était à la fois décontractée et studieuse. Durant la première semaine, j'ai eu l'opportunité de me former sur les technologies de Microsoft et sur les solutions logicielles proposées par Microsoft pour les entreprises. L'autre aspect que j'ai pu découvrir durant cette première semaine est le rôle d'un consultant sécurité informatique en entreprise.

1.2 Sujet et contexte général

Contenu de la situation particulière qu'a connu mon début de stage et l'obligation du télétravail sans aucun préavis, mon sujet de stage à subi un changement. En effet, le sujet initial voulait que je travaille sur la sécurisation des données stockées dans le Cloud et sur les technologies de sécurité du Cloud que propose Microsoft, Google et Amazon. Néanmoins, le contexte de cette période a amené l'agence Digital Security de Toulouse à s'adapter et à se concentrer sur des projets prioritaires. Les projets liés à mon sujet de stage ont été interrompus et certains de mes collègues ont dû recourir au chômage partiel. Un autre sujet m'a donc été proposé portant sur la gestion des identités et des accès, et une présentation du client et de l'environnement technique m'a été faite (nom du client que je n'ai pas droit de citer dans ce rapport).
Pour retrouver mon sujet de départ, il était nécessaire qu'il y ait un retour à la normale. La première étape de mon sujet initial était de passer la certification Microsoft MS-500. Les candidats à cet examen mettent en œuvre, gèrent et surveillent les solutions de sécurité et de conformité pour Microsoft 365 et les environnements hybrides. J'ai pu ainsi me concentrer sur cette partie à la fin du mois de Juillet, date à laquelle les choses ont repris leur cours quasi-normal.
Je me suis positionné sur ce nouveau thème pendant les premiers mois de mon stage car je voulais approfondir le sujet « IAM ». L'IAM et le PAM sont des sujets très présents chez Digital Security. Cela fait partie de la culture de l'entreprise puisque c'était la spécialité d'une des deux sociétés impliquées dans la création de Digital Security. Mon tuteur d'entreprise m'a laissé assez de liberté et j'ai pu, en parallèle de la formation que j'ai suivi sur une solution IAM de Microsoft qu'un de nos client utilise, faire un état des connaissances sur ce domaine et profiter des retours des consultants sur ces sujets ou sur des sujets liés à la cybersécurité. Ainsi, des parties sur les principes de la gestion des identités et des accès, une recherche des produits disponibles sur le marché avec leurs catégories et enfin une analyse des tendances en cours dans le secteur de la gestion des identités et des accès sont présentés dans le troisième chapitre.
Un système de gestion des identités est une branche de la technologie de l'information qui régit la manière dont les technologies numériques peuvent être utilisées pour la gestion des identités d'entreprise[1].
Le choix technique que notre client avait décidé d'utiliser (et cela avant notre collaboration) pour administrer et gérer les comptes utilisateurs et les ressources du réseau de l'entreprise était Microsoft Identity Manager (MIM). MIM aide à gérer les utilisateurs, les informations d'identification, les stratégies et les accès au sein d'une organisation. En outre, MIM 2016 ajoute une expérience hybride des fonctionnalités de gestion des accès privilégiés et la prise en charge de nouvelles plateformes. Microsoft Identity Manager (MIM) 2016 s'appuie sur les fonctionnalités de gestion des identités et des accès de Fore-

front Identity Manager (FIM).
L'architecture technique de l'annuaire d'entreprise est présentée dans le troisième chapitre. Sa description comprendra :

— Une présentation générale de l'annuaire d'entreprise

— La description des services fonctionnels

— L'architecture fonctionnelle

— L'architecture technique

J'aborderai à la fin du troisième chapitre dans sa partie « IAM », la gestion des identités et des accès basée sur l'utilisation de la Blockchain et les solutions et tendances pour une application en entreprise. À première vue, il pourrait sembler que la Blockchain n'a rien à voir avec l'IAM. Mais il y a deux aspects de la Blockchain et des technologies connexes qui ont un sens dans le contexte de l'IAM :

— L'identité auto-souveraine

— Piste d'audit

Ces deux points seront approfondis dans le troisième chapitre.
Je voulais ainsi inclure dans ce rapport une partie orientée recherche car c'est un domaine qui me passionne.

1.3 Planning et réalisations

La figure 1.1 présente le planning que j'ai suivi pendant mon stage qui s'est partagé entre recherches, formations, mises en pratique et cas d'entreprise.

	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24	S25	S26	S27
Formation technique environnement Microsoft																											
Principes, solutions et tendances IAM																											
Formation technique MIM																											
Réalisation technique MIM pour le client																											
Préparation certification MS-500																											
Création d'outils d'audit Azure - Docker																											

Table 1.1 – Planning stage Digital Security

Quelques détails sur les principaux sujets que j'ai pu traiter pendant ce stage (tableau 1.2)

Réalisations	Commentaires
• Analyse des solutions • Principes IAM • Tendances IAM	- Rapport sur les tendances IAM actuelles, les différents types de solutions du marché et leur positionnement - Recherche des documents de référence (Gartner, Kuppingercole, Forrester, TechVision Research) - Analyse de produits et critères identifiés : fichier de sélection des produits - Etudes « Techvision » et « Forrester » pour l'analyse des tendances - Etude des différentes architectures (On premise, Hybride, Cloud)
• Architecture CLOUD	- Cloud Azure, AWS et Google
• MIM 2016	- Formation et réalisations techniques
• Certification MS-500	- Microsoft 365 Security Administration

TABLE 1.2 – Réalisation

1.4 Méthodologie

1.4.1 Analyse des solutions et tendances IAM

L'analyse des produits a été faite sur la base des analyses « Kuppingercole » [30] suivantes :

— Access governance et Intelligence (juin 2018)

— Access management et fédération (février 2019)

— CIAM Plateforms (décembre 2018)

— IdaaS : Single Sign-On to the Cloud (Juin 2017)

J'ai commencé par établir une première liste de produits et une analyse synthétique basée sur les documents. Les critères techniques n'ont pas été les seuls points de l'analyse, j'ai également pris en compte des critères comme la réputation de l'entreprise, sur quelle zone graphique l'entreprise est présente et comment elle était perçue par Digital Security.
L'analyse des tendances a été effectuée sur la base des documents suivants :

— « The Future of Identity Management (2018-2023) » du cabinet « TechVision Research »

— « The Future Of Identity And Access Management » du cabinet « Forrester »

1.4.2 Analyse des solutions IAM basées sur la Blockchain

Pour effectuer cette analyse, je me suis intéressé à 11 approches avec differents niveaux de perfectionnement et de disponibilité.

Chapitre 2

Cadre et objectifs du stage

Mon stage a démarré le 16 Mars 2020, l'offre de stage qui m'a été proposée mentionne un poste de consultant en sécurité des systèmes d'informations et couvre un large champ d'activités :

— Audits techniques

— Protection des infrastructures (design d'une architecture sécurisée...)

— Protection des identités, des accès et des données (mise en œuvre de solutions de sécurité, design, implémentation...)

Cela signifie que je n'ai pas eu de spécialité prédéfinie, ce qui en soit m'a plu car j'ai pu exercer un ensemble d'activités différentes. Ainsi, pendant les premiers mois de mon stage, je me suis concentré sur la partie gestion des identités et des accès (IAM).
Mon tuteur m'a inclus dans un projet IAM et m'a proposé des formations sur les solutions techniques utilisées dans ce projet. Cela a été la méthodologie que j'ai suivi durant ce stage, c'est à dire qu'avant de pouvoir participer efficacement aux différentes missions, je suis passé par une première étape d'exploration du projet qui consistait à comprendre le contexte du projet puis éventuellement à monter en compétence sur les solutions utilisées en parcourant de la documentation, qu'elle soit fournie par le client, par mes collègues ou par le propriétaire de la solution. Ce travail d'auto-formation est requis pour pouvoir travailler efficacement. De plus, il ne se limite pas à de la documentation technique mais peut se baser sur de la documentation commerciale comme les propales commerciales pour comprendre le besoin du client.
Je me suis également familiarisé avec de nouveaux vocabulaires qui sont liés au domaine de la gestion de projet et au domaine commercial. Je me suis imprégné de ces enseignements pour ensuite écrire à mon tour de la documentation à destination du client que cela relève du volet technique, par exemple un document d'architecture technique, des documents d'exploitation de solutions.
Mon stage était donc, par le biais de projets et de missions, une longue formation (technique et méthodique) au métier de consultant sécurité informatique.

Dans ce qui suit, je vais aborder une présentation du projet IAM, son contexte métier, les domaines scientifiques traités et les objectifs fixés pour ce projet. Je décrirai dans la section suivante la problématique de recherche que j'ai étudiée en suivant les mêmes points que la première section.

2.1 Projet IAM

2.1.1 Présentation

La première mission à laquelle j'ai participé est une mission IAM pour le compte d'un client du secteur de l'aéronautique. l'IAM est un processus qui permet d'adapter les droits d'accès ou les habilitations des utilisateurs de l'entreprise en fonction de leur rôle de leur fonction ou de leur responsabilité hiérarchique. Digital Security a repris ce projet après que notre client ait décidé de changer de sous traitant. Je suis arrivé sur ce projet quelques mois après que DS ait gagné ce contrat. Le client disposait d'un annuaire centralisé reposant sur 3 composants :

— La gestion des identités portée par la solution IAM MIM

— Des annuaires ADLDS contenant l'ensemble des utilisateurs synchronisés

— Des applications Web pour la visualisation et l'administration des informations utilisateurs

La prestation Tierce maintenance applicative (TMA) arrivait à son terme et le client souhaitait procéder à son renouvellement. L'objectif était donc de choisir un prestataire qui gérera le Maintien en condition opérationnelle (MCO), les correctifs et le développement des évolutions. Un des objectifs du client pour ce projet est d'utiliser au maximum les fonctionnalités des logiciels afin de minimiser les développements. Il fallait limiter au maximum les développements spécifiques et privilégier les fonctionnalités natives des solutions. Il était aussi impératif que tout code développé réponde aux besoins sans augmenter les coûts de possession et même, lorsque cela est possible, en les diminuant. L'ensemble des éléments de l'annuaire d'entreprise était à prendre en compte.
Pour mener à bien ce projet dès son début, Digital Security avait prévu quatre phases :

— Appropriation

— Lancement

— Construction

— Traitement

Je suis arrivé lors du début de la phase de traitement.
J'ai pris connaissance de tous les détails des précédentes phases afin, dans un premier temps, de pouvoir me mettre à niveau sur ce qui a déjà été fait sur ce projet, mais aussi

d'acquérir des notions sur la gestion d'un projet depuis son démarrage.
La phase d'appropriation (phase qui pose les fondements du projet) avait pour objectif d'assurer la cohérence globales des méthodes et outils, de prendre connaissance des règles techniques et fonctionnelles mise en place, la création d'un environnement Iso-fonctionnel, de définir les indicateurs de pilotage et enfin de garantir au client une transition sans perte de connaissances et un service opérationnel dès le démarrage. Pour atteindre les objectifs de cette phase, des ateliers avec le prestataire sortant ainsi qu'une étude de la dernière mise à jour de la documentation ont été faits.
Les phases lancement et construction faisaient suite à la phase d'appropriation, elles mettaient en oeuvre, techniquement, les objectifs fixés lors de la phase d'appropriation. Ainsi, une initialisation organisationnelle, une initialisation technique et la création de l'environnement iso-fonctionnel étaient les points clés de ces étapes.
La figure 2.1 résume ces démarches.

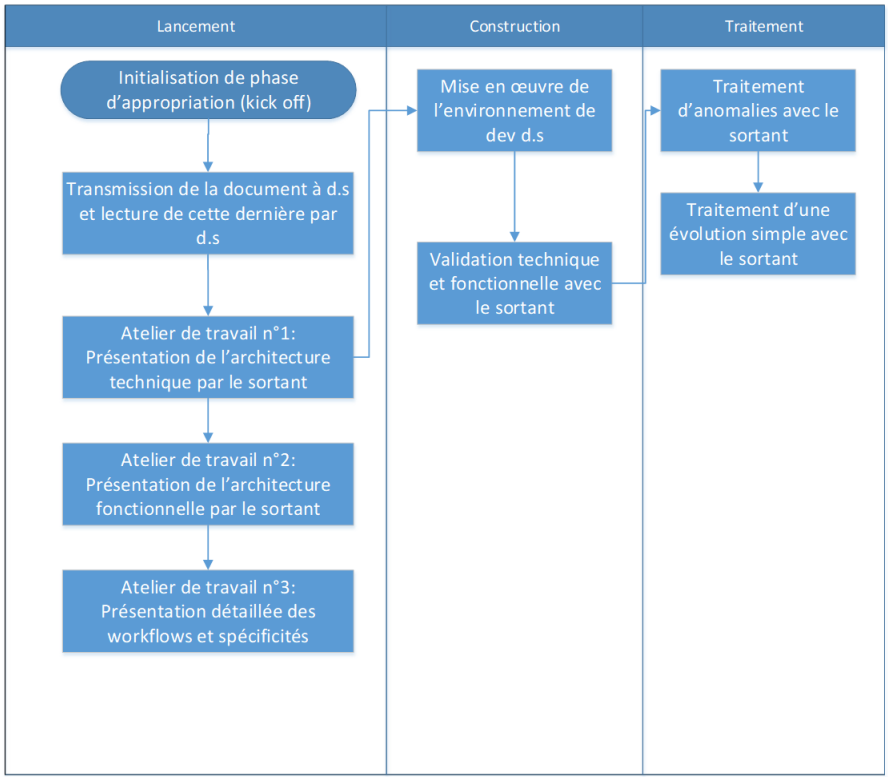


FIGURE 2.1 – Phases projet client

Le cœur du dispositif pour ce projet est basé à Toulouse. Un dispositif de débordement est prévu, les consultants sécurités des autres agences de Digital Security pourront renforcer l'équipe en cas de besoin.
Le produit IAM qu'avait préalablement décidé d'utiliser notre client est MIM 2016[38] de Microsoft. Son choix s'est porté sur cet outil car ce dernier répondait le mieux à ses besoins métiers. En effet, les enjeux recherchés par le client au moment où il avait commencé son

projet de Gestion des Identités et des Accès (GIA) était multiples comme le montre le tableau 2.1 :

Enjeux	Commentaires
Sécurité	Gestion des droits d'accès au plus près du métier Maîtriser la forte mobilité des agents et les multi-rôles au sein de l'organisation
Gouvernance	Traçabilité et correction des accès : pouvoir auditer et passer en revue les habilitations pour les utilisateurs. Maintenir un référentiel des rôles métiers, profils, droits d'accès
Humains	Simplifier l'attribution de droits d'accès lors d'arrivée/mutation départ d'utilisateurs et éviter les temps d'attente

TABLE 2.1 – Enjeux liés à la mise en place de l'outil IAM

Digital Security a modélisé les flux par attributs et par connecteur et a effectué une comparaison entre les deux environnements afin de s'assurer de la bonne configuration. Les éléments différenciants ont fait l'objet d'un suivi afin d'éviter des erreurs lors de la transmissions d'une évolution.

2.1.2 Organisation et démarche

J'ai intégré l'équipe IAM qui était composée de mon tuteur de stage et de moi même. Digital Security avait comme mission de maintenir l'infrastructure MIM 2016 et de faire évoluer le système selon les besoins du client. Ainsi, Nous recevions chaque semaine, via un outil de ticketing JIRA, une description des améliorations à apporter à l'outil. Les missions pouvaient être assez simples à réaliser ne demandant que peu de connaissances techniques (Changer le rôle d'un membre de l'équipe France, modifier les caractères autorisés dans un Distingue Name ...), d'autres par contre exigeaient des notions techniques avancées de l'outil MIM 2016 et l'utilisation d'un langage de programmation (C#) pour implémenter les solutions demandées.
Afin de mener à bien les missions confiées, l'équipe IAM avait préalablement créé un environnement de test répliquant ainsi dans les grandes lignes l'architecture technique du client. N'ayant pas d'expérience préalable sur cet environnement technique, l'objectif qui m'a été assigné en premier lieu a été de me former et de monter en compétence sur MIM 2016. Pour cela, une documentation m'a été fournie par mon tuteur (Microsoft Identity Manager 2016 Handbook) accompagnée d'une formation proposée par le site Alphorm d'une durée de 12 heures.
En parallèle de cette formation, j'ai réalisé un état de l'art sur les solutions et tendances IAM. L'objectif était de faire des recherches ciblées et approfondies de toutes les informations préexistantes concernant les solutions et tendances IAM utilisées dans l'industrie.

En complément de cela, et grâce à des retours d'expériences des consultants de Digital Security, j'ai pu acquérir des notions sur la démarche à suivre sur un projet orienté gestion des identités et des accès en partant du début. En effet, implémenter une solution IAM sur des systèmes d'information de très grandes tailles est une chose assez complexe et le fait d'avoir pu en discuter longuement fut très enrichissant.

2.2 Problèmatique de recherche : IAM et *Blockchain*

2.2.1 Présentation

En m'intéressant aux solutions IAM du moment, j'ai été interpellé par le fait que la majorité de ces solutions utilise un système centralisé. Par exemple, le Lightweight Active Directory Protocol (LDAP), qui est le protocole d'interrogation et de modification des services d'annuaire le plus utilisé en entreprise, enregistre les données utilisateurs dans une base de données de l'entreprise. Vu que le temps le permettait, je me suis intéressé à une autre manière de faire en prenant comme principal critère la faisabilité de la chose pour un système d'information avec les exigences et contraintes d'une entreprise d'assez grande taille. D'article en article (c.f bibliographie), une technologie que l'IAM pourrait adopter pour résoudre ses problèmes actuelles, ressortait le plus souvent. Cette technologie est la *Blockchain*. A l'origine, la *Blockchain* a été développée pour résoudre un problème particulier : interdire la «double dépense» de la crypto-monnaie sans administrateur central [2]. Mais cette dernière a un meilleur potentiel. L'idée d'utiliser cette technologie est venue d'une alternative pour l'IAM actuel qui est le concept d'auto-souveraineté de l'identité, qui redonne le contrôle des données personnelles à l'utilisateur final. Une autre alternative est le remplacement d'un service d'identité central détenu par une seule entreprise ou par une solution multipartite régie par le réseau détenue par une coentreprise ou par un consortium. Ces deux solutions sont essentiellement basées sur la technologie *Blockchain*.

2.2.2 Organisation et démarche

Durant ma formation à l'INSA, stage compris, j'ai eu l'occasion de réaliser des états de l'art sur des sujets de la sécurité informatique. Ces différentes expériences m'ont appris la méthodologie à appliquer pour effectuer un tel travail. Ainsi, la première étape a consisté à établir une liste de mots clés, à collecter des éléments bibliographiques et à les sélectionner. La constitution des mots clés est faite en allant du général au spécifique. Ensuite, vient l'étape de la lecture approfondie et de la critique des références. le dernier exercice à faire est la synthèse. La préparation d'un bon état de l'art exige non seulement une capacité à sélectionner les articles, les brevets et les travaux de R&D les plus pertinents, mais aussi une capacité à comprendre ces travaux et à les analyser de façon à en tirer des critiques constructives (avantages, inconvénients, verrous scientifiques et technologiques).

Pour revenir au sujet qui est ce que peut apporter la *Blockchain* à l'IAM, fondamentalement, les problèmes inhérents à la crypto-monnaie peer-to-peer comme le *Blockchain* sont différents de ceux de la gestion des identités et des accès ; ces différences doivent être comprises avant de tenter de faire correspondre les technologies *Blockchain* à IAM.

Chapitre 3

Réalisations

3.1 Principes fondamentaux, solutions et tendances IAM

3.1.1 L'identité numérique socle de la gestion des identités et des accès

Nous sommes en 2002 sur un grand site industriel d'une société Française de la filière Nucléaire. Un projet d'harmonisation du Système d'Information vient d'être lancé. Il s'agit de centraliser et gérer les identités dans un référentiel standard accessible aux applications. Le service annuaire alimenté par un flux RH permettra d'avoir des données à jour et devra refléter :

- Tout mouvement de personnel (arrivée, mutation, départ, ...)
- Fournir la valeur d'un attribut identité en réponse à une application en faisant la demande
- Permettre la localisation de toute personne afin de faciliter les échanges au sein des métiers et des directions transverses
- Servir de base au « Single Sign On » pour l'accès aux applications

Ce premier projet de gestion des identités va durer deux ans et aboutir aux mises en place d'un annuaire d'entreprise LDAP et d'une infrastructure applicative basée sur un socle J2EE. Il aura cependant fallu faire face à d'importantes difficultés techniques, à l'incrédulité de certains quant à la réalisation du projet (ça ne marchera jamais...), à l'accompagnement des changements liés aux nouvelles technologies, au dépassement du budget liés au projet (conception, nouvelles technologies, développements coûteux) et aux remises à plat de certains processus.

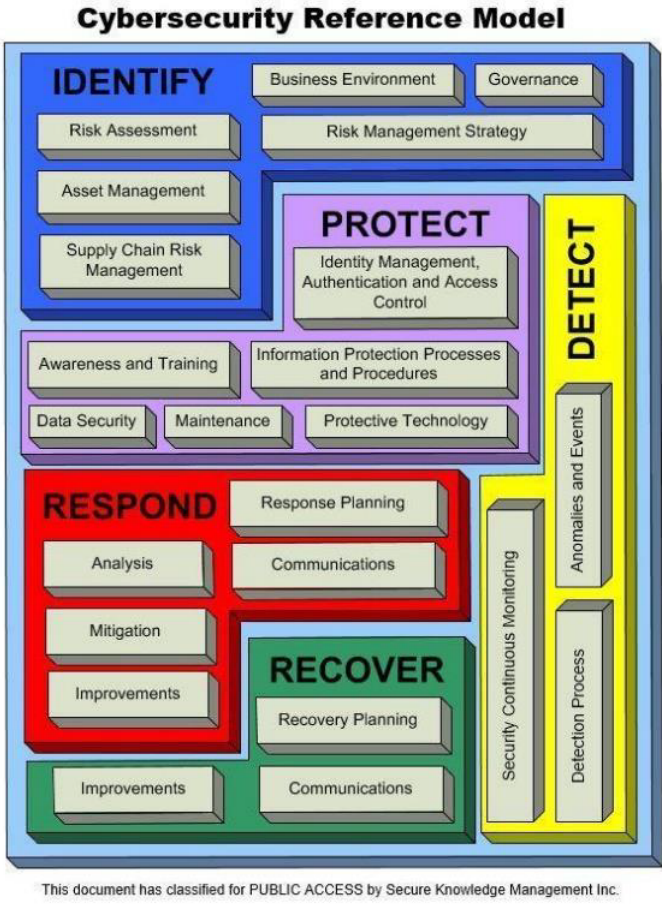


FIGURE 3.1 – IAM dans le modèle de référence Cybersécurité

Les problématiques de l'époque sont toujours d'actualité mais l'environnement n'est plus le même. L'IAM fait face aujourd'hui à de nouveaux défis : le Cloud, la mobilité, les objets connectés et les nombreuses obligations de conformité imposées par la législation et les normes industrielles.

Le système d'information qui était cloisonné et centré sur lui-même se retrouve non seulement ouvert aux employés mais également aux clients et partenaires.

La sécurité mode « château fort » n'est plus de mise, l'entreprise doit s'adapter à l'ouverture avec un modèle de sécurité plus adapté.La gestion des identités et des accès devient un maillon essentiel pour la protection des accès aux différentes ressources du SI. Aujourd'hui les données d'identités peuvent être hébergées dans le Cloud et synchronisées avec des référentiels « On Premise »[32]. La tâche de l'IAM s'est complexifiée et a imposé l'apparition d'une nouvelle génération de solutions accèes sur le Cloud et sur le client. L'adoption des infrastructures de Cloud public s'accélère et amène son lot de problèmes de sécurité. Plusieurs fuites de données majeures ont fait ressortir des lacunes dans la sécurité IaaS et PaaS des entreprises. L'analyse du « Center for Internet Security » pour « AWS » montrent que 71,5 % des violations concernant le cloud Amazon AWS ont trait à la gestion des identités et des accès ! Viennent ensuite la surveillance avec 19,0 %, le

réseau avec 5,9 % et enfin la journalisation avec 3.6%.
Comment dès lors gérer et gouverner efficacement les identités au travers de plusieurs systèmes, applications et environnements ? Une gestion des identités et des accès rigoureuse associée à de bonnes pratiques d'authentification et d'habilitations semblent essentielles pour garantir la confiance et la protection contre les cyberattaques et fraudes. Comme le montre la figure 3.2, l'IAM constitue le socle de base de la protection des SI et son rôle est primordial.

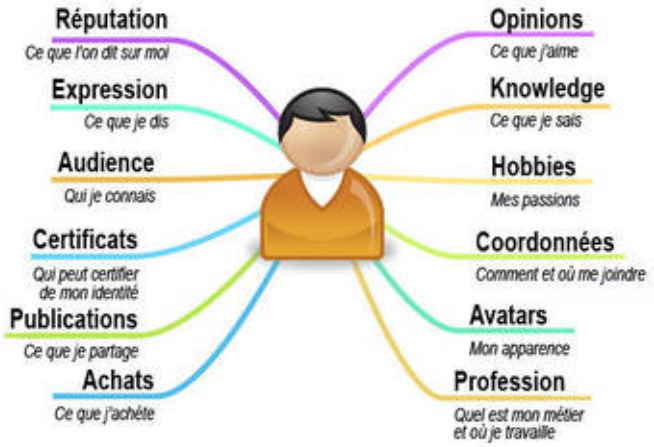


FIGURE 3.2 – IAM dans le modèle de référence Cybersécurité

3.1.1.1 Identité

Dans l'article « Trust Requirements in Identity Management » [32], l'identité est définie comme « un ensemble de caractéristiques propres par lesquelles une personne ou une organisation est connue ou reconnue. Ces éléments peuvent être définis, comme le nom, l'adresse, la nationalité, ou peuvent être innés comme les empruntes digitales. Pour l'identité d'une organisation, les caractéristiques sont acquises ».
Le standard international ISO/IEC 24760-1[3], basé sur la recommandation UIT-T Y.2720 rédigée par l'Union Internationale des Télécommunications, étend la définition d'identité à l'« information utilisée pour représenter une entité dans un système d'information et de communication ». Une entité représente une personne physique ou morale (organisation, entreprise, ...), une ressource (un objet tel qu'un matériel informatique, un système d'information ou de communication) ou un groupe d'entités individuelles.

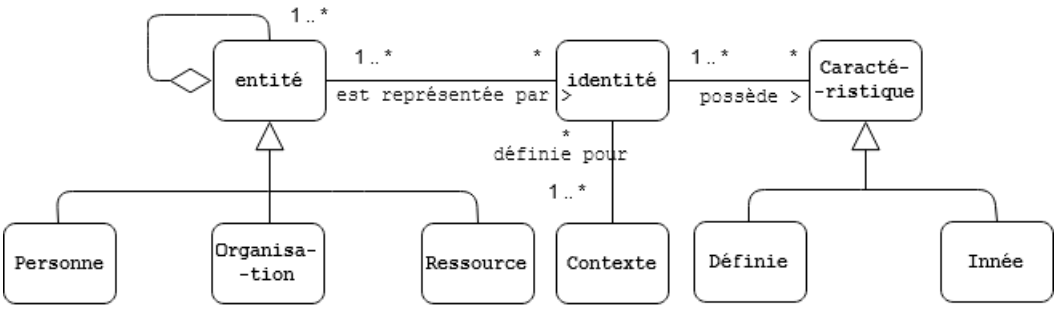


FIGURE 3.3 – Pseudo diagramme de classe du concept d'identité

Une identité numérique [31] peut être définie par une organisation externe (administration, banque en ligne, etc.) ou être composée librement par une personne (réseau social). L'identité numérique est le socle de toute démarche d'authentification et permet le contrôle de la connexion et l'accès aux services. Elle peut de ce fait exposer son propriétaire à des risques d'usurpation car la sécurité est fluctuante d'un service à l'autre.
Comme dans la vie réelle, l'identité numérique est un mélange entre « ce que je montre, ce que je cache, ce que les autres perçoivent et ce qui m'échappe ». Elle se construit au fur et à mesure des interactions accomplies sur Internet et renseigne de manière fragmentaire nos centres d'intérêts, relations, activités et points de vue disséminées dans nos multiples identités. L'identité numérique est unique pour un service donné et fournit des informations sur son détenteur regroupées dans des profils qui sont une combinaison d'attributs propre à chaque entité (personne, application, machine). Ces attributs sont constants (nom, prénom, profession, sexe), variables (login, mot de passe, adresse IP, adresse électronique), liés ou non à l'identité réelle. Ils peuvent faire partie des données à caractère personnel et donc soumis à la réglementation. Les facteurs de contrôle de l'identité appartiennent à trois catégories : « ce que l'on sait » (mot de passe...), « ce que l'on a » (badge, téléphone...) et « ce que l'on est » (biométrie).
Une entité peut posséder plusieurs identités numériques. Chaque identité permet alors d'exposer des informations en fonction de l'environnement. Ainsi, un individu peut présenter, par exemple, des informations publiques le concernant dans le cadre de son activité professionnelle, ce qui représentera une identité et d'autres informations personnelles le présentant dans son contexte familial, ce qui désignera une autre identité.
Une entité pourra accéder aux ressources informatiques mises à disposition dans une entreprise par l'intermédiaire de comptes. Un compte est défini par un identifiant d'accès, généralement un mot de passe et des attributs techniques en fonction de l'environnement. Il existe plusieurs types de comptes (utilisateur, administration, service, générique) attribués pour une personne ou pour un composant précis d'un système. On va habiliter l'utilisateur d'un ensemble de permissions sur une ressource.
Un rôle applicatif est un ensemble de permissions nécessaires à l'utilisation d'une applica-

tion ou d'une ressource. Il est défini de façon fonctionnelle et attribué en fonction du poste opérationnel au sein de l'organisation. Pour faciliter la gestion des habilitations, on met en œuvre un profil fonctionnel regroupant des rôles applicatifs différents pour l'exécution d'un rôle métier. Un utilisateur peut avoir plusieurs rôles métiers en fonction de l'entreprise (exemple : Ingénieur réseaux et Chef de secteur). Il disposera donc des habilitations relatives à ces deux rôles métiers. Le modèle RBAC [36] est construit autour des rôles métiers. Ces rôles représentent le lien entre les utilisateurs et les ressources.
Le CLUSIF [35] définit les six enjeux liés à l'IAM avec leurs composants de gestion (3.1)

Enjeux	Composants de gestion
Améliorer et simplifier la gestion des identités, des droits et des comptes	Gestion des identité
Piloter, auditer et contrôler les identités, les droits et les accès	Gouvernance des identités
Authentifier les utilisateurs	Gestion des accès
Contrôler et simplifier l'accès aux applications	Gestion des accès
Étendre les services IAM/IAG et IAI	Gestion intelligente
Tirer partie du cloud	Gestion des identités et des accès dans le Cloud

TABLE 3.1 – Enjeux de la gestion des identités et des accès

3.1.1.2 La gestion des identités

Le CLUSIF [35] définit la gestion des identités comme la gestion du « cycle de vie des personnes (embauche, promotion, mutation, départ, etc...) au sein de la société et les impacts induits sur le système d'information ». Ces changements ont des conséquences sur les informations connues et gérées par le domaine d'identité de l'organisation.
Je définirai la notion de **gestion des identités** comme étant l'ensemble des processus mis en œuvre pour gérer le cycle de vie des personnes (embauche, promotion, mutation, départ, etc...) ou des objets au sein d'une organisation. Elle fait intervenir plusieurs composants comme le « provisionning » des comptes, la synchronisation des attributs, la gestion de la structure organisationnelle, le système d'habilitations, l'audit, les processus métier, les règles et stratégies.

3.1.1.3 La gestion des accès

Les systèmes de **gestion des accès** assurent le contrôle d'accès aux ressources du système d'information. Ils offrent une couche globale d'authentification dépendant des capacités d'intégration offertes par les composants applicatifs. Le contrôle d'accès s'applique aux collaborateurs, aux partenaires, aux clients « consommateurs » ou aux entités non humaines. Les systèmes de contrôle d'accès se basent de plus en plus sur des systèmes à plusieurs facteurs (MFA) surtout pour les opérations sensibles (administration, connexion depuis l'extérieur). Dans beaucoup de cas, une solution de type **identifiant et mot de passe** est utilisée pour l'authentification. Dans les infrastructures « OnPremise », la stratégie des mots de passe est en général imposée par l'infrastructure AD et peut être dictée par des contraintes applicatrices (longueur ou inclusion de certains caractères spéciaux). Trouver les bonnes fréquences de changement ou longueurs du mot de passe est également un sujet de préoccupation [34]. **La gestion des autorisations** concerne les droits accordés aux utilisateurs sur les ressources auxquelles ils accèdent. Ils sont déterminés par la stratégie organisationnelle.
Le **SSO** désigne une architecture permettant à un utilisateur de s'authentifier de manière unique pour avoir accès à un ensemble de services au sein d'un unique domaine. La Fédération d'identité vise à établir une authentification unique vers des services appartenant à des domaines différents. Cette architecture fait intervenir trois entités principales dans les échanges : l'utilisateur, le « Service Provider (SP) » et « l'identity Provider (IdP) ». Il s'agit d'établir un cercle de confiance entre un ou plusieurs IdP/SP d'organisations différentes ayant conclu un accord. La fédération sert à propager des identités aux applications en mode SaaS, aux applications de partenaires ou aux applications de type e-commerce. La gestion des identités appartient à chaque entité, mais leurs services d'authentification sont interconnectés. Un utilisateur a ainsi accès aux ressources qui lui sont allouées par l'entité partenaire.

3.1.2 Analyse des solutions IAM du marché

Il existe de nombreuses solutions IAM que l'on peut classer de la façon suivante :

— Les produits de gestion d'identités et d'accès orientés consommateur (CIAM)

— Les produits « Identity As A service Service » (IDAAS)

— Les produits « Gestion des accès et fédération » (AM-FEDE)

— Les produits « Gouvernance des identités et des accès » (IGA) et « Identité et accès intelligent » (IAI)

Parmi ces produits on distingue :

— De grands éditeurs généralistes comme IBM, SAP ou Oracle qui disposent de solutions IAM performantes avec cependant une tendance à favoriser leurs produits ou

à déployer des produits de la marque.

— Des éditeurs spécialistes reconnus depuis de nombreuses années avec des orientations plus gouvernance (Sailpoint ou OneIdentity), gestion des accès (Ping identity) ou plus orienté vers le CIAM (Forgerock). Ils ont acquis une bonne notoriété grâce à leurs produits et ont un bon réseau de partenaires.

— Des éditeurs moins connus intervenant sur un marché plus restreint, un pays, une région par exemple l'Europe (Evidian, UbiSecure ou Tools4Ever).

— Des éditeurs qui ont fait le choix d'une solution « full cloud » avec des solutions IDaaS (Okta ou OneLogin ou Usercube). Ces solutions intéressent de nombreuses entreprises par la rapidité de mise en oeuvre et de bonnes caractéristiques identités et accès. A noter que bon nombre d'éditeurs proposent des solutions « OnPremise » et en mode Saas.

— Les ténors du cloud Public que sont Microsoft et ses solutions Azure, Google Cloud identity et Amazone Web Service et qui fournissent des offres liées à leur écosystèmes.

La plupart des acteurs clés IAM ciblent les marchés Amérique du Nord, d'Europe et d'Asie de l'Est. Ils nouent des partenariats avec des intégrateurs spécialisés ou des collaborations stratégiques avec d'autres éditeurs IAM afin de se différencier. On peut citer par exemple le partenariat entre « Sailpoint » spécialiste de la Gouvernance et « Ping Identity » spécialiste de la gestion des accès et de la fédération. Sur des grands comptes, un partenariat de ce type peut s'avérer payant. Ainsi pour un client de la distribution, un intégrateur concurrent à Digital Security a remporté un appel d'offres avec ce type de partenariat. Bien sûr cela n'a pas été le seul élément différenciateur. D'autres critères interviennent comme de bon retour d'expériences liées à des projets conséquents ou la capacité à fournir des offres très structurées. Il faut analyser en détails les points techniques précis de chaque solution pour avoir une vision explicite et surtout expérimentée. La mise en place d'un POC s'avère aujourd'hui obligatoire pour le choix du produit répondant le mieux aux besoins. L'IAM et le PAM sont une activité importante pour Digital Security. Les anciens partenariats sont conservés (SailPoint, Ping, CA). La volonté est d'anticiper la tendance du marché et d'aller vers les solutions « IDaaS » d'où la nécessité de trouver de nouveaux partenariats comme Okta ou Forgerock.

3.1.3 Les nouvelles tendances liées à l'IAM

3.1.3.1 Gouverner les identités

Historiquement les projets de gestion d'identité se sont initialement préoccupés du provisioning des comptes, des groupes et des tâches à faible valeur ajoutée (création ou modifications de comptes). L'idée principale de la gouvernance des identités est donc de permettre à un ensemble d'acteurs (responsables sécurité, auditeurs) de suivre l'évolution des identités et des accès des utilisateurs au sein du SI. Ce type d'outil doit permettre de répondre aux questions suivantes : Qui a accès à quoi ? Quelles sont les anomalies ? Les risques associés ? Quels sont les écarts par rapport à mes règles de gestion ? par rapport aux réglementations en vigueur ? Comment la situation a-t-elle évoluée ?
Aujourd'hui, la demande est plus forte sur la gestion des habilitations et notamment sur les problématiques de revue et certification des comptes. Il est nécessaire d'évaluer si le système est conforme à une politique de sécurité en vigueur ou à un nouveau règlement à venir.
On trouve aujourd'hui des fonctionnalités « gouvernance » dans des produits estampillés « gestion des identités ». La frontière entre ces deux types de gestion n'est pas très claire et peut varier en fonction des éditeurs. Par exemple les fonctionnalités de contrôle de conformité et de recertification peuvent être intégrées dans des solutions IAM.
Ces dernières années, le SI des entreprises s'est grandement ouvert à Internet : SaaS, IaaS, PaaS, mobilité, télétravail, partenaires et clients accédant au SI, etc... La plupart des solutions en place étaient faites pour le « On premise ». Les entreprises ont dû s'adapter à ces nouveaux usages quand cela était possible. Ces nouveaux cas d'usages impactent les processus et nécessitent parfois la mise en place d'un autre logiciel en remplacement ou en complément. Le tableau 3.2 montre la différence d'objectifs entre Gestion et Gouvernance des identités.

Objet	Niveau d'abstraction	Caractéristiques principales	Objectifs	Utilisateurs du système
Gestion des identités	Bas Proche de la technologie	o Synchronisation des données o Intégration de systèmes o Format des données o Transformation de données o Connecteurs et protocoles réseaux	o Accélérer les processus IT o Réduire les coûts IT o Automatiser o Améliorer efficacité des centres d'appel	Administrateurs IT
Gouvernance des identités	Élevé Proche du métier	o Processus métiers o Règles métiers o Stratégies o Structure organisationnelle	o Identifier « Qui a accès à quoi » ? o Trouver les anomalies o Identifier les risques o Vérifier la mise en conformité	Responsable sécurité, auditeurs, managers

Table 3.2 – Comparaison Gestion et Gouvernance des identités

3.1.3.2 L'émergence des solutions « Identity as a service » : IDaaS

Les services d'annuaire aujourd'hui utilisés sont le plus souvent des annuaires LDAP. Ils ont été conçus à l'ère des architectures clients-serveurs et leurs implémentations se basent généralement sur un système fermé. Microsoft a su imposer son annuaire Active Directory comme une brique essentielle pour les entreprises.
Disponible depuis une petite vingtaine d'années, AD est une application d'infrastructure gérant en priorité les comptes internes, les composants machines et les logiciels. Il assure la connexion au SI des utilisateurs et l'accès aux applications et ressources. Le couple (AD + MIIS-FIM-MIM[38]) était jusqu'à présent l'approche traditionnelle pour la gestion des identités dans beaucoup d'entreprises. L'ouverture du SI a provoqué une rupture en intégrant la décentralisation des systèmes. Les entreprises doivent aujourd'hui gérer des identités internes, externes et sécuriser les accès aux ressources « OnPremise » et «Cloud».
La solution IdaaS (identity as a service) permet de gérer l'ensemble de ces problématiques. Une telle solution en mode Cloud est attrayante parce qu'elle adopte une approche plus « neutre », rapidement opérationnelle en réduisant considérablement les étapes d'intégration. De nombreux acteurs IAM se sont positionnés pour entamer cette transition comme l'éditeur « SailPoint » qui voit « Dans cette tendance un mouvement tout naturel, poussé par la manière dont les utilisateurs accèdent à leurs données et applications, notamment en Cloud, à partir de multiples terminaux ».
Cette transition semble bien amorcée pour devenir un standard car de plus en plus d'entreprises s'intéressent à ces nouvelles solutions. La couverture fonctionnelle est pour le moment à l'avantage des solutions « OnPremise » mais pour combien de temps ? De nombreux éditeurs incluent une offre cloud dans leurs offres et certains ont fait le choix du « full cloud ».
L'obsolescence des solutions IAM internes déployées ces dernières années semblent être le premier vecteur de migration dans les environnements Grands Comptes. Certaines entreprises telles que la SNCF ont fait des choix stratégiques en basculant une grande partie du SI dans le Cloud. C'est un axe stratégique majeur répondant à un besoin de faire évoluer rapidement le modèle en place.
Dans la majorité des cas, Il faudra cependant tenir compte de l'existant en choisissant des produits intégrant notamment des composants passerelles (pour les annuaires AD, LDAP) ou adopter une position plus radicale en migrant l'ensemble des ressources dans le Cloud. Les éditeurs tels que « Okta », « OneLogin » ou « Ping Identity » proposent des solutions s'appuyant le plus souvent sur l'existant et ne cherchent pas pour le moment à le remplacer.
Les entreprises doivent se poser les bonnes questions sur ce qu'elles cherchent à faire, sur l'évolution et les tendances en cours, sur les services qu'elles veulent rendre aux clients

internes de l'entreprise. L'expression «as a Service » résume assez bien cette nouvelle approche.

3.1.3.3 Les offres métiers centrées sur le client : l'approche CIAM

Le CIAM (Customer Identity and Access Management) est l'évolution de la gestion des identités en entreprise. L'IAM est généralement associé au B2B, alors que CIAM est davantage destiné aux clients finaux (B2C). L'IAM permet une gestion des identités maîtrisées par l'entreprise (employé, partenaire). Le CIAM permet une gestion de l'identité orientée client/consommateur centré sur le métier de l'entreprise. Les différences entre IAM et CIAM sont explicités comme le montre le tableau 3.3.

Capacités	IAM Traditionnel	CIAM
Cible	L'entreprise : systèmes conçus pour être utilisés par les employés, les sous-traitants et les partenaires	Les clients (consommateurs) : systèmes conçus pour être utilisés par les clients de l'utilisateur final
Accessibilité	Web	Tous points d'accès (Web + mobile)
Inscription	Création par formulaire des employés externes, employés internes proviennent généralement source RH	Formulaires accessibles Web + Mobile processus d'enrôlement simplifié
Authentification	Services d'annuaires Interne	Social Login ou authentifications traditionnelles
Confiance	Fort (les employés, partenaires)	Faible (comptes « bidons », multiples comptes)
Volumétrie	Milliers voire centaines de milliers d'identités.	Millions voire Milliards d'identités.
Besoin en Performance	Fort (sécurité, IT)	Critique car touche le métier (image, client, confiance)
Sources de données	Référentiels interne (RH, annuaire d'entreprise)	Référentiels décentralisés (social login) ou centralisé (base interne)
Gestion données personnelles et consentement	Peu mis en oeuvre	Les outils prévoient un accès par le client à ces attributs personnels afin de pouvoir supprimer ce qu'il juge nécessaire.
Profils	Données collectées pour des tâches opérationnelles	Données collectées pour des sujets liés au métier (marketing, personnalisation, analytics)
Approche	Sécurité (IT)	Marketing (métier)

Table 3.3 – Comparaison IAM traditionnel et CIAM

Le CIAM se base sur une approche « business » avec des caractéristiques propres. Il vise à fournir une expérience utilisateur personnalisée. L'identité et les données associées sont fortement valorisées. Elles vont amener le client à souscrire à des services avec comme objectif sa fidélisation. Cela permettra la création de publicités ciblées ou de promotions personnalisées. D'un point de vue sécurité, le CIAM doit accorder les besoins de sécurité de l'identité et d'expériences client. Les objectifs sont le contrôle des identités, le respect les contraintes liées à la protection des données personnelles et une grande disponibilité du service métier.

Une solution CIAM couvre 3 briques technologiques comme le montre la figure 3.4 :

— Enregistrement et accès : fournit des services d'enregistrement et de connexion indépendamment du moyen d'accès (site web, mobile...) : API/SDK, fédération d'identité, social login...

— Stockage et traitement : fournit des services de stockage et de traitement des données : profiling, mise en qualité, agrégation...

— Intégration : fournit des connecteurs permettant au CIAM d'échanger des données avec les différentes solutions marketing de l'entreprise.

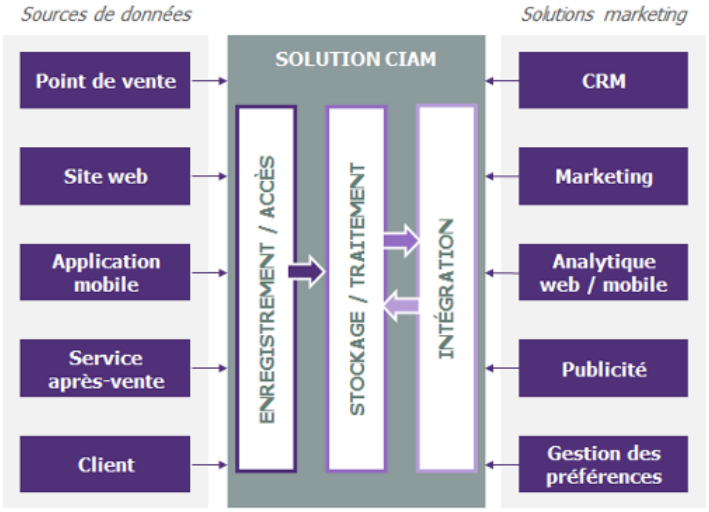


FIGURE 3.4 – Composants d'une solution CIAM

3.1.3.4 L'évolution de la réglementation

La Loi de programmation militaire (LPM), la transposition de la directive NIS (Network and Information System Security en mai 2018), les normes ISO 270XX8 et le RGPD (mai 2018) ont renforcé les dispositifs réglementaires liés à la cybersécurité.
La LPM et la directive NIS concernent les infrastructures critiques et essentielles. La

directive NIS vise à assurer un niveau élevé de sécurité des réseaux et des systèmes d'informations dans l'union européenne. Deux grandes catégories (opérateur public ou privé) sont concernées : les OSE (opérateurs de services essentiels) et les FSN (fournisseurs de services numériques) dans les domaines de l'énergie, transport, finance, assurance, santé ou restauration. Ces organisations doivent mettre en œuvre des chantiers de mise en conformité selon quatre principales dimensions :

— Gouvernance de la sécurité (plan SSI, homologation SIE)

— Protection (sécurité, architecture, administration et accès SI)

— Défense (détection et traitement incident SI)

— Résilience (gestion de crise)

Le RGPD concerne toute entreprise manipulant les données à caractère personnel (DCP). Les cas de violation du RGPD sont désormais pris de plus en plus au sérieux par les autorités nationales en matière de sécurité. Récemment, L'organisme britannique chargé de la protection des données personnelles (ICO) a infligé une amende de 204 millions d'euros à la compagnie aérienne British Airways. L'ICO a estimé qu'environ 500 000 clients ont vu leurs données « compromises » pendant un incident démarré en juin 2018 et attribué à « de mauvais systèmes de sécurité ». Les pirates ont profité de cette faille pour détourner le trafic sur un site frauduleux identique. Ils ont ainsi dérobé des informations comme le nom, l'adresse, le mail et les données bancaires des victimes.
Le cadre réglementaire actuel incite à la mise en place et l'évolution de projets IAM pour les infrastructures critiques (OIV, OSE, FSN) mais également pour tous les SI concernés par la réglementation et les normes. Pour les petites entreprises (PME) et les entreprises de taille intermédiaire (ETI) ces aspects ne sont pas toujours faciles à gérer. Cela demande beaucoup d'efforts car ces projets sont transversaux et organisationnels. L'IAM aide les sociétés à répondre aux enjeux de sécurité et de conformité. C'est la base d'une politique de sécurité efficace même si elle est reléguée parfois au second plan par rapport à d'autres priorités cybersécurité. Les mesures à mettre en place sont réparties en plusieurs domaines dont l'identification, l'authentification, les droits d'accès, les comptes d'administration, la traçabilité et les indicateurs.
Un IAM traditionnel gère les données des employés interne par l'intermédiaire du service RH ou par métiers en fonction par exemple de rôles attribués. Elle apportera un niveau d'abstraction entre l'identité et les droits d'accès à l'ensemble des applications du SI. Le CIAM avec son utilisation orienté client est souvent liée à la mise en conformité RGPD. Il permet au client-consommateur d'accéder et de gérer plus facilement les données que l'entreprises rassemble sur lui. On l'a vu ce genre de solution stocke les DCP du « consommateur » et administre son consentement. Le client doit pouvoir demander où gérer par lui-même la suppression de ses propres DCP (article 17 du RGPD : droit à l'oubli et la suppression).

Une solution IAM doit être complété par d'autres solutions afin de couvrir l'ensemble des obligations prévues par la réglementation européenne. En effet, une solution CIAM ne peut gérer par exemple les données stockées sur un service cloud tel que «Google Drive».

3.1.3.5 Une forte demande cloud avec AWS, Microsoft et Google

Le cloud « computing » est un service mutualisé et virtualisé dont le coût varie en fonction de l'utilisation réelle. En Avril 2018, le Gartner positionnait Amazone Web Services, Microsoft et google comme leaders du « Cloud Infrastructure As a Service ». Une tendance forte se dégage dans les sociétés pour l'utilisation des services Cloud.
On distingue trois grands modèles de cloud : IaaS (Infrastructure as a Service), PaaS (Platform as a Service) et SaaS (Software as a Service). Dans le modèle IaaS, l'entreprise cliente a un accès complet au système d'exploitation, ainsi qu'aux logiciels installés et aux données de ses machines virtuelles. Dans le modèle Paas l'entreprise garde la maîtrise de son application et du code ainsi que des données générées. Le système d'exploitation n'est pas administrable et est géré par le fournisseur. Dans le modèle SaaS, les applications peuvent donc louées pendant une période, facturées à l'utilisation ou par utilisateur avec des mises à jour sont automatiques. Les offres sont riches fonctionnellement et tout est fait pour faire attirer le client.
Les principaux avantages du cloud sont prometteurs mais vulnérables aux différents types d'attaques réseau et problèmes de confidentialité. Selon le Cloud Security Alliance (CSA) et son rapport sur les menaces (Treacherous 12 Top Threats to Cloud Computing), il y a au moins douze vulnérabilités très importantes dans les systèmes de Cloud. Parmi ces vulnérabilités, on peut distinguer celles qui ont un lien avec la gestion IAM accés : le vol de compte, les API non sécurisées et une gestion de l'identité et accès médiocre.
Les grands acteurs du Cloud ont l'expérience de la gestion de centaines de millions d'identités et proposent leurs compétences aux entreprises. Microsoft dispose d'une offre très complète, notamment avec ses solutions Azure AD destinées à gérer les identités et faire collaborer clients, partenaires et fournisseurs. Microsoft dispose d'un avantage par rapport à ces concurrents : son annuaire Active Directory historique et son pack Office 365 ont poussé/poussent la plupart des entreprises à souscrire à une offre Azure. AWS dispose également d'un service IAM permettant de gérer les identités, service gratuit en apparence nécessitant cependant de disposer de ressources afin de profiter de l'offre. Ces services sont facturés à l'utilisation. Les systèmes IAM dans le cloud gèrent les identités, authentifications et autorisations lors de la mise à disposition des ressources en veillant à ce que les bonnes personnes soient bien autorisées. Le tableau 3.4 propose une classification des services de sécurité cloud avec une vue globale hiérarchisée des composants et des technologies liées à la gestion des accès.
Il est bon de noter que la responsabilité de protéger les données d'entreprise n'est pas du ressort du fournisseur de services mais bien de l'utilisateur. Cependant, les enjeux sécurité

Editeur	Produit	Type	Plateforme	Commentaire
Microsoft	Azure AD	IAM	Cloud Microsoft	Bonne couverture fonctionnelle et lié à l'environnement Microsoft (AD, Office 365)
Google	Google Cloud Identity (IAM)	IAM	Cloud Google	Services et données cloud pour profiter de l'offre
AWS	AWS Identity and Access Management (IAM)	IAM	Cloud AWS	Services AWS pour profiter de l'offre

TABLE 3.4 – Offres IAM dans le Cloud Public

sont aujourd'hui critiques pour l'adoption du cloud par les organisations. Les fournisseurs agrémentent donc leurs offres de solutions complémentaires. Par exemple, la solution « Azure Identity protection » permet la détection plus ou moins rapides de vulnérabilités au niveau de l'identité (hybride et cloud) et ainsi proposer des actions (manuelles ou automatiques) avec l'aide de mécanismes comme l'analyse comportementale.

3.1.3.6 Gérer les identités des nombreux objets connectés

Le monde de l'IOT est vaste, il représente tout et n'importe quoi. On parle également d'IoE (Internet of Everything), expression inventée et promue depuis 2015 par Cisco qui engloberait l'univers IoT mais également les données, les processus et les personnes. Les perspectives s'annoncent mirobolantes avec des chiffrages avoisinant des dizaines de milliard d'objets connectés à partir de 2020.
La connexion sécurisée des appareils intelligents à un réseau représente un défi pour de nombreuses entreprises. Il s'agit des appareils et des objets connectés à Internet, des applications qu'ils exécutent, des services dans le cloud auxquels ils accèdent et algorithmes d'intelligence artificielle qu'ils sollicitent. Gérer l'identité est essentiel pour une communication fiable et sécurisée. Comme pour l'identité des personnes, l'identité des machines possèdent des caractéristiques permettant de les définir. Une identité permet à un objet d'accéder aux systèmes et données avec des moyens cryptographiques (certificats numériques et clés cryptographiques). L'identité des machines peut se baser sur ces clés et certificats TLS, SSH ou les clé API.
Un objet connecté peut être relié à son environnement de trois façons :

— Avec le Système d'Information de l'entreprise : Chaque objet communique à l'aide d'une identité unique et des droits d'accès associés. L'objet doit également s'authentifier auprès des applications afin de pouvoir les utiliser.

— Avec les clients finaux : comme on l'a vu, il y une interaction via la plateforme CIAM entre l'objet enregistré et l'utilisateur qui l'utilise. Les deux sont appairés. L'objet doit par exemple identifier les services auxquels l'utilisateur a droit.

— Avec les employés de l'entreprise et ses partenaires : ils interagissent directement avec les objets

De même que pour les personnes, les identités des objets connectés doivent être gérés avec des processus adéquats. L'état d'un objet va certainement évoluer (maintenance,

réparation, destruction). Le cycle de vie de ces objets doit donc être géré avec par exemple des plateformes hébergées soit dans une infrastructure « OnPremise » ou dans le « Cloud ». Les offres cloud AwS IoT et Azure IoT offrent de nombreuses fonctionnalités, produits, tutoriels permettant de mettre en application et développer des applications IoT.

3.2 Démarche projet orientée gestion des identités et des accès

Je me suis aussi intéressé pendant ce stage aux étapes que doit suivre un consultant en cybersécurité sur un projet de gestion des identités et des accès pour un système d'information donné et cela en partant du début.
La difficulté de ce type de projet évoquée lors des retours d'expériences réside dans la complexité des systèmes d'information existants qui ne permettent pas de construire un ensemble cohérent d'informations. En effet, les informations sont réparties dans de nombreux référentiels. De ce fait, il n'existe aucun moyen d'établir aisément la relation entre identité et habilitations et d'identifier les profils métiers ou les rôles applicatifs. C'est pourquoi il est conseillé d'établir au préalable une cartographie qui prend en compte tous les systèmes d'information permettant de recueillir des informations sur les personnes, les comptes utilisateurs , les profils métiers, les rôles ainsi que les ressources auxquelles ils accèdent.
La cartographie doit permettre de mettre en évidence des besoins. L'étape suivante consiste donc à fixer les priorités tant au niveau du système d'information global qu'au niveau fonctionnel. Les différents niveaux de priorité vont définir les objectifs que le système de gestion des identités et des accès devra atteindre . Chaque besoin doit être associé à un responsable ou une maîtrise d'ouvrage métier qui devient alors un des commanditaires, appelé sponsor du projet. La gestion des identités ayant un impact sur les processus liés aux ressources humaines, au moins en tant que consommateur des informations, un responsable doit donc être impliqué au plus tôt dans le projet.
Une difficulté supplémentaire évoquée lors des retours d'expériences de projets de gestion des identités est une durée trop importante qui est responsable de la diminution de l'implication des équipes fonctionnelles. Comme évoqué pour les démarches séquentielles, le manque de visibilité sur l'avancement du projet peut démotiver les clients du projet. C'est pourquoi Digital Security préconise de suivre une méthode itérative avec des livrables visibles à chaque étape.
La démarche préconisée est donc proche des modèles Agiles[37]. Chaque itération d'une durée n'excédant pas un mois doit permettre de livrer un composant de la gestion des identités et des accès auquel sera associé un sponsor correspondant au product owner des méthodes Agiles.

Les différentes étapes s'inscrivent dans un schéma à long terme reposant sur trois phases. La première phase consiste à bâtir une base solide pour les services de gestion des identités et des accès. Ce socle repose sur la connaissance des associations compte-identité. Pour cela il est nécessaire de nettoyer et mettre en cohérence les différents systèmes et de mettre en place un identifiant unique personnel.
La seconde phase est le déploiement des services de gestion des identités et des accès. Elle intègre la formalisation et l'automatisation des processus de gestion des habilitations. Elle a pour objectif d'offrir un moyen de gérer les accès et d'en réaliser un audit et de produire des rapports.
La dernière phase doit fournir une gestion fine des rôles. Elle débute par une réconciliation des rôles et des accès afin de déterminer qui accède à quelle application, à quel compte, selon quelle règle et avec quels privilèges. L'objectif est de fournir un moyen de gérer intuitivement cet ensembles d'informations.

3.3 Projet IAM Digital Security

3.3.1 Microsoft Identity Manager 2016

Microsoft Identity Manager 2016 (MIM 2016) n'est pas un produit unique, mais une famille de produits travaillant ensemble pour faire face aux difficultés liées à la gestion de l'identité. La figure 3.5 présente une vue d'ensemble de la famille MIM et des composants les plus pertinents pour une implémentation MIM 2016.

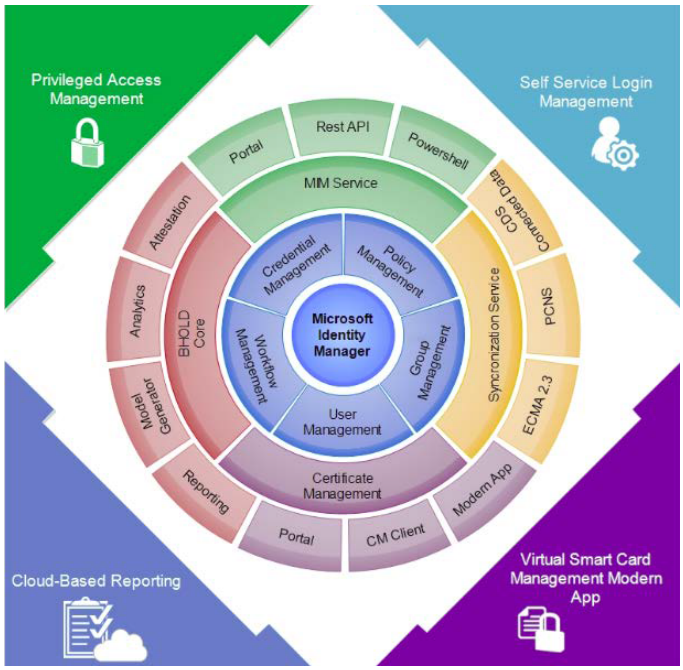


FIGURE 3.5 – Microsoft Identity Manager 2016

3.3.1.1 L'histoire de Microsoft Identity 2016

En 1999, Microsoft a acheté une société appelée Zoomit, qui avait un produit appelé VIA, un produit de synchronisation d'annuaire. Microsoft a incorporé Zoomit VIA dans son produit connu sous le nom de Microsoft Metadirectory Services (MMS). Le MMS n'était disponible qu'en tant que solution de Microsoft Consulting Services.
En 2003, Microsoft a lancé Microsoft Identity Integration Server (MIIS), qui était la première version publique du moteur de synchronisation que nous connaissons aujourd'hui sous le nom de MIM 2016 Synchronization Service.
En 2005, Microsoft a acheté une société appelée Alacris. Alacris avait un produit appelé IdNexus qui gérait les certificats et les cartes à puce, que Microsoft a renommé Certificate Lifecycle Manager (CLM).
En 2007, Microsoft a fusionné le MIIS (maintenant avec le Service Pack 2) et pour donner un nouveau produit appelé Identity Lifecycle Manager 2007 (ILM 2007). ILM 2007 était un outil de synchronisation des annuaires avec la fonction optionnelle de gestion des certificats.
En 2010, Microsoft a publié Forefront Identity Manager 2010 (FIM 2010). FIM 2010 a ajouté le composant Service FIM, qui fournit des capacités de flux de travail, des capacités de libre-service et une option d'approvisionnement sans code au moteur de synchronisation.
Microsoft a annoncé l'acquisition en 2011 d'une partie de la suite BHOLD , qui est un produit qui fournit des fonctionnalités de gouvernance des identités et des accès. Un an plus tard, en 2012, FIM 2010 R2 a été publié.

3.3.1.2 Les compoants de MIM 2016

Le tableau 3.5 présente les principaux composants de MIM 2016.
De ce qui suit, je décris, sans entrer dans les détails techniques (c.f. partie suivante), uniquement le composant MIM Synchronization Service car c'est sur ce dernier que j'ai implémenté les évolutions du client. Le service de synchronisation MIM est le plus ancien composant de la famille des identités de Microsoft. Quiconque a travaillé avec MIIS 2003, ILM 2007, FIM 2010 ou MIM 2016 trouvera le moteur de synchronisation MIM très similaire. Visuellement, les outils de gestion se ressemblent. Le service de synchronisation MIM peut fonctionner seul sans qu'aucun autre composant MIM ne soit installé, bien que toutes les fonctionnalités du produit ne sont pas disponibles en utilisant uniquement le service de synchronisation MIM.
Le service de synchronisation MIM est comme un cœur qui pompe les données d'identité entre les systèmes. Les données d'identité peuvent être un nouveau compte utilisateur, une mise à jour du service d'une personne, un membre d'un groupe mis à jour, la modification d'un contact, etc...

Composant	Description	Détail
MIM Synchronization Service, Sync Engine, ou MIM Sync	C'est le service qui gère l'identité et la synchronisation des mots de passe entre les systèmes.	Ce composant MIM est requis. Il utilise une base de données SQL pour stocker sa configuration et les informations d'identité configurées.
MIM Portal	Il s'agit du site Web IIS qui peut être utilisé pour la gestion administrative et le libre-service des utilisateurs.	Il utilise la base de données SQL pour stocker son schéma, ses politiques et ses informations d'identité.
MIM Service	Il s'agit du service Windows qui fournit au portail MIM des API web.	Il s'agit d'une composante facultative de MIM. Il depuis obligatoire pour déployer le portail MIM ou la réinitialisation de mot de passe en libre-service.
BHOLD	Il s'agit de la suite de services et d'outils qui s'intègre à MIM et améliore ses offres en ajoutant RBAC, l'attestation, l'analyse et le reporting de rôle.	Il s'agit d'un composant facultatif de MIM

TABLE 3.5 – Les principaux composants de Microsoft Identity Manager 2016

3.3.1.3 Architecture et fonctionnement interne du service de synchronisation de MIM 2016

Le but de cette partie est de présenter de manière générale la solution IAM qu'utilise notre client. Comme précisé précédemment, Notre client avait décidé d'utiliser Microsoft Identity Manager comme solution méta-annuaire. MIM est un outil proposé par Microsoft pour gérer les identités à l'intérieur d'une organisation. Un annuaire peut se définir comme étant un groupe d'objets soumis à un même schéma, à une même configuration et aux mêmes règles de sécurité. Un méta-annuaire (Metadirectory) est un logiciel qui permet de synchroniser plusieurs sources de données (plusieurs annuaires), principalement venant de la base de données LDAP (Lightweight Directory Access Protocol) tout en maintenant un répertoire de référence. MIM utilise les composants suivants :

— Metaverse : Le metaverse est une base de données contenant les informations d'identité intégrées (jointes) depuis de multiples sources de données connectées. Toutes les informations à propos d'une personne ou d'un objet spécifique, qui sont stockées dans de multiples sources, sont synthétisées dans une seule et même entrée du metaverse.

— Connector space : Le connector space est un espace de stockage utilisé par les agents pour exporter ou importer les données d'une source de données connectées.

— Source de données connectées : Une source de données connectées est un annuaire, une base de données ou tout autre espace contenant des données d'identité destinées à être intégrées par le méta annuaire. Les sources de données peuvent être des annuaires d'entreprise, une base des RH, ou des données sous forme de fichier plat tels que des fichiers LDIF, DSML ou texte délimité.

— Management Agent : Un agent relie une source de données spécifique au méta annuaire. Il prend en charge le déplacement des données depuis une source de données vers le méta annuaire. Quand une donnée du méta annuaire est mise à jour (via une action en ajout, effacement ou modification), l'agent peut aussi exporter les changements vers les sources de données pour les garder synchronisées.

— Le moteur de synchronisation : Ce module contrôle l'interaction des agents entre les sources de données et le metaverse, exécute les règles définies sur les objets et attributs ; vérifie l'intégrité des données et que la convergence entre les différentes données peut être assurée.

La figure 3.6 retranscrit les fonctionnalités principales de Microsoft Identity Manager

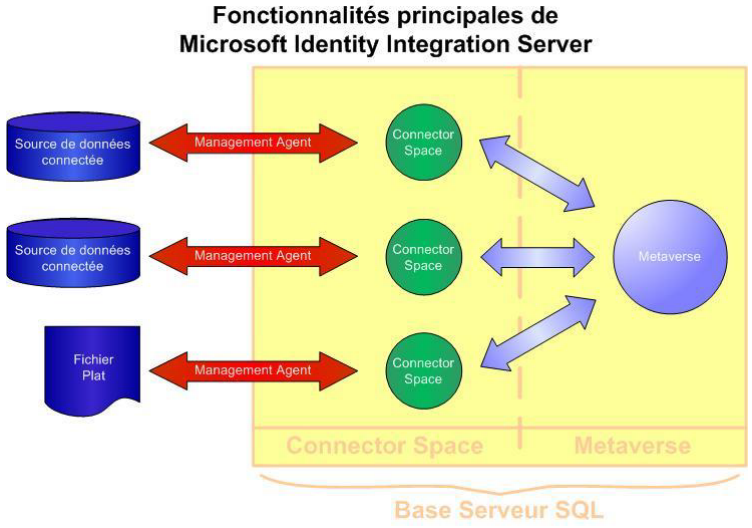


FIGURE 3.6 – Architecture interne de Microsoft Identity Manager 2016

3.3.2 Architecture technique

Le but de cette partie est de présenter le schéma de l'architecture technique de l'annuaire d'entreprise du client. Sa description comprendra :

— Une présentation générale de l'annuaire d'entreprise

— La description des services fonctionnels

— L'architecture fonctionnelle

— L'architecture technique

3.3.2.1 Présentation générale de l'annuaire d'entreprise

Le client souhaitait mettre en place un référentiel d'annuaire au service de ses utilisateurs ainsi qu'à ses filiales. L'annuaire de référence devait : être accessible par les utilisateurs via une interface Web et par les applications via LDAP, permettre de gérer les comptes Active Directory dans l'intranet et la DMZ, Intègrer les données sous forme de fichier CSV des autres sociétés du groupe et filiales et enfin elimenter une base Oracle avec l'annuaire et l'annuaire du personnel de l'entreprise et filiales sous forme de fichiers à envoyer aux filiales.
L'annuaire Pages Blanches est constitué de quatre modules fonctionnels 3.7 :

— Le méta-annuaire

— L'annuaire

— Le service de consultation

— Les consoles d'administration

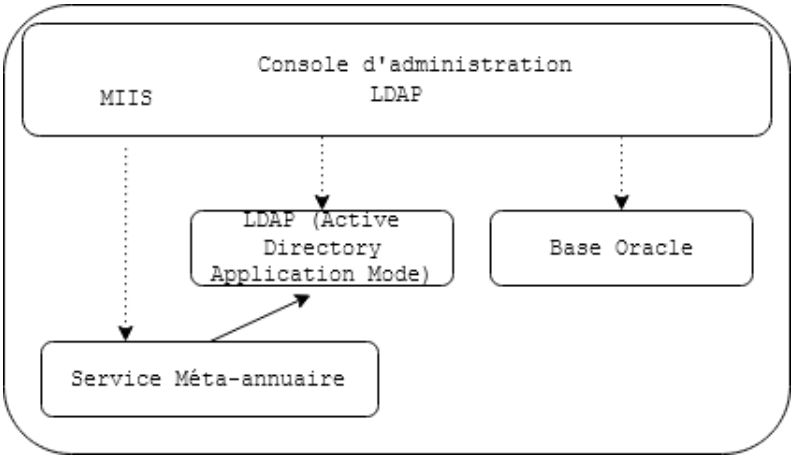


FIGURE 3.7 – Représente les modules énumérés précédemment

Le serveur MIIS est installé sur le réseau interne, le serveur d'annuaire principal est installé sur le réseau international. Ils sont accessibles seulement par les administrateurs.

Le serveur de méta-annuaire Microsoft Identity Integration Server (MIIS 2003 SP2) offre le service :

- De synchronisation des bases sources :
  - HR Access,
  - Base téléphonie (tables Oracle),
  - Fichiers consolidés pour le personnel des autres entités du client
- D'alimentation des bases cibles
- D'envoyer aux administrateurs en cas d'erreur, d'un rapport de synchronisation.

La figure 3.8, résume les différentes interfaces applicatives connectées au service Microsoft Identity Lifecycle Manager (Microsoft Identity Integration Server 2003 SP2) :

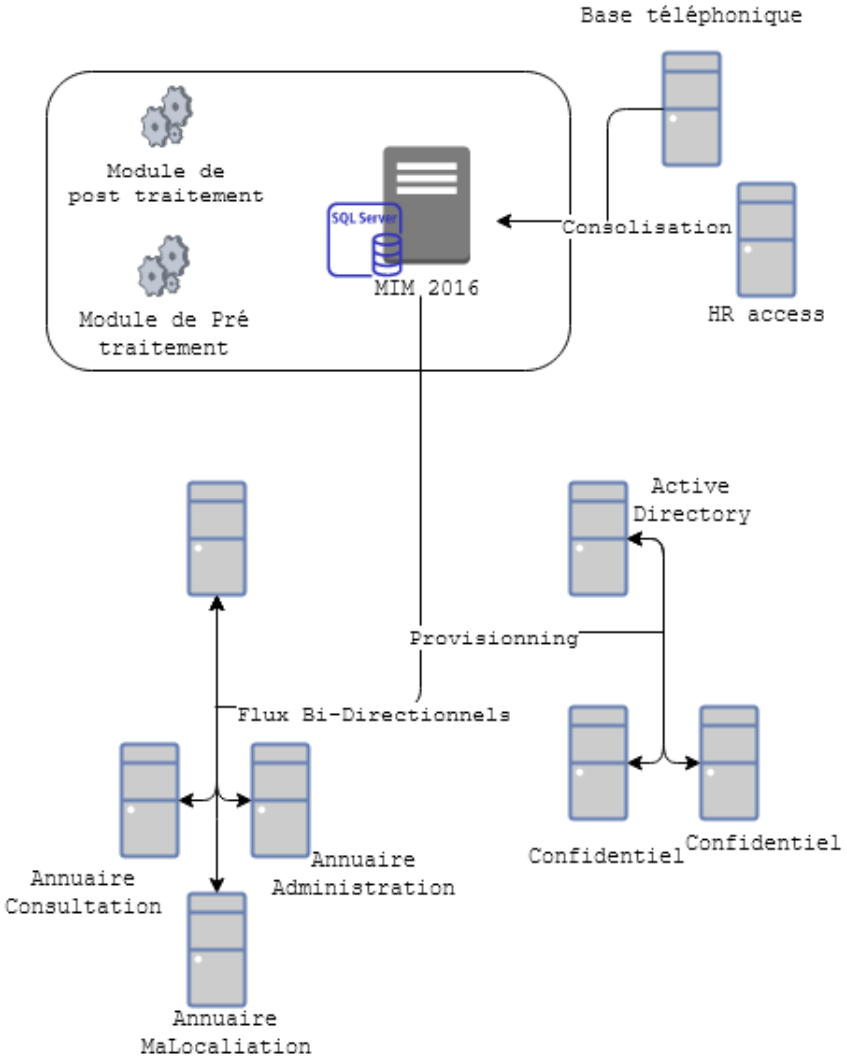


FIGURE 3.8 – Interfaces applicatives connectées au service

3.3.2.2 Description des services fonctionnels

Les principales fonctions apportées par ce service sont :

— La recherche des personnes et tout autre type d'objet (ressources, sites, organisations, historique et administration) à gérer selon différents critères paramétrables,

— L'affichage des résultats de la recherche

— L'affichage des fiches d'informations correspondant aux personnes ou à tout autre type d'objet géré par l'application.

— La navigation géographique,

— Le service de gestion des données permet à l'administrateur de créer, sélectionner, modifier ou supprimer tout objet présent dans l'annuaire en fonction des autorisations donées.

3.3.2.2.1 Principales interfaces applicatives

L'application Pages Blanches permet de consulter en mode anonymous l'ensemble des données de l'annuaire stocké. L'application Administration permet la gestion des personnes sur l'ensemble de l'entreprise du client. L'application Ma Localisation permet aux utilisateurs de gérer leur localisation pour les sites ouverts à cette fonctionnalité. Le schéma suivant 3.9 décrit les principales interfaces de l'annuaire :

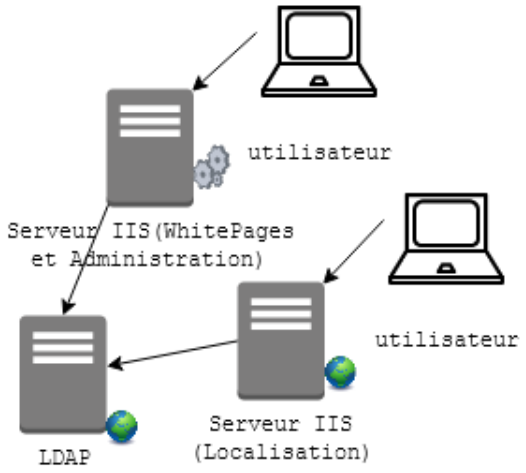


FIGURE 3.9 – Interfaces applicatives

3.3.2.3 Architecture fonctionnelle

L'architecture de la synchronisation des données du client utilise l'ensemble de produits suivant :

— Un annuaire centralisé pour stocker et gérer les informations d'identité

— Microsoft Identity Manager 2016 pour fournir les services de méta annuaire : MIIS permet l'intégration et la gestion des informations d'identité à travers les différentes sources de données. MIM met à jour l'annuaire centralisé en assurant le provisioning et la synchronisation des informations d'identité.

L'architecture de l'annuaire est composée de deux réseaux distincts :

— Le réseau interne : Le serveur MIM 2016 est installé sur le réseau interne. Le serveur MIM lit, filtre, organise et stocke les données consolidées dans sa base de données SQL 2005 à partir des informations disponibles dans chacune des sources. Le serveur MIM provisionne aussi ses données consolidées vers les cibles telles qu'une base oracle, l'annuaire d'entreprise, etc. Des développements additionnels, tel que le générateur de clef informatique, sont également disponibles. Un serveur IIS support l'application Ma Localisation.

— Le réseau IWAN : Les deux instances d'annuaire sont présentes dans le réseau IWAN. La première instance stocke les informations d'identité du client. Ces données sont répliquées, offrant ainsi une grande tolérance aux pannes. Sur le même serveur est installé les applications Administration et WhitesPages La deuxième instance stocke les informations d'identité et où est également installé les applications Administration et WhitesPages.

Le schéma suivant 3.10 décrit l'emplacement des différents composants de l'annuaire.

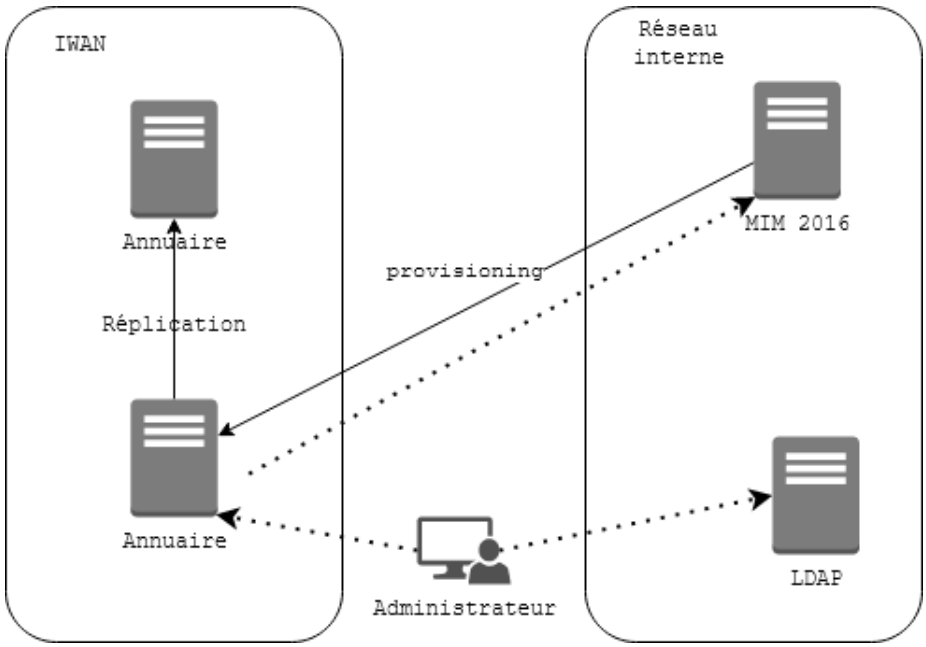


FIGURE 3.10 – Interfaces applicatives

3.3.2.4 Architecture technique

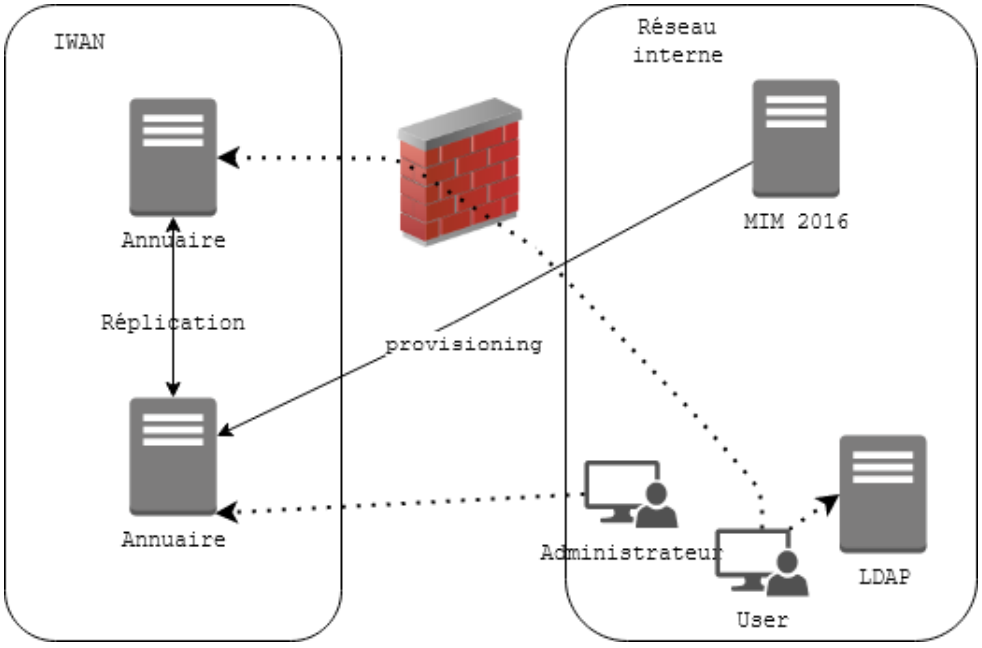


FIGURE 3.11 – Architecture technique annuaire

3.3.2.4.1 Description des flux

- MIM 2016 :
  - Flux LDAP avec le serveur : alimentation à partir de MIIS de l'annuaire
  - Flux réseau Windows : dépôt sur répertoire partagé du serveur RPMIIS des fichiers gérés par le service CFT.
  - Flux FTP
- Serveur d'annuaire :
  - Flux LDAP avec le serveur MIM 2016 : alimentation à partir de MIM de l'annuaire
  - Flux LDAP entre les serveurs d'annuaire pour la réplication
  - Flux de consultation de l'application WhitePages
- LDAP :
  - Flux de consultation et d'administration du service d'annuaire

3.3.3 Réalisations techniques

3.3.3.1 Évolution FR_IM-80 : Création d'un attribut multivalué pour SSO

Dans le cadre de l'évolution FR_IM-80, le client souhaitait créer un nouvel attribut dans un connecteur qui contiendra le ou les logins de connexion sous la forme domaine-login. Ce nouvel attribut permettra d'appliquer l'authentification unique (Single Sign-On : SSO) afin d'accéder à plusieurs applications informatiques de l'entreprise en ne procédant qu'à une seule authentification.
Les exigences étaient les suivantes :

— Création d'un nouvel attribut multi value de type string <EDactiveDirectoryKeys> qui est l'annuaire centralisé pour stocker et gérer les informations. L'attribut contiendra le ou les logins de connexion sous la forme domaine-login.

— Le développement devra être réalisé de façon générique pour pouvoir être exploité dans de futurs nouveaux agents.

— L'attribut sera constitué de tous les agents ayant l'attribut *login*

3.3.3.1.1 Réalisation technique

Afin de mener à bien cette évolution j'ai suivi les étapes suivantes :

1. Création d'un nouvel attribut dans le LDAP
2. Création d'une nouvelle règle dans la DLL MAExtension

La première étape était triviale à effectuer. Pour ce qui est de la deuxième, Il était nécessaire d'ajouter un flux d'export dans MIM pour permettre la synchronisation et la réplication des données dans les différentes sources.

3.3.3.2 Évolution FR_IM-190

Dans le cadre de l'évolution FR_IM-190, le client souhaitait modifier la valeur de l'attribut *userAccountControl* lors de l'historisation du compte. MBDA souhaite pousser la valeur *514* au lieu de *546*.

3.3.3.3 Évolution FR_IM-85

Dans le cadre de l'évolution FR_IM-85, le client souhaitait mettre à disposition une API permettant la création et modification d'un partenaire. Le but étant d'améliorer le processus de référencement des prestataires et la création de badges. Il était souhaité de mettre en place une fonctionnalité permettant de générer automatiquement un code utilisateur informatique (UtInfo).

3.3.3.3.1 Correctif

L'évaluation contenait aussi les correctifs suivants suite à la recette de l'évolution :

- Certains attributs ne sont pas pris en compte à la création.
- Dans le cas de la création, si un paramètre était mis pour EDwideKey, il y avait une erreur non documentée ERROR_API_CREATE.
- Dans le cas de la création, si le code site est absent, c'est une erreur de valeur qui est générée.
- Dans la cas d'une modification, les contrôles des valeurs n'est pas effectué.
- Mise à jour de la documentation

3.3.3.4 Évolution FR_IM-129

Dans le cadre de l'évolution FR_IM-129, le client souhaitait mettre à disposition une API permettant la mise à jour des numéros de téléphone sur une fiche d'une personne.

3.3.3.4.1 Correctif

L'évaluation contenait aussi les correctifs suivants suite à la recette de l'évolution :

- Dysfonctionnement lors de la mise à jour d'un numéro sur un site pour une personne qui n'a aucun site
- Ajout d'une fonctionnalité permettant de supprimer le numéro de téléphone d'un site
- Demande d'ajout d'information dans la table de log
- Mise à jour de la documentation

3.3.3.5 Évolution FR_IM-172

Dans le cadre de cette évolution, le client souhaitait gérer la création du compte AD lors de la création d'un externe via le portail d'administration.

3.3.3.5.1 Fonctionnement

Cette évolution implique la modification de deux éléments, l'application d'administration et la dll MVExtension responsable du provisionning des comptes.

- Application d'Administration :
  - Modification du formulaire de création d'un externe. Ajout d'un liste contenant les différentes valeurs possible. Une liste et un attribut dans les fichiers de configuration permettent de gérer le contenu et la valeur par défaut.
  - Modification de la fonction de création pour prendre en compte le nouvel attribut

— MVExtension :

— Modification des conditions de provisionnings d'un connecteur AD spécifique.

3.3.3.6 Évolution FR_IM-195

Dans le cadre de l'évolution FR_IM-195, le client souhaitait ajouter une variable permettant de spécifier une valeur pour le domaine SIP dans chaque environnement.

3.4 Problématique orientée recherche

La gestion des identités et des accès basée sur l'utilisation de la `Blockchain` et les solutions et tendances pour une application en entreprise.

3.4.1 Avant-propos

Les solutions traditionnelles de gestion des identités qui ont été décrites plus haut délèguent à des solutions centralisées internes ou externes. La tâche est de stocker les données privées des utilisateurs et de fournir à ces derniers des `tokens` d'identification tels que des cartes d'identité, des certificats, des identifiants de connexion ou du matériel spécifique. Grâce à ces `tokens`, les utilisateurs peuvent accéder aux ressources et aux services de l'entreprise.

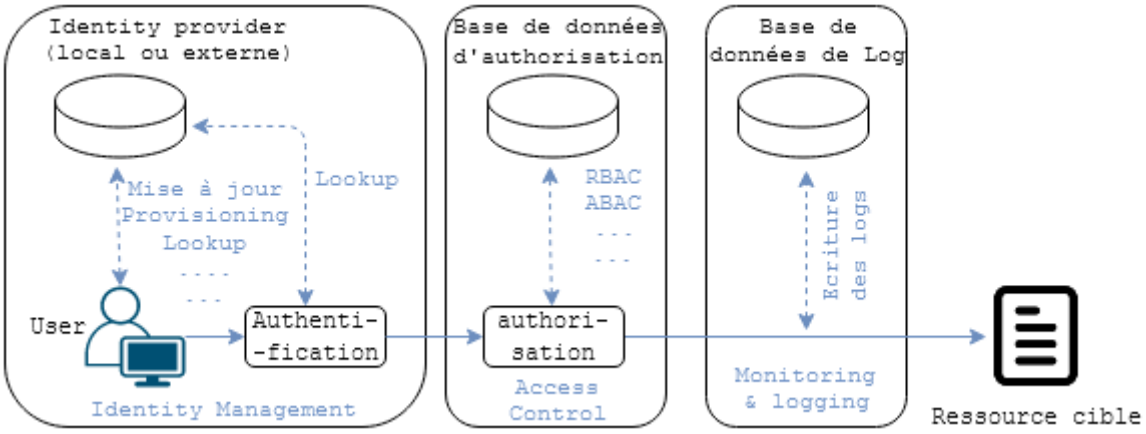


FIGURE 3.12 – Aperçu des fonctionnalités de l'IAM

Zhu et al. [4] affirment que l'approvisionnement, la mise à jour, la révocation et la consultation des identités constituent un ensemble d'opérations de base de la gestion des identités. Les identités de toutes les entités communicantes doivent être sécurisées pour prévenir le vol d'identité. Les données et les réseaux doivent être protégés par des mécanismes de contrôle d'accès afin d'empêcher tout accès non autorisé aux ressources de l'entreprise et aux données confidentielles. Enfin, l'IAM intègre des fonctionnalités de surveillance et de journalisation pour pouvoir stocker et tracer les informations critiques de manière sûre et vérifiable. La figure 3.12 résume ces trois principales fonctions de l'IAM.
Cette approche a donné lieu à quatre grandes catégories de problèmes : Les problèmes des utilisateurs individuels, les problèmes de partage d'informations, les problèmes de coordination des informations gouvernementales et les problèmes de confidentialité. Ainsi, En concurrence avec les solutions IAM existantes, les concepts et les produits basés sur la `Blockchain` ont évolué. La technologie `Blockchain` fait l'objet d'une attention croissante. Une `Blockchain` est une base de données distribuée d'enregistrements vérifiables

contenant des transactions qui sont partagées entre les parties participantes. Chaque transaction est vérifiée par consensus. Les enregistrements d'une `Blockchain` sont liés par des hachages cryptographiques. Chaque bloc contient la valeur de hachage du bloc précédent [5]. Plus de détails sur la technologie `Blockchain` sont fournis dans la partie 3.4.2.1. Ses partisans la préconisent donc pour une grande variété de cas d'utilisation, y compris l'IAM. De ce fait, Des solutions basées sur cette technologie apparaissent en grand nombre. Reste que ces derniers sont généralement accueillies avec beaucoup de critiques et de réserves dans les environnements professionnels. Le but de la partie 3.4 est de fournir un cadre d'évaluation composé de 18 critères appliqués aux 11 offres que j'ai pu recenser. L'analyse qui en résulte porte sur les fonctionnalités, les prérequis, la disponibilité sur le marché, la facilité d'intégration du produit dans l'environnement de l' entreprise et les coûts (estimés). Cette analyse inclut aussi mon point de vue.
Le reste de cette partie est structuré comme suit : Dans la section qui va suivre, je présente les fondements en décrivant plus en détail la technologie `Blockchain` et son utilisation en entreprise pour de l'IAM. Par la suite, je fournis une analyse approfondie des travaux connexes. Dans la partie 3.4.4, je définis les critères d'évaluations des solutions IAM qui vont être utilisés dans la section 3.4.5 pour évaluer les offres. La dernière section conclut la partie 3.4.

3.4.2 L'IAM basé sur la technologie `Blockchain` dans le contexte d'une entreprise

Dans cette partie, j'examine de plus près la technologie `Blockchain` et comment peut-elle potentiellement être appliquée pour de l'IAM.

3.4.2.1 Technologie `Blockchain` : Au-delà des crypto-monnaies

La technologie `Blockchain` a été introduite pour la première fois comme technologie habilitante pour la crypto-monnaie Bitcoin. Bitcoin implémente un réseau `Blockchain`, c'est-à-dire un ensemble décentralisé de nœuds qui détiennent tout une copie valide de la `Blockchain`. Le réseau doit établir un consensus sur la chronologie des transactions afin d'établir un journal des transactions finales faisant autorité sur tous les nœuds [6]. Dans les `Blockchains` dites publiques telles que Bitcoin, l'accès au réseau n'est pas limité. Ainsi, n'importe qui peut adhérer et participer.
Pour empêcher les `Blockchains` publiques d'être vulnérables aux attaques sibylles [7], des mécanismes de consensus avec une complexité de calcul exponentiel tel que la preuve de travail (proof of work) sont appliqués. Cependant, des collisions temporaires peuvent apparaître dans les `Blockchains` publiques en raison de la latence du réseau, ce qui nécessite l'application de règles de résolution de conflits [8].

Dans un réseau `Blockchain` privé, les participants sont connus et sont mis sur une whitelist. Ce type de système est également appelé `Blockchain` privée ou à accès nécessitant une autorisation. Les nœuds qui établissent une `Blockchain` privée doivent être initialement autorisés par une autorité de confiance [9]. Ce processus peut être appelé **gestion de l'identité des nœuds** [8]. Plusieurs frameworks s'appuyant sur la `Blockchain` ont été développées à des fins différentes et avec différentes fonctionnalités et propriétés de conception. Le projet **Hyperledger** est un exemple bien connu qui vise à l'établissement d'un standard ouvert pour les transactions commerciales d'entreprises basées sur la `Blockchain`. D'un point de vue sécurité, l'architecture Hyperledger prévoit l'authentification des nœuds via une autorité de certification qui distribue les certificats d'inscription aux nœuds. Les transactions sont chiffrées à l'aide d'une clé symétrique que tous les pairs du réseau détiennent. Chaque `Blockchain` possède sa clé symétrique de chiffrement. Pour les versions futures, un chiffrement plus fin (Fine-grained encryption) des transactions est prévu [10]. Grâce au gestionnaire de l'identité des nœuds, les `Blockchains` privées peuvent s'appuyer sur des mécanismes de consensus basés sur le vote et peu coûteux, permettant ainsi le traitement de dizaines de milliers de transactions par seconde. Une classe de mécanismes de consensus pour les `Blockchains` privées qui est actuellement utilisée est basée sur le protocole **Byzantine Fault-Toleran** (BFT) [11]. Les mécanismes de consensus BFT offrent une **finalité de consensus**, ce qui signifie que tous les nœuds qui fonctionnent correctement traiteront de la même manière les blocs dans leur copie de la `Blockchain` (par exemple en appliquant les mêmes règles et politiques). Cette condition empêche l'apparition de collisions [8]. La figure 3.13 illustre un processus de validation de transaction simplifié dans une `Blockchain`.

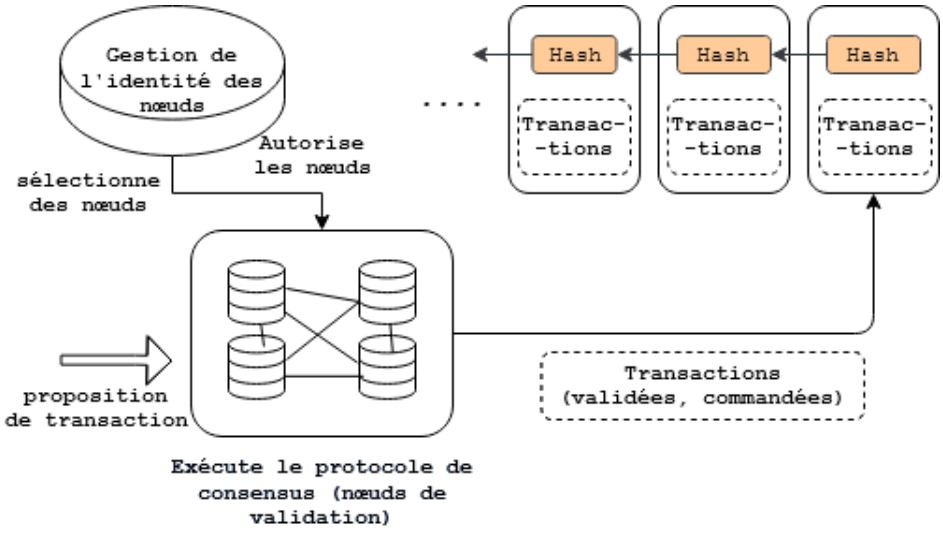


FIGURE 3.13 – Processus de validation simplifié pour une blockchain privée

Une entité qui souhaite soumettre des données à la `Blockchain` encapsule la requête dans une transaction et la propose aux nœuds de validation. Les nœuds de validation appliquent un ensemble de données de règles contractuelles par l'exécution répétée de contrats intelligents. Les contrats intelligents sont des scripts qui vérifient que les propriétés d'un contrat numérique arbitraire sont appliquées. Un contrat intelligent peut être déclenché en émettant une transaction à son adresse (qui est unique) sur la `Blockchain` [6]. Le protocole de consensus garantit que les transactions appliquées sur chaque nœud ne divergent pas. Grâce à la réplication de la machine d'état [12], il est possible de reproduire de manière cohérente un contrat intelligent dans un réseau décentralisé. Dans le cas de Hyperledger Fabric, un mécanisme de consensus basé sur le BFT est appliqué [10]. Pour éviter les divergences d'état entre les nœuds, les contrats intelligents doivent être déterministes. Dans le cas de l'Hyperledger Fabric, les contrats intelligents peuvent être installés sur chaque nœud de la `Blockchain` en émettant une transaction dite de déploiement. La figure 3.13 indique en outre qu'un gestionnaire d'identité des nœuds est nécessaire pour sélectionner les nœuds de validation. Des ensembles de nœuds de validation à changement dynamique sont prévus pour les futures versions de l'Hyperledger Fabric. Les nœuds non validateurs sont supportés et reçoivent les transactions et les transmettent aux nœuds validateurs [10].
Vukolic [8] affirme qu'un réseau BFT conserve toujours son état correct et sa finalité consensuelle malgré une asynchronie arbitrairement longue. Selon Fischer et al. [13], des nœuds défectueux peuvent conduire à un état dans lequel le consensus n'est jamais atteint lorsqu'un réseau est entièrement asynchrone. L'intégrité de la `Blockchain` serait toujours maintenue dans ce scénario. Cependant, le système serait empêché de prendre d'autres décisions consensuelles. Ainsi, la disponibilité du service pourrait être affectée.

3.4.2.2 Solution IAM basée sur la technologie Blockchain dans le contexte d'une entreprise

La littérature récente décrit des approches et des idées prometteuses concernant l'utilisation de la technologie `Blockchain` pour améliorer l'IAM et cela spécifiquement pour l'entreprise. La figure 3.14 illustre un modèle simplifié de l'interaction potentielle des différentes fonctions IAM et de la `Blockchain`. Elle illustre que la technologie `Blockchain` peut être appliquée aux trois opérations de base d'une solution IAM, à savoir la gestion des identités, le contrôle d'accès et la surveillance. Bien sûr, il existe de nombreuses limites et défis techniques que j'omets pour rester concentrer sur l'idée générale. Cette figure a été inspirée des implémentations présentes dans la littérature. Sur la figure 3.14, Les identités sont conservées sur une `Blockchain` et gérées par des transactions. Les propriétaires créent de manière aléatoire les paires de clés utilisées pour générer des identifiants et des informations d'identification à partir du même seed utilisé pour leur propre identité. Les identités des appareils contiennent en outre la signature du propriétaire comme attribut. Il serait intéressant d'utiliser la `Blockchain` pour stocker les droits d'accès à une ressource spécifique de manière sécurisée et pour gérer ces droits via des transactions `Blockchain`. La propriété de stockage inviolable est bénéfique pour le développement de mécanismes de surveillance robustes. Les utilisateurs ne peuvent nier avoir approuvé une transaction car l'authenticité de la `Blockchain` est vérifiée par un réseau de nœuds. Un attaquant devrait forger une signature numérique et prendre le contrôle d'une plus grande part de nœuds dans le réseau pour modifier les informations contenues dans une `Blockchain`. Ainsi, seules les transactions valides peuvent être conservées dans une `Blockchain` qui garantit la non-répudiation des informations enregistrées.

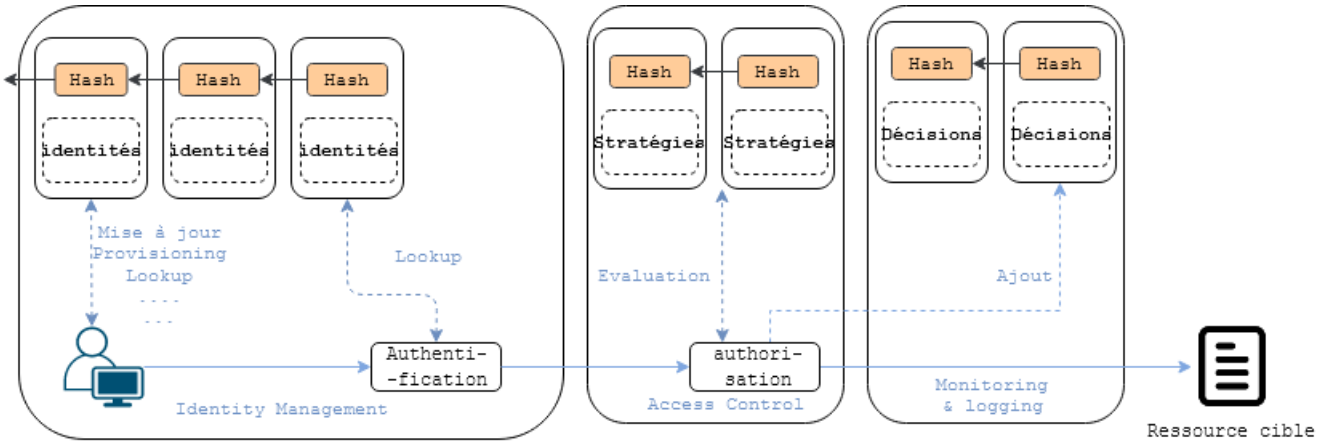


FIGURE 3.14 – Blockchain et les fonctions IAM

3.4.3 Travaux liés

Dans [14], Lim et al. donnent un aperçu de la technologie `Blockchain` pour l'IAM et l'authentification. Bien qu'ils couvrent certaines des offres analysées dans cette partie, ils n'ont pas fait de recherches sur le support des normes et protocoles IAM. Certaines des offres les plus prometteuses (telles que Civic) sont absentes.

Dans [15], Gruner et al. examinent la pertinence de la `Blockchain` pour l'IAM, en appliquant un modèle de décision à uPort, Sovrin et ShoCard. Cependant, ils limitent l'analyse pour quelques utilisateurs et ne considèrent pas l'intégration des applications comme un critère d'évaluation.

Dans [16], Muhle et al. réalisent une enquête sur ce qu'ils considèrent comme les composantes essentielles d'une solution pour l'identité auto-souveraine. Cependant, leur travail ne cherche pas à savoir si les composants/offres trouvés peuvent être intégrés dans des architectures d'entreprise déjà établies, en utilisant des interfaces et des protocoles standardisés.

Dans [17], Stokkink et Pouwelse introduisent un «modèle de revendication prouvable générique». Leur travail vise à implémenter une identité auto-souveraine pour les Pays-Bas et faisait partie d'un projet pilote mené par le gouvernement en 2018. Cependant, l'article ne présente pas comment la solution pourrait s'intégrer aux applications informatiques existantes.

Dans [18], Schanzenbach et al. présentent un prototype d'un système d'identités auto-souveraines, mais sans `Blockchain` ni composants DLT. Contrairement à la plupart des approches d'identité auto-souveraine, les auteurs discutent de la manière dont leur approche peut participer à un standard établi (ici, OpenID Connect).

Dans [19], Baars a comparé (à partir de 2016) plusieurs solutions d'identité basées sur la `Blockchain` et a également vérifié leur compatibilité avec la bibliothèque JavaScript passport.js, qui prend en charge plus de 300 méthodes d'authentification. L'auteur propose une nouvelle solution, mais la solution n'a pas encore été mise en œuvre.

Un nombre important de publications à jour sur la gestion des identités et sur l'utilisation des `Blockchains` pour l'IAM sont régulièrement fournies par des sociétés d'études de marché, notamment Gartner et d'autres.

3.4.4 Critères d'évaluation

Les critères d'évaluation introduits dans cette partie seront utilisés dans la partie suivante pour analyser les offres identifiées. Ils sont regroupés dans le tableau 3.6 (critères de conformité), le tableau 3.7 (Expérience utilisateur final) et le tableau 3.8 (critères de technologie, de mise en œuvre, d'intégration et d'exploitation).

Numéro	Description
CR01	Conformité et assistance GDPR
CR02	Contrôle de la répartition géographique des données
CR03	Piste d'audit conforme au GDPR
CR04	Le trafic du réseau IAM depuis/vers les applications backend utilisant l'IAM peut être isolé du trafic internet
CR05	L'exportation et le transfert d'identité peuvent être contrôlés pour empêcher le vol d'identité
CR06	Modèle de paiement pour l'utilisation de services et les prix fixes dans une monnaie convertible

Table 3.6 – Critères de conformité

Numéro	Déscription
U01	Les utilisateurs finaux n'ont pas à payer séparément pour les services d'identité de base
U02	Solution compatible SSO
U03	L'identité est utilisable à partir d'appareils mobiles
U04	L'identité est utilisable à partir d'appareils de bureau
U05	La solution supporte la MFA
U06	L'auto-inscription est possible
U07	Les identités peuvent être structurées en hiérarchies

Table 3.7 – Expérience utilisateur final

Numéro	Description
T01	Le réseau blockchain est autorisé à garantir que seules les parties autorisées peuvent configurer des nœuds, accéder aux données et voter
T02	La pertinence de la cryptographie quantique pour la sécurité de l'implémentation a été étudiée
T03	Only the public key of the identity is stored on-chain ; the wallet address is derived from it
T04	Les membres du réseau peuvent voter sur les règles et la gouvernance
T05	Les nœuds peuvent choisir de ne stocker qu'une partie pertinente des données
T06	Seuls les hachages d'assertions et de revendications sont stockés sur la chaîne

Table 3.8 – Critères de technologie, de mise en œuvre, d'intégration et d'exploitation

3.4.5 Les offres du marché pour les IAMs basées sur la `Blockchain`

Abacus [20] est un «protocole d'identité et de conformité open-source pour les tokens d'accès» basé sur Ethereum : le protocle implémente un workflow dans son backend pour KYC, AML, etc... Ses principaux objectifs sont les fintechs et la crypto-monnaie. La page d'accueil et le livre blanc d'Abacus ne divulguent pas de modèle commercial et ne fournissent pas d'interface utilisateur ni d'application aux utilisateurs finaux.

BitID [21] est un simple «protocole open-source d'authentification Bitcoin» conçu pour l'authentification utilisant la propriété essentielle de la cryptographie à clé publique : le serveur présente un défi au client, le client le signe avec la clé privée et le serveur vérifie la signature en utilisant la clé publique. Dans BitID, l'identité est l'adresse Bitcoin. BitID n'est pas une offre d'identité auto-souveraine complète, même si l'identité qu'il utilise ne peut être enlevée par une autorité centralisée. Des exemples d'implémentation d'applications pour smartphone avec BitID sont fournis, mais l'utilisation de BitID sur le marché a été très faible.

Bloom [22] se décrit comme un «protocole de bout en bout pour l'attestation d'identité, l'évaluation des risques et le crédit scoring». Il offre une plate-forme d'identification autonome basée sur Ethereum et IPFS ; Des applications iOS et Android sont fournies. Les paiements intra-réseau et la gouvernance sont mis en œuvre à l'aide du token BLT propriétaire. Le site Web de Bloom ne répertorie aucun client ni aucune intégration.

«Cambridge Blockchain» [23] fait la publicité d'une solution (bien que n'étant pas un produit nommé) qui est présentée comme une simplification de la conformité d'identité. Il est décrit comme basé sur une `Blockchain` privée (bien qu'aucune technologie spécifique ne soit spécifiée et que la mise en œuvre ne soit ni expliquée ni téléchargeable).

Blockpass [24] présente sa solution comme un système d'identité pour «les industries réglementées et l'Internet de tout». Blockpass se décrit comme un «service de vérification d'identité auto-souverain qui stocke uniquement une représentation cryptographique de l'identité vérifiée de [l'utilisateur] sur une liste blanche dans une `Blockchain`» afin que les données d'un utilisateur «soient stockées sur l'appareil mobile de [l'utilisateur]» et partagées uniquement avec ceux que l'utilisateur choisit.

Civic [25] se décrit comme un «écosystème d'identité sécurisé» et avec plus de 90 intégrations (y compris les ICO). Il possède l'une des plus grandes part de marché des identités basées sur la `Blockchain`. Civic affirme que son application aide à contrôler et à protéger les identités tout en utilisant la biométrie et la `Blockchain` sur un appareil

mobile. Civic est conçu de manière à ce que les données d'identité résident sur les appareils mobiles des utilisateurs et non sur l'infrastructure de Civic. Ainsi, les données d'identité doivent être échangées directement entre un utilisateur Civic et un fournisseur de services. Civic n'est pas une autorité d'authentification, cette solution ne peut donc pas révoquer ou invalider les affirmations d'identité ou les données. Civic définit une «vérification d'identité» pour la connexion sans mot de passe et l'authentification multifacteur.

Le terme "Sovrin" [26] fait le plus souvent référence au réseau Sovrin, un service public qui permet l'auto-souveraineté de l'identité sur Internet. Sovrin est un projet open source qui offre les outils et les bibliothèques pour créer des solutions de gestion de données privées et sécurisées qui s'exécutent ensuite sur le réseau d'identité Sovrin. La blockchain sous-jacente est publique mais nécessite une autorisation. Il n'y a pas d'application Sovrin officielle disponible dans les magasins d'applications pour Android ou iOS. Sovrin est bien documenté, à différents niveaux d'abstraction et avec des exemples. Dans Sovrin, une personne (identité) peut utiliser plusieurs identifiants, c'est-à-dire un pour chaque service. Les interactions dans Sovrin sont conçues en utilisant des pseudonymes («cryptonymes») pour minimiser les corrélations indésirables.

Pillar [27] est un projet qui vise à redonner la propriété des données personnelles aux utilisateurs. Il y a un an, il s'agissait simplement d'un portefeuille open-source pour les crypto-monnaies et les tokens. La fonctionnalité *data locker* qui propose une gestion des identités, fait partie des projets de l'entreprise pour 2020. Selon leur site Internet, Pillar compte déjà 60 employés.

ID2020 [28] est une alliance qui considère les identités numériques portables et sécurisées par MFA comme un moyen d'améliorer la situation des réfugiés. ID2020 est soutenu par l'ONU, l'ITU et d'autres agences. Les partenaires fondateurs de son écosystème comprennent Microsoft, Accenture et d'autres entreprises ainsi que des fondations. Avec un modèle de gouvernance élaboré et un manifeste, ID2020 adopte une approche très systématique, y compris une sélection des candidats à la solution. Aucune implémentation ou architecture n'existe encore.

L'Ethereum Enterprise Alliance (EEA) [29] est un consortium d'entreprises visant à encourager l'adoption par les entreprises de la `Blockchain` open source Ethereum et cela en utilisant les bonnes pratiques. L'AEE comprend des groupes d'intérêts spéciaux (SIG) et des groupes de travail techniques (tels que la "Digital ID Task Force"), mais les deux sont ouverts uniquement aux membres payants. La spécification client a été rendue publique par l'EEA en mai 2008 et comprend des dispositions relatives aux transactions privées, bien qu'aucune mise en œuvre n'ait encore commencé.

3.4.6 Évaluation

3.4.6.1 Résumé de l'évaluation

L'analyse de toutes les offres dans la section précédente montre qu'aucune d'entre elles ne satisfait les critères présentés dans les tableaux 3.6, 3.7 et 3.8.
Les solutions Blockpass IDN et Civic sont les deux qui remplissent le plus de propriétés. Sovrin présente un attrait particulier car c'est la seule solution soutenue par un consortium multi-fournisseurs plutôt que par une seule société.
Civic s'efforce également de créer un écosystème plutôt qu'un simple composant qui peut être réutilisé. Pour toutes les offres, la pertinence pour l'utilisateur final et la pénétration du marché sont à un stade très précoce. La grande majorité des offres ne dispose pas d'interfaces conformes aux normes (telles que OAuthor SAML) pouvant être intégrées par les fournisseurs de services avec la même facilité que les solutions IAM classiques. Même sans ces normes, aucune des offres ne peut se vanter d'une intégration au niveau de la production avec une large base d'utilisateurs.

3.4.6.2 La conformité

En termes de conformité, toutes les offres étudiées en sont à leurs tout débuts. En particulier, la conformité au RGPD. Cette dernière ne peut être offerte qu'en exécutant un réseau consortial autorisé où l'emplacement des nœuds de la `Blockchain` est strictement réglementé. Pour le réseau Sovrin, il existe une série d'articles couvrant les détails du RGPD, mais aucune garantie n'est donnée. Aucune des solutions n'est certifiée par un tiers de confiance.

3.4.6.3 Technologie et implémentation

Dans une entreprise, l'infrastructure IAM existante est la pièce maîtresse essentielle pour les utilisateurs et les applications. Très souvent, il est basé sur Microsoft Active Directory fonctionnant dans une configuration multi-serveurs tolérante aux pannes (sur site ou dans le cloud). Pour les installations de grande taille et critiques, il est actuellement irréaliste de remplacer à court terme complètement une telle installation par une solution basée sur la `Blockchain`. Par conséquent, la solution basée sur la `Blockchain` (par exemple pour l'identité souveraine) doit être intégrée dans un tel environnement. Aucune des offres étudiées n'a de concept ou de feuille de route pour cette tâche importante.

3.4.7 Conclusion

Des identités souveraines et décentralisées ont été créées pour faire face aux limites des systèmes IAM centralisés et conventionnels. Envisageant des écosystèmes et des réseaux avec moins d'intermédiaires, cette nouvelle approche doit rivaliser avec les solutions IAM actuelles. La technologie de la `Blockchain` est à la fois prometteuse et compliquée. L'adoption de l'IAM basée sur cette technologie a été assez lente malgré les attentes élevées. Pour réussir, les nouvelles approches identitaires doivent offrir des avantages substantiels aux demandeurs et aux prestataires de services. Ces avantages peuvent inclure la sécurité, la facilité d'utilisation, la protection des données, la transparence et également la réduction des coûts - en tenant compte des coûts de migration et de formation des utilisateurs.

Chapitre 4

Conclusions et perspectives

Actuellement, Digital Security est toujours le sous traitant pour la prestation Tierce maintenance applicative (TMA) pour ce client. De ce fait, il continue de gérer le Maintien en condition opérationnelle (MCO), les correctifs et le développement des évolutions de MIM 2016. D'après moi, un projet de gestion des identités et des accès sort du périmètre strict de l'informatique pour couvrir d'autres domaines métiers. Il est donc nécessaire d'avoir, d'une part un engagement fort des parties prenantes métiers et d'autre part l'implication, la disponibilité et une parfaite coordination des experts techniques des différents domaines (annuaire, base de données, Windows, etc...). La gestion des identités et des accès est devenue une infrastructure essentielle. Les enjeux sont importants et les entreprises, dont notre client, sont confrontées à un panorama d'identités numériques de plus en plus complexe et déroutant.
Le point le plus important que j'ai pu retenir de ce travail est qu'un projet IAM a une vie après la mise en production. On trouve encore dans certaines entreprises, des clients qui pensent que le projet s'arrête au déploiement de la solution. Mais ce n'est définitivement pas le cas. La vraie vie d'une solution d'IAM commence avec son déploiement. Le jour où la solution d'IAM passe aux mains des opérations est en réalité le premier jour de sa vie. Ce projet a été très enrichissant tant d'un point de vue technique que d'un point de vue humain car j'y ai pu :

— Élargir mes compétences techniques sur les différentes technologies abordées dans le cadre de ce projet.

— Des notions sur comment gérer la conduite et le déroulement d'un projet de grande envergure.

— Élargir mon réseau au sein même de Digital Security en travaillant en étroite collaboration avec des acteurs métiers IT et hors IT.

Dans une seconde partie, j'ai abordé un sujet orienté recherche. Le fait d'avoir inclus cette partie était important pour moi car mon projet professionnel qui va suivre ce stage est d'effectuer une thèse de doctorat.

De nos jours, les utilisateurs se méfient de plus en plus du fait que de nombreuses entreprises numériques en sachent trop sur eux et que le contrôle de l'identité, devrait d'une manière ou d'une autre, être récupéré par les utilisateurs finaux.
La *Blockchain* est arrivée à un moment critique avec une série de promesses liées à la sécurité, dont beaucoup sont apparemment applicables à l'identité, même si ce n'est que de manière vague. De nombreuses entreprises IAM ont vu le jour «sur la *Blockchain*». De larges affirmations ont été faites selon lesquelles cette nouvelle famille de solutions perturberait l'IAM traditionnelle. La partie dédiée à l'application de la *Blockchain* pour l'IAM recense les principaux travaux sur ce sujet.

Annexes

Annexe 1 : Présentation de la société

L'entreprise Digital Security est une entité appartenant à la galaxie du groupe Econocom dont l'effectif est de 10 700 collaborateurs répartis dans 19 pays. Son chiffre d'affaires est de 3,0 milliards d'euros. Le groupe se positionne sur le financement et l'accélération de la transformation digitale des entreprises. Il dispose de la taille critique pour la gestion de projets d'envergures.

La société Digital Security est une société de conseil créé en 2015 par un groupe d'experts en sécurité. Elle est née de la fusion du CERT européen Digital Security et de la société Cyber Security. La structure a décidé de s'associer au groupe Econocom afin de bénéficier de l'appui d'un grand groupe tout en conservant une liberté d'autonomie et de réactivité. Il emploie actuellement environ 250 consultants et experts en sécurité basés à Paris, en Belgique, au Luxembourg et en régions. Digital Security se considère comme le premier CERT européen en partie dédié aux objets connectés.

Ses prestations couvrent les domaines de :

— L'audit,

— Le CERT,

— Le conseil,

— La formation,

— L'intégration de projets sécurité

— L'exploitation en centres de services

Digital Security a décroché le 27 Février 2019 auprès de l'ANSSI la conformité PASSI Loi de Programmation Militaire (LPM). Le 20 Mars 2019 était obtenu la conformité PASSI Monaco délivré par L'Agence Monégasque de Sécurité Numérique (AMSN). La qualification PRIS (Prestataires de réponse aux incidents de sécurité) a été obtenue récemment.

L'agence « Occitanie Toulouse » (OCC) est la deuxième agence régionale ouverte en Juin 2018, celle de « Auvergne Rhône Alpes » était la première (début 2018), vient ensuite celles de Bordeaux et Lille en septembre 2018 et Aix en octobre 2018. L'Agence OCC est implantée dans les locaux d'Econocom à Labège. Elle compte actuellement une dizaine de collaborateurs sous la responsabilité de Hicham GONDOUIN (responsable de l'Agence) et de Fréderic Priem (Directeur régions). Les effectifs de l'agence OCC devraient augmenter

ces deux prochaines années avec un objectif annoncé de 30 collaborateurs. L'agence se structure autour des domaines d'expertise suivants :

— Intégration de Projets sécurité et architecture

— Tests d'intrusion

— Conseils et Gouvernance SSI

Annexe 2 : Cas d'utilisation d'une IAM

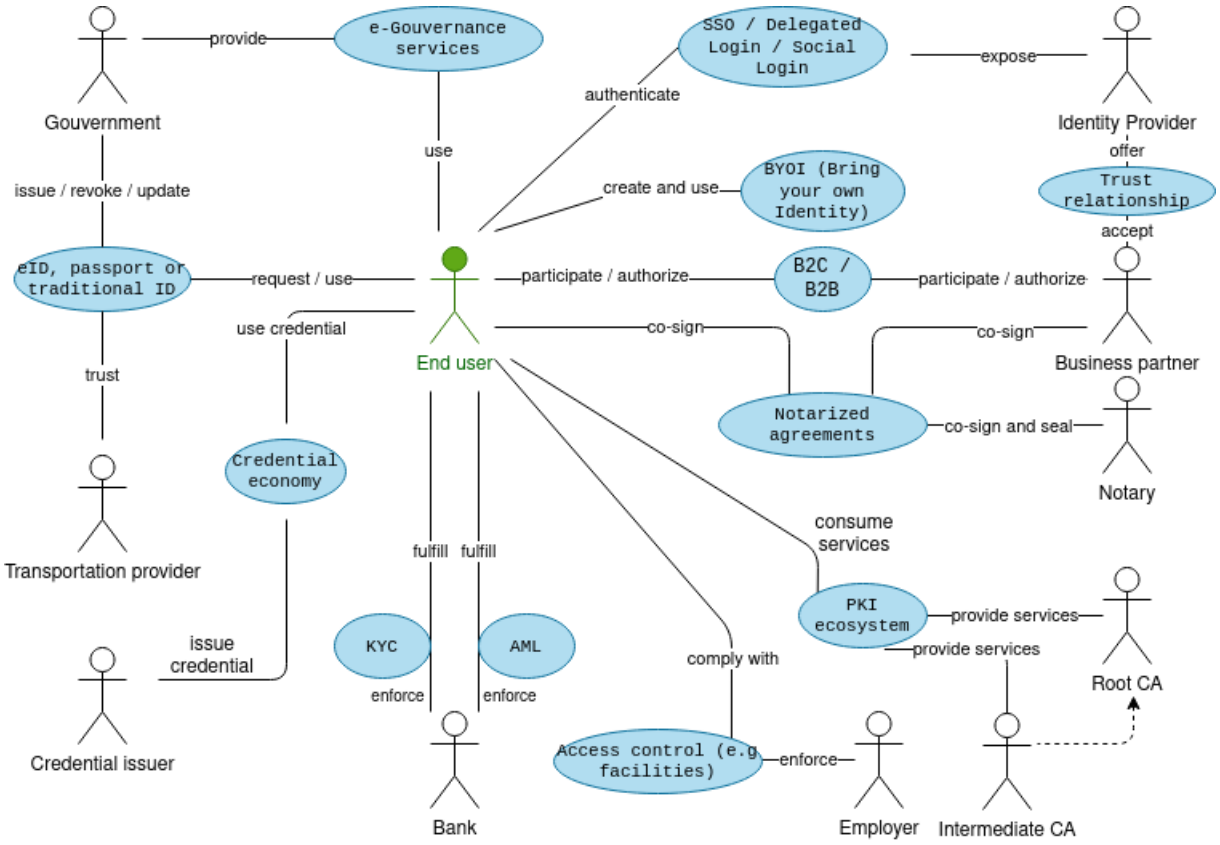
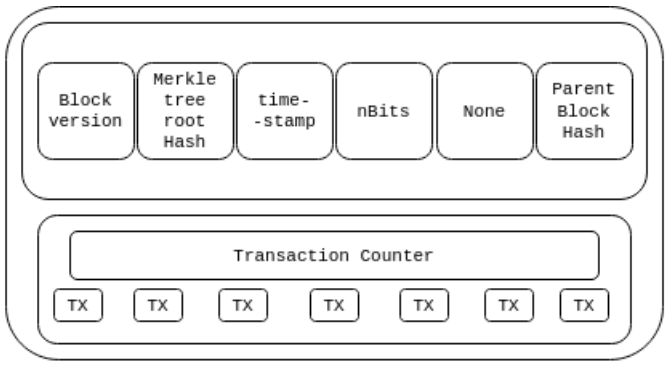


FIGURE 4.1 – Une sélection de cas d'utilisation et d'acteurs dans le domaine de la gestion des identités et des accès (IAM)

Annexe 3 : Blockchain et transactions



- Block version: indique quelles régles de validation de block à suivre.
- Merkle tree root hash: hash de tous les transactions du block.
- Timestamp: l'heure actuelle en seconde depuis le 1er Janvier 1970.
- nBits: La taille en bits d'un hash de block valide
- None: champ qui prend 4 octets.
- Parent block hash: hash du block parent

FIGURE 4.2 – Structure d'un Block d'une Blockchain

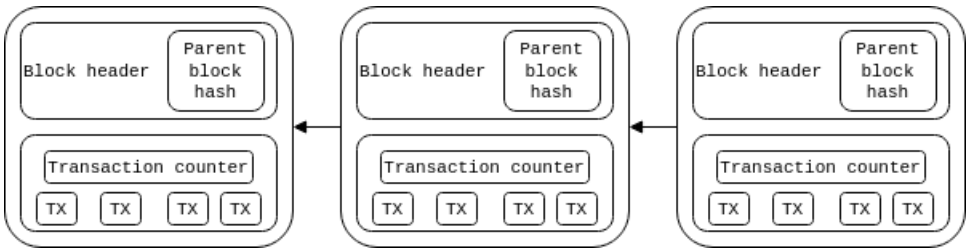


FIGURE 4.3 – Exemple d'une Blockchain

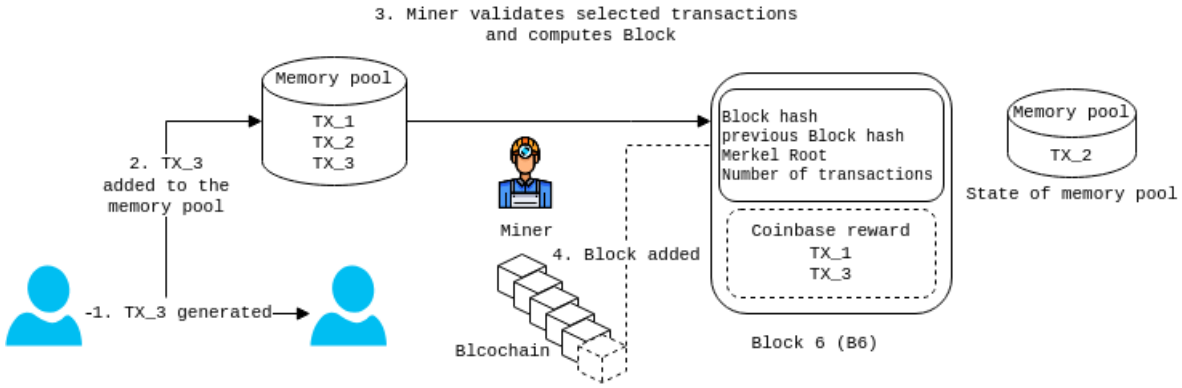


FIGURE 4.4 – Cycle de vie d'une transaction de crypto-monnaie basée sur le consensus PoW. L'utilisateur A génère une transaction pour l'utilisateur B. La transaction est stockée dans le pool de mémoire avec d'autres transactions non confirmées. Le *Miner* valide les transactions à partir du pool de mémoire et calcule un bloc. Un bloc valide est ajouté à la Blockchain

Annexe 4 : LEXIQUE

Terme anglais	*Terme francais*	*Définition*
Block validation	Validation de bloc	Opération informatique utilisée pour rendre un bloc infalsifiable et le valider dans une chaîne de blocs.
Consensus	Consensus	Mécanisme permettant de s'assurer que chaque nœud du réseau dispose bien de la même information avant d'enregistrer définitivement une opération dans la blockchain.
Cryptocurrency	Crypto-monnaie ou Cybermonnaie	Monnaie dont la création et la gestion reposent sur l'utilisation des techniques de l'informatique et des télécommunications.
Distributed ledger technology	Registre partagé distribué	Registre de données partagé entre tous les participants de la blockchain. Seule la validation d'une transaction par le biais d'un consensus peut opérer la modification de son contenu.
Fiat money	Monnaie légale	Terme désignant les monnaies étatiques ayant cours légal et un pouvoir libératoire. Elles s'opposent notamment aux crypto-monnaies, dépourvue de valeur légale propre.
Fintech	Entreprises de technologie financières	Cette appellation, contraction de « technologie » et « finance », désigne selon le contexte les entreprises de nouvelles technologies spécialisées dans la conception de services innovateurs dans le domaine de la finance, ou les services eux-mêmes.
Miner	Mineur	Personne physique ou morale mettant à disposition sa puissance de calcul informatique pour les besoins du minage.
Mining	Minage	Validation de bloc donnant lieu à la création de nouvelles unités de compte au profit du participant dont le bloc a été retenu par le réseau.
Node	Nœud	Matériel informatique relié à la blockchain qui est chargé d'effectuer les calculs. (v. également « mineurs »).

Bibliographie

[1] James A. Martin and John K. Waters. What is identity management ?

[2] Zheng, Zibin Xie, Shaoan Dai, Hong-Ning Chen, Xiangping Wang, Huaimin. (2017). An Overview of Blockchain Technology : Architecture, Consensus, and Future Trends. 10.1109/BigDataCongress.2017.85.

[3] ISO/IEC 24760-1 :2011(E). ISO/IEC, 20 pages, 2011.

[4] Zhu, X., Badr, Y., Pacheco, J., Hariri, S. : Autonomic identity framework for the internet of things. In : Cloud and Autonomic Computing (ICCAC), 2017 International Conference on. pp. 69–79. IEEE (2017).

[5] Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. : Blockchain technology :Beyond bitcoin. Applied Innovation2, 6–10 (2016).

[6] Christidis, K., Devetsikiotis, M. : Blockchains and smart contracts for the internet of things. IEEE Access 4, 2292–2303 (2016).

[7] Douceur, J.R. : The sybil attack. In : International Workshop on Peer-to-Peer Systems. pp. 251–260. Springer (2002).

[8] Vukolic, M. : The quest for scalable blockchain fabric : Proof-of-work vs. bft replication. In : International Workshop on Open Problems in Network Security. pp.112–125. Springer (2015).

[9] Shafagh, H., Hithnawi, A., Duquennoy, S. : Towards blockchain-based auditable storage and sharing of iot data. arXiv preprint arXiv :1705.08230 (2017).

[10] Cachin, C. : Architecture of the hyperledger blockchain fabric. In : Workshop on Distributed Cryptocurrencies and Consensus Ledgers (2016).

[11] Lamport, L., Shostak, R., Pease, M. : The byzantine generals problem. ACM Transactions on Programming Languages and Systems (TOPLAS)4(3), 382–401 (1982).

[12] Schneider, F.B. : Implementing fault-tolerant services using the state machine approach : A tutorial. ACM Computing Surveys (CSUR)22(4), 299–319 (1990).

[13] Fischer, M.J., Lynch, N.A., Paterson, M.S. : Impossibility of distributed consensuswith one faulty process. Journal of the ACM (JACM)32(2), 374–382 (1985).

[14] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F.Ang, and R. Ismail, “Blockchain Technology the Identity Managementand Authentication Service

Disruptor : A Survey,"International Journalon Advanced Science, Engineering and Information Technology, vol. 8,no. 4-2, pp. 1735–1745, 2018.

[15] A. Gruner, A. Muhle, and C. Meinel, "On the relevance of blockchainin identity management," 2018.

[16] A. Muhle, A. Gruner, T. Gayvoronskaya, and C. Meinel, "A Surveyon Essential Components of a Self-Sovereign Identity," 2018.

[17] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," 2018.

[18] M. Schanzenbach, G. Bramm, and J. Schutte, "reclaimID : Secure,Self-Sovereign Identities using Name Systems and Attribute-Based Encryption,"CoRR, vol. abs/1805.06253, 2018. [Online]. Available : http ://arxiv.org/abs/1805.06253.

[19] D. Baars, "Towards Self-Sovereign Identity using Blockchain Technology," Master's thesis, University of Twente, 2016.

[20] Abacus Protocol. [Online]. Available : https ://abacusprotocol.com/.

[21] BitID. [Online]. Available : https ://github.com/bitid/bitid.

[22] "Bloom Identity Protocol." [Online]. Available : https ://bloom.co.

[23] Cambridge Blockchain. [Online]. Available : https ://www.cambridge-blockchain.com/.

[24] Blockpass IDN. [Online]. Available : https ://www.blockpass.org/.

[25] Civic. [Online]. Available : https ://www.civic.com/.

[26] Sovrin. [Online]. Available : https ://sovrin.org/.

[27] Pillar. [Online]. Available : https ://pillarproject.io/.

[28] ID2020. [Online]. Available : https ://id2020.org.

[29] Enterprise Ethereum Alliance.[Online]. Available : https ://entethalliance.org/.

[30] KuppingerCole. `https://www.kuppingercole.com/`. Organisation internationale et indépendante d'analystes.

[31] ISO/IEC 24760-1 :2019. `https://www.iso.org/fr/standard/77582.html`, 2019. Sécurité IT et confidentialité — Cadre pour la gestion de l'identité.

[32] Cloud versus on-premise computing, January 2018. American Journal of Industrial and Business Management.

[33] B. Hay J. Dalziel S. Pope. A. Jøsang, J. Fabre.

[34] ANSSI. `https://www.ssi.gouv.fr/guide/mot-de-passe/`, 2020. L'ANSSI émet des recommandations de sécurité.

[35] CLUSIF. Gestion et gouvernance des identités et des accès, guide pratique - mise en oeuvre. `https://clusif.fr/publications/gestion-gouvernance-identites-acces-guide-pratique-mise-oeuvre/`, 2017.

[36] Greg Williams Edward Chow. Role Based Access Control (RBAC). https://www.coursera.org/lecture/advanced-system-security-topics/role-based-access-control-rbac-bYvzS, 2020. Advanced System Security Topics.

[37] Nazri Kama Kaiss Elghariani. Review on Agile requirements engineering challenges. https://ieeexplore.ieee.org/abstract/document/7783267/, 2016.

[38] Microsoft. Microsoft Identity Manager 2016. https://docs.microsoft.com/fr-fr/microsoft-identity-manager/microsoft-identity-manager-2016, 2016.