INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA INFORMÁTICA




LOGICAL ACCESS ANALYSIS

TONY JORDAN SERRA TEIXEIRA
Outubro de 2020

POLITÉCNICO
DO PORTO

Instituto Superior de Engenharia do Porto

LOGICAL ACCESS ANALYSIS

Tony Teixeira

A dissertation submitted in partial fulfillment of the requirements for the degree of Master of Science, Specialization Information and Knowledge Systems

Supervisor: Prof. Jorge Pinto Leite

Co-Supervisor: Prof. Paulo Proença

Júri:

Presidente:

[Nome do Presidente, Categoria, Escola]

Vogais:

[Nome do Vogal1, Categoria, Escola]

[Nome do Vogal2, Categoria, Escola] (até 4 vogais)

Porto, October 14, 2020

Dedicatory

To my wife, family and friends who supported me on this journey and who never let me give up in the most difficult moments despite the difficulties.

Resumo

A informação disponibilizada é um ativo importante no quotidiano das empresas, e como tal há que proteger essa informação de forma a dar o acesso somente às pessoas devidamente autorizadas.
A informação tem de estar organizada e num formato adequando de forma a poder ser útil a quem vai utilizar.
Infelizmente a rigidez da segurança com que os utilizadores se deparam para poderem aceder à informação quando chegam a determinadas empresas faz com que vários dias sejam desperdiçados até terem os acessos necessários atribuídos para poder trabalhar.
Os controlos de acessos dos utilizadores da Natixis são complexos e necessitam de uma atenção especial. É utilizada uma ferramenta de "Self-Service" que permite aos utilizadores solicitarem os acessos. Dada a quantidade de utilizadores, este procedimento obriga a uma atenção permanente e um esforço de gestão elevado.
A solução apropriada consiste em simular a implementação de uma arquitetura que visa facilitar a gestão dos acessos em várias perspetivas, nomeadamente na ótica dos utilizadores, das equipas de segurança, das equipas de controlos e em potenciais auditorias.
Essa arquitetura deverá ser uma alternativa à atual, fazendo uma análise crítica da arquitetura atual de forma a verificar-se quais os pontos que podem ser explorados e melhorados.

Os resultados obtidos na implementação da nova arquitetura permitiriam à Natixis reduzir significativamente o número de acessos disponibilizados aos utilizadores, facilitando os processos relacionados com o pedido de acessos e a sua manutenção.

Infelizmente devido ao momento que estamos a passar devido ao COVID 19, a implementação foi somente feita no ambiente de testes, não podendo tirar valores conclusivos sobre a possibilidade de implementar esta arquitetura no ambiente de produção, que é o ambiente utilizado pelos utilizadores finais da Natixis.

Contudo será possível que as equipas envolvidas no processo e que tenham acesso ao ambiente de testes possam expor as suas conclusões relativamente à solução apresentada.

Keywords: Informação, Segurança, Controlo de acessos, Self-Service, Auditorias

Abstract

The information provided is an important asset in the daily lives of companies, and as such, it is necessary to protect that information to give access only to duly authorized persons.

The information must be organized and in a suitable format to be useful to those who will use it.

Unfortunately, the rigidity of security that users face to be able to access information when they arrive at certain companies means that several days are wasted until they have the necessary accesses assigned to be able to work.

Access controls for Natixis users are complex and require special attention. A “Self-Service” tool is used that allows users to request access. Given the number of users, this procedure requires permanent attention and a high management effort.

One of the possible solutions is to simulate the implementation of an architecture that aims to facilitate access management from various perspectives, namely from the perspective of users, security teams, control teams and potential audits.

This architecture should be an alternative to the current one, making a critical analysis of the current architecture to verify which points can be explored and improved.

The results obtained in the implementation of the new architecture would allow Natixis to significantly reduce the number of accesses made available to users, facilitating the processes related to the access request and its maintenance.

Unfortunately due to the moment we are going through due to COVID 19, the implementation was only made in the testing environment, and it cannot draw conclusive values about the possibility of implementing this architecture in the production environment, which is the environment used by Natixis end users.

However, it will be possible for the teams involved in the process and who have access to the testing environment to be able to present their conclusions regarding the solution presented.

Keywords: Information, Security, Access Controls, Self-Service, Audits

Acknowledgement

First, I would like to thank my supervisor professor Jorge Pinto Leite and co-supervisor professor Paulo Proença for all the support given, despite the difficulties that arose during the process.

I would also like to thank Natixis for giving me the chance to work on a topic related to the company, and a special thanks to my colleague José Eduardo Bastos.

Finally, I would like to thank my wife for all the support she has given me throughout the process and has not let me give up.

Index

List of Figures

List of Tables

List of Acronyms

AD	Active Directory
DC	Domain Controller
DN	Distinguished Name
GUID	Globally Unique Identifier
IAM	Identity Access Management
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
OU	Organizational Unit

1 - Introduction

This chapter intends to give a general description of the subject addressed in this dissertation. In other words, creating a potential architecture that allows for more efficient management of the accesses available to users, simplifies the management of security teams and auditors. The subject is presented in Section 1.1 and then in Section 1.2, it sets out the objectives of this work. Finally, Section 1.3 presents the structure of the document.

1.1 Context

Information is present in the daily lives of companies, is essential for companies in the most diverse scenarios, including the exploration of new investment opportunities and the discovery and sharing of information.

Information has become the lifeblood of companies, and as such, it is essential for companies to protect themselves from a potential loss of information. The information must be relevant and in an appropriate format, to ensure that each stakeholder accesses only the information that concerns them.

Managing information within the enterprise has always been a vital and important task to support the day-to-day business operations and to enable an analysis of that data for decision making to better manage and grow the business for improved profitability. To do all that, clearly the data must be accurate and organized so it is accessible and understandable to all who need it. (Chuck Ballard, et al., 2014)

In view of this need, access controls have emerged, which should ensure that each user has access only to what is allowed, thus preventing each user from having access to information that he should not have.

Each company has its own architecture to provide access to its users, sometimes using internal platforms so that the user can request access so that they go through a validation flow before being assigned.

In this specific project, the identity management systems will be analyzed, and subsequently the solutions made available on the market to ensure a more efficient Identity and Access Management Systems, analyzing the pros and cons of each of the alternatives.

That will allow that at a later stage it will be able to say objectively whether the new architecture proposed in this project should be designed in one of these alternatives or not.

Identity management systems are usually information systems or technologies that are used by the company to ensure the management of identities.

The main objective of these systems is to ensure a set of important criteria:

- Identification (a user claims an identity)
- Authentication (a claimed identity is verified)
- Authorization (what the identity can have permissions for)

It is crucial that these systems can confirm the user's identity through their digital signature.

1.2 Objectives

Within the scope of this work, the existing tools on the market will be identified and analyzed, and an analysis of the strategy currently used by Natixis, a company in the financial sector, which has more than 15,000 employees spread across different countries, will also be carried out. As such, an exhaustive analysis will be carried out to analyze the architecture currently used and make a critical analysis to verify the points that can be explored and improved. Based on this analysis, a potential architecture will be realized to be implemented.

In summary, the following steps will be performed:

- **Analysis of the existing architecture**

Analysis of the existing architecture identifying the aspects that must improve to ensure the evolution of the management of access by identities.
Analysis of the current context of the company.

Identify some tools and features used in the context of the problem

Study and analysis of existing tools in the market to be aware of the tools that the market must make available, validating their applicability in solving the problem.

- **Simulate the development and implementation of a new architecture**

Design, if applicable, a new architecture to solve the problem.

Justification of each decision taken to build the architecture

Simulation of the development of an improved architecture that will make it possible to bridge the gaps identified in the current architecture.

- **Evaluate the developed architecture against the existing architecture and draw conclusive values from the comparison.**

The evaluation of the developed architecture is essential to know what impact the architecture will have on the teams' daily work.

The developed architecture was placed in the testing environment in a first phase, and one of the future works may be related to the transition from architecture to the production environment, which is the environment accessible to end users.

1.3 Document Structure

After the introduction Chapter, the document is organized into five more Chapters.

The second Chapter contains all theoretical information that will be addressed in the design of the potential architecture.

In the third chapter concerns an analysis of the management of the life cycle of users in a company, and some existing solutions on the market.

In the fourth Chapter is the proposal of the solution and its possible simulation is presented.

The Modeling and Simulation component is explained in the fifth Chapter.

Finally, the conclusions of this work are shown in the final Chapter.

2 - Problem

This thesis is developed to study the architecture used by Natixis to control accesses that are complex and need special attention.

A “Self-Service” tool is used that allows users to request access. Given the number of users, this procedure requires permanent attention and a high management effort.

The problem is to simulate the implementation of an architecture that aims to facilitate access management from several perspectives, namely from the perspective of users, security teams, control teams and potential audits.

In order to be able to simulate this implementation, it is necessary to identify and analyze the tools offered by the market within the scope of the simulation of this implementation in order to design a solution that is simpler for users to know which accesses to request.

For this study to be efficient and to meet what was intended, concepts such as the life cycle and identity management were addressed, as well as the systems that do this management and the systems that automate the process of assigning and removing accesses.

This section contains the context of this dissertation, in addition to the following sections:

Section 2.1 is an explanation of what identity management is and what systems exist to do that management (section 2.1.1).

As an example of these systems, Active Directory (section 2.1.2) and Enterprise resource planning (ERP) (section 2.1.3) were defined. These two sections will have subsections, where both concepts are presented, and their main characteristics are explained in more detail.

2.1 Identity Management

It is essential that companies ensure total control over resources and who accesses those resources, and as such, the concept of identity management appears to respond to this need.

Identity management is the organizational process capable of performing information exchange, identify, authenticate, and authorize individuals or groups of people to have access to applications, systems, or networks by associating user rights and restrictions with established identities (SearchSecurity, s.d.).

As the accounts are within the company's domain, it is simpler for security teams to ensure the management of the type of access for each identity, and to ensure that identities follow all internal security policies (Firewall Rules, for example).

The main goal of this concept is to ensure that only authorized users can access to specific resources / applications for which they have authorization.

2.1.1 Identity Management System

Evolution of computing systems from single user to multiuser machines led to the necessity of shielding users and running processes from one another.

Controlling access to computing systems is the first defense against disclosing information to unauthorized persons. Systems and network access are based on trusted methods for identifying users and programming agents (Benantar, 2006).

From a business point of view, it is important to manage the persons who work directly or indirectly for the company.

Identity management systems are usually information systems or technologies that are used by the company to ensure the management of identities.
The main objective of these systems is to ensure a set of important criteria:

- Identification (a user claims an identity)
- Authentication (a claimed identity is verified)
- Authorization (what the identity can have permissions for)

It is crucial that these systems can confirm the user's identity through their digital signature (Password or other type of authentication).

But these systems do not make miracles regarding identity theft.

Being proactive and vigilant is the best defense against identity theft and the invasion of privacy. This recurrent advice from the public broadcasting attests that security breaches can happen and no identity management system can provide full-proof security (Ty Mey Eap, Marek Hatala, & Dragan Gasevic, 2007).

As examples of identity management systems include Active Directory (AD) which is commonly used in companies.

2.1.2 Active Directory

AD is Microsoft's own directory service for use on Windows domain networks, and it is one of solutions used by companies.

It is a distributed hierarchical database structure that shares infrastructure information to locate, protect, manage and organize computer and network resources, including files, users, groups, peripherals and network devices (PAESSLER, s.d.).

One of the services provided by AD is named Active Directory Domain Services, which provides integrated large-scale authentication and authorization services.

Each part of the AD organizational structure limits either authorization or replication to within that sub-part.

2.1.2.1 How objects are stored and identified

Data stored within AD is presented to the user in a Hierarchical fashion like the way data is stored in a file system. Each entry is referred to as an object.

From Figure 1 we can get a sense of how the hierarchy of objects is made available in AD.

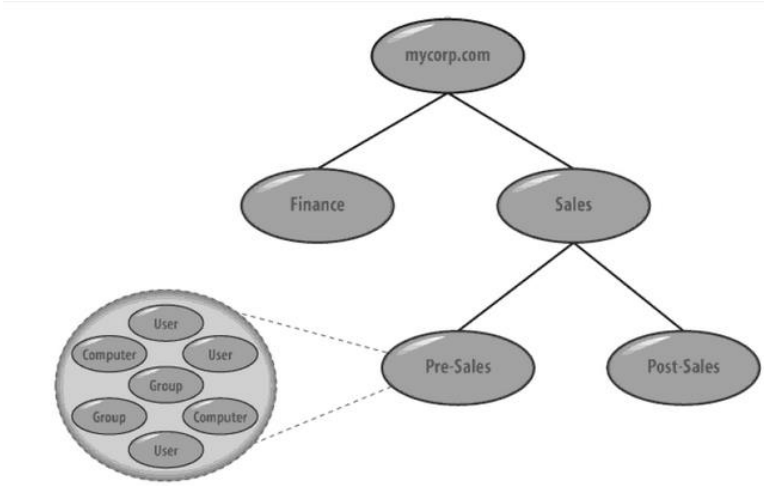


Figure 1 - A Hierarchy of object

Source: (etuturials)

Each object has to be uniquely locatable and identifiable, as such, each object has a Globally Unique Identifier (GUID) with 128-bit number assigned to these objects by the system in order to ensure the authenticity of each object (Desmond, Richards, Allen, & Lowe-Norris, 2009). Of course, this GUID is not easy to remember, so alternatively distinguished name (DN) is used, which are defined in the LDAP standard as a means of referring to any object in the directory and which are more commonly used.

Example of how root paths are defined:
dc=isep,dc=ipp,dc=pt

In the previous DN, we represent the root domain http://isep.ipp.pt using a comma to separate and prefix each part with the letter DC.

Another of the prefixes that are used a lot is the Organizational Unit (OU), which are widely used to represent the department where a user is inserted.

In figure 2 we have other prefixes that can be used and the one that is most used is the CN.

Key	Attribute
CN	Common Name
L	Locality Name
ST	State or Province Name
O	Organization Name
OU	Organizational Unit Name
C	Country Name
STREET	Street Address
DC	Domain Component
UID	Userid

Figure 2 - Attribute Types

Source: (Desmond, Richards, Allen, & Lowe-Norris, 2009)

2.1.2.2 Domains and Domain Trees

The logical structure of AD is built around the concept of domains.

The purpose of a domain is to break the directory into smaller pieces to control replication. A domain limits Active Directory replication to only the other domain controllers within the same domain.

An AD domain is made up of the following components:

- A based hierarchical structure of containers and objects
- A DNS domain name as a unique identifier
- A Security service, which authenticates and authorizes any access to resources via accounts in the domain or trusts with other domains
- Policies that dictate how functionality is restricted for users or machines within that domain

(Desmond, Richards, Allen, & Lowe-Norris, 2009)

The set of these components ensures that only duly authenticated and authorized users will be able to access company resources, being an extra layer of security in accessing information.

A domain controller (DC) can have authority for one and only one domain, and it is not possible to host multiple domains on a single domain controller.

A domain (example http://XPTO.com) is automatically created as the root node of a hierarchical structure called a domain tree, if XPTO added domains called Europe and the Americas, the names would be http://EUROPE.XPTO.com and http://AMERICAS.XPTO.com.

It would be literally a series of domains connected hierarchically, all using a contiguous name scheme and the tree of this domain would be known as the http://XPTO.com tree, with each domain tree being called by the name given to the root of the domain tree.

Each tree could manage and have access to resources in his own domain. All domains in a domain tree trust each other with transitive trusts (Desmond, Richards, Allen, & Lowe-Norris, 2009).

In the Figure 3 we can see how the domain tree would be implemented.

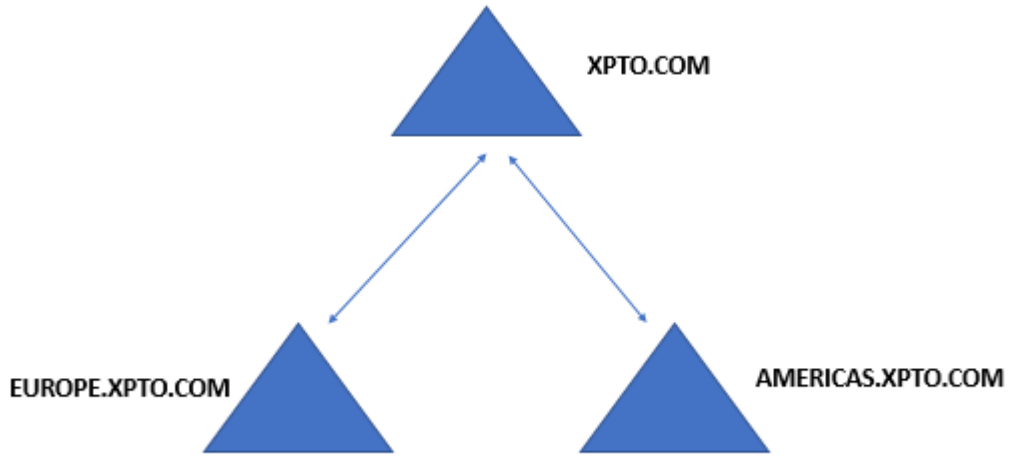


Figure 3 - The XPTO.com domain tree

2.1.2.3 Domain Controllers

Domain controllers are Windows servers with the Domain Controller role, which contain the Active Directory database and perform functions related to AD, including authentication and authorization.

Each domain controller stores a copy of the AD database that contains information about all objects in the domain storing the schema for the entire forest, as well as all information about the forest. A domain controller does not store a copy of any schema or forest information from a different forest, even if it is on the same network (PAESSLER, s.d.).

Figure 4 gives an example of how the Domain Controller can be implemented in companies.

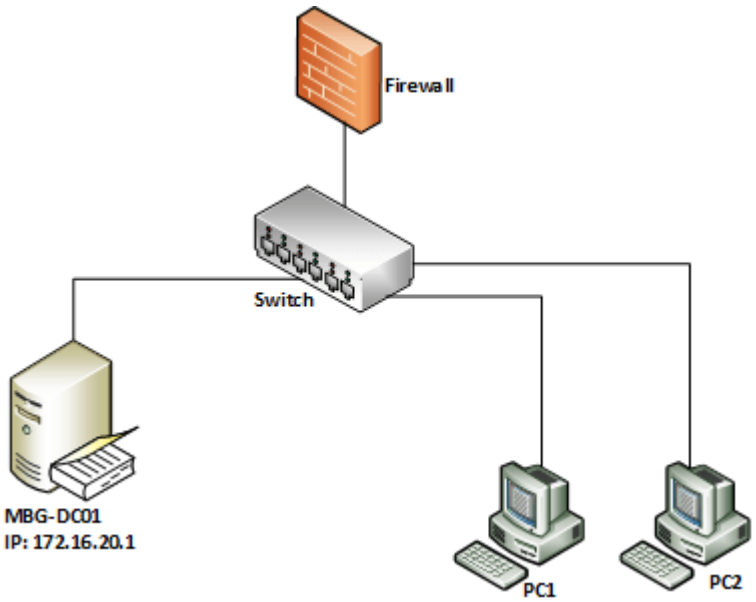


Figure 4 - Domain Controller implemented

Source: (Must be geek)

2.1.2.4 Forests

A forest is a security boundary within an organization and is the highest level in the organization's hierarchy. A forest allows delegation of authority to be separated into a single environment allowing the administrator to have full access rights and permissions, but only to a specific subset of resources. It is possible to use only a single forest on a network, and forest information is stored on all domain controllers, in all domains, within the forest (Desmond, Richards, Allen, & Lowe-Norris, 2009).

A domain tree is a set of domains, and a forest is a set of one or more domain trees, where these domain trees share common configurations, and the trees are all linked to transitive trusts.

Trust relationships do not compromise security in any way, they are used to allow access to resources, and these accesses need to be assigned by administrators. Once a trust is established, everyone in the trusted domain will also be able to access / request access to resources.

If you have a business unit that is independent and wish to be isolated, is possible to put the domain in a different forest.

In AD, you can never remove the forest root domain, or the forest will be irretrievably destroyed.

Figure 5 shows the transitive trusts between the domain trees.

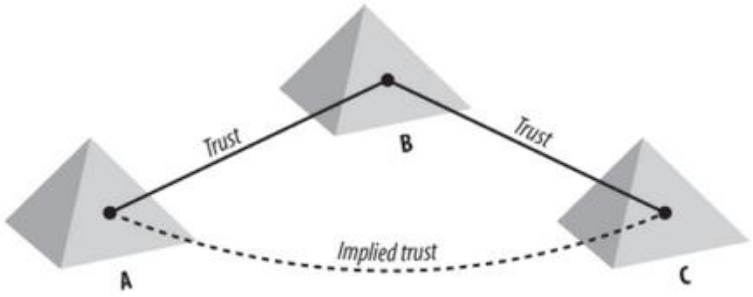


Figure 5 - Transitive trust

Source: (Desmond, Richards, Allen, & Lowe-Norris, 2009)

2.1.2.5 Organizational Units

An OU is a container in a domain that contains users, groups, computers, and other objects. You use an OU to store similar objects, making them easier to access and manage. An OU will always be contained within a single domain used to delegate control within functional groupings and should be used to implement and limit security and roles among groups providing the grouping of authority over a subset of resources from a domain.

You can also place sub-OUs within an OU - in a process called nesting - to create a hierarchical structure and facilitate management. OUs have group policies applied to it and are usually created to mimic the company's functional or business structure (PAESSLER, s.d.).

We can see Figure 6 an example of an OU structure of a specific company.

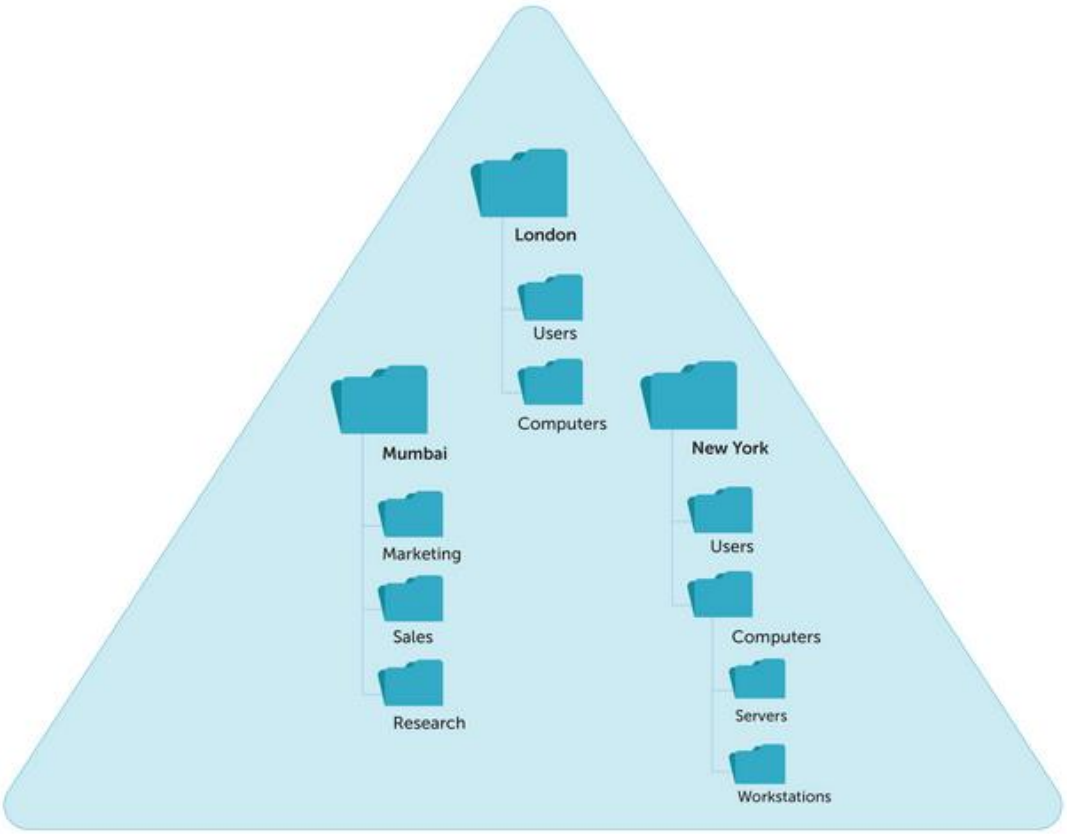


Figure 6 - Example of an OU structure

Source: Active Directory 360

2.1.2.6 Groups

In AD, groups are used as an extra layer to give access to company resources, groups must allow the management of user accounts, technical / application accounts, computer accounts and other types of groups within manageable units.

Adding this extra layer greatly facilitates the work of IT teams who must give access to users, since working with groups instead of managing each user individually helps to simplify the maintenance and administration of the company's internal network.

There are two types of groups used in AD, Distribution and Security groups.

Distribution Groups

Used to create an email distribution list, these groups can only be used with email applications in order to send email to a list of users.

As a rule, this type of group has a list of users as members, and it is more convenient for a user to send email to the distribution group and all members to receive email in their email box.

Security Groups

Used to assign permissions to the company's shared resources, which can be access to applications, printers, servers, files servers or any other shared resource in the domain. The role of security groups must be defined by the administrator of the AD, and the parameterization of this type of groups will determine what this group will actually give access to, for example a security group can be created to access a specific server, and only those who are members of the group can access the server.

Of course, the management of users who may be members of a certain security group is done by the teams responsible for managing the AD.

With the use of security groups, users can be assigned access by defining which security groups users can use, thus having control over shared access.

We can see in Figure 7 an example of some Security Groups created in AD.

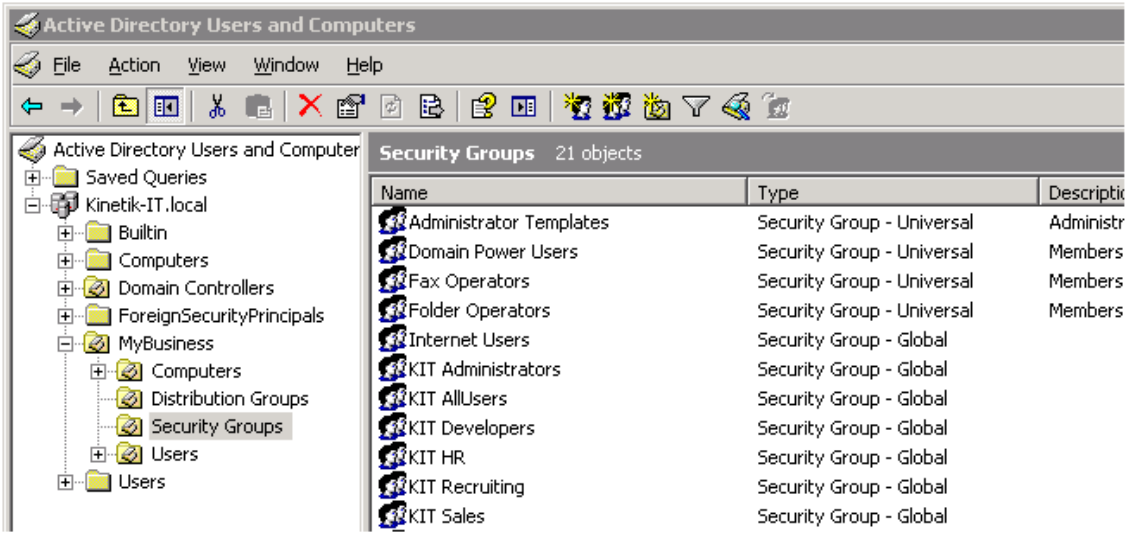


Figure 7 – Some examples of Security Groups

Source: (Access Security Blog)

2.1.3 Enterprise resource planning (ERP)

ERP are information's systems used by companies to integrate departments and functions of a specific company in a single system, we can see in the Figure 8 an example of an integration of ERP in a company.

Of course, it is a challenge for companies that ensure that ERP is fully adapted to the company's reality, as each department has its specificities.

By default, an ERP uses a single database that allows hosting all departments and data in the company and allows easier access to information (Ward, 2006).

Figure 8 - ERP integrated in a company

Source: (Ufamfsi2014)

But ERP as an identity management system also has a level of security that allows access to each user.

"A flexible organization is one that can use its existing resources and competencies to quickly respond to changing conditions in its environment without significant decreases in performance " (D'Souza, D.E. & Williams, F., 2000).

2.1.3.1 Characteristics of ERP

As we can see in Table 1, ERP has a set of characteristics that demonstrate why companies choose more and more of these Information Systems, forming a fundamental platform for the information management of an enterprise.

Table 1 Main characteristics of ERP systems

Characteristics	**Explanatory elements**
Integration	Interconnections between functions and hierarchical levels Interaction between the various processes
Completeness (generic function)	Wide range of functions Applicable to various types of firms Connectivity with the outside
Homogenization	Unique data referential Uniformity of human-machine interfaces Unicity of the system's administration
Real-time	Real-time update and consultation
Adaptability (flexibility)	Capability to follow rule and organization changes (made possible by parametering)
Openness (evolutionary)	Modularity Portability
Transversality (process-oriented view)	System designed in regard to the business processes necessary to achieve objectives Focus on value rather than authority flows
Best practices	System imbeds best practices in the field
Simulation	Business processes can be simulated

Source: (Sylvestre Uwizeyemungu & Louis Raymond, 2004)

2.1.3.2 Integration

As we can see in Table 1, it concerns the interaction between the various processes and the interconnection between functions and hierarchical levels.

Integration emerges as an important feature, as it is what distinguishes ERP systems from traditional Information Systems, eliminating what until then was the gap between the organization's functions, the result of little communication, or the great difficulty in communicating (Rowe, 1999).

Integration ends up promoting interactions within the system, which ends up resulting in greater efficiency in communication.

2.1.3.3 Completeness

Completeness turns out to be a complement to Integration and expanding the range of functions.

This allows the ERP to be applied to various types of firms and ensures connectivity with the outside.

Obviously, it is impossible for a generic system to be applicable and efficient in all types of companies, as it is common sense that an ERP must be adapted to the reality of the company.

The fact that it is customizable is what differentiates an ERP system, making it a great advantage for companies. The potential for configurations to customize is what differentiates ERP from conventional systems, allowing that before an ERP is implemented in a company it can be pre-configured with the desired alternatives ensuring that it is in the customer's image (Klaus, Helmut, Rosemann, Michael, & Gable, Guy G., 2000).

2.1.3.4 Homogenization

Homogenization will ensure that the processes are homogeneous, namely that the framework where the data is housed is exclusive, as are the system administration and the man-machine interfaces (Sylvestre Uwizeyemungu & Louis Raymond, 2004).

But as mentioned in the previous point, ERP systems allow to be customized and adapted to the reality of the company, and this is one of the main reasons that lead to homogenization.

2.1.3.5 Real-Time

The Real-Time feature is directly linked to updating and querying data in real time.

The operation of this feature is highly dependent on the successful integration of ERP (Sylvestre Uwizeyemungu & Louis Raymond, 2004).

The integration of ERP in a company must consider the Hardware and Systems used by the company, so that the use of ERP can be fully used.

Real-Time when implemented in a company will allow the same information to be made available in real time throughout the organization, regardless of whether it is after changes have been made or not.

2.1.3.6 Adaptability

The ability to follow rules and changes in the organization is another feature related to this characteristic.

The definition of rules will define how the system should behave, in turn, changes in the organization can always be readjusted when necessary, so that the implemented solution is always in the company's image.

2.1.3.7 Openness

This feature can show a lot the composition of an ERP, especially the modularity present in ERP systems, that is, it allows the system to be divided into different parts. A portability present in the ERP also defines its ability to be compiled or executed in different distinct architectures, namely in several different Hardware.

Openness is qualified with adaptability due to its modularity and portability (Byrd & Turner, 2000).

2.1.3.8 Transversality

Transversality is directly linked to the process-oriented view of a system ERP, and to the fact that systems ERP has several modules available (Carbonel, 2001).

You must perform an analysis for the systems used by the company before the ERP and be implemented in such a way that transversality is ensured, preventing anomalies from arising and calling into question or causing the ERP itself.

2.1.3.9 Best Practices

The best practices are made available in the fields by the ERP system, although some experts have the opinion that this characteristic cannot be considered a competitive advantage (Davenport, 1998) it is necessary to recognize that this characteristic fit perfectly for the common user.

With this feature, users' margin of error when filling in the fields will be reduced.

2.1.3.10 Simulation

As you can see in Table 1, this characteristic depends on the fact that the business processes are simulated.

Nowadays it is very common for companies that sell ERP systems to make demonstrations adapted to the client's business to show the ability to customize these systems.

3 - Identity and Access Management (IAM)

In this section, the concept of Identity and Access Management (IAM), life cycle management (3.1.1), Data Access Governance and Automatic Provisioning (3.1.2 and 3.1.3, respectively). In a phase subsequent to the increase of section 3.2 with Identity Access Management Providers, they will be analysed as alternatives available on the market and will be analysed in the subsections that follow, until section 3.2.2, a matrix is made to compare each of the alternatives analysed

3.1 Identity and Access Management (IAM)

Identity and Access Management (IAM) guarantees the authenticity and security of the user and ensures the management of the applications that the user must have access to or not.

It is used to guarantee that the user can authenticate and can access to the company's resources, for example, to applications (if has the permissions to).

As previously mentioned, AD is one of the identity management systems most used by companies, granting a specific type of permissions assigned to each user in order to ensure that the user only access in what he is supposed to has access.

To synthesize the work of the security teams to be able to do a better and more effective access management and their monitoring, it arises the need to implement an IAM in companies. That will allow to give users freedom to request the access they want and allow security teams not to be limited only to the allocation of access.

The main objective of this point is to analyze how IAM work, and what is their relationship with the identity management systems and the life cycle of these entities.

After realizing how IAM work, it becomes more efficient to be able to compare the solutions presented on the market in order to be able to check whether the existing solutions on the market could be a viable alternative to the internal tool used by Natixis.

3.1.1 Lifecycle Management

The life cycle of an identity is a set of steps through which an identity goes from its creation to its deactivation and later elimination.

As a rule, when a user arrives at a certain company, an account is created to identify him, that account will undergo a set of actions, for example, attribution of accesses, corporate email, attribution of password, etc.

But when an identity leaves the company, the suppression of accesses must be done in such a way that the set of accesses and parameters that have been defined for the user are unusable and that the user cannot access information that no longer concerns him.

Identity lifecycle management allows you to securely activate the correct application accesses from an access point granted during your life cycle at the company, which includes a potential change of function, addition or deletion of accesses when the link finish, we can see in the Figure 9 an example of an Identity LifeCycle.

Figure 9 - Example of an Identity Lifecycle

Source: (Evolveum)

3.1.2 Data Access Governance

A set of policies related to access control are duly defined in the IAM systems to ensure that only duly authorized users can request access to certain resources.

To meet the objectives defined by the companies, Governance emerged, which is nothing more than an extra layer of security that will allow users to request certain accesses through the IAM System used in the company.

As a rule, the Governance layer is associated with another layer of security, which is called provisioning.

The Governance layer must be modelled through profiles so that they are available on an internal portal so that the user can request accesses himself.

As we can see in Figure 10, the data access governance is directly linked to the identity life cycle and access control. Governance will allow efficient reports, reconciliation of access to users' accounts, review of access by those responsible and ensure that the policy is being followed in the profiles present in the governance layer.

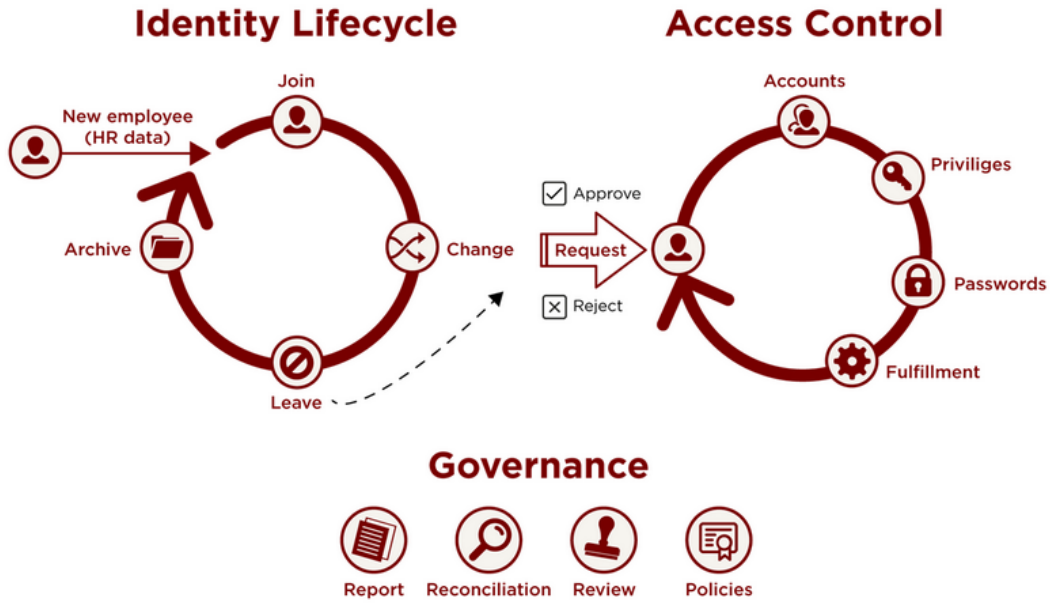


Figure 10 - Identity Lifecycle and Governance

Source: (RSA)

3.1.3 Auto Provisioning

Despite last section, the Governance Layer without the provisioning layer is not very useful. For the Governance System to be efficient, it must be added to a specific application access, whether in the AD or another directory used in the company.

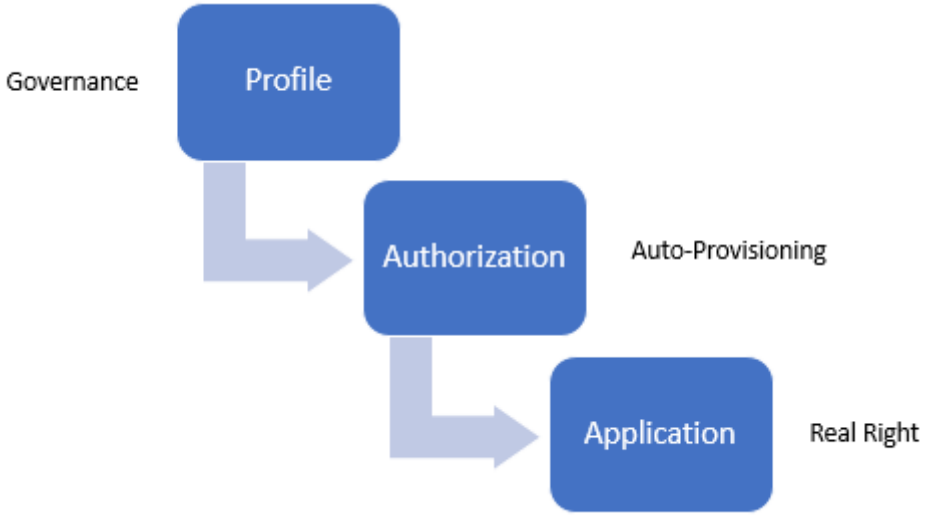


Figure 11 - Example of a Governance System with an Auto-Provisioning Authorization

Source: (Teixeira, 2020)

Of course, to ensure that the assigned accesses are duly authorized, there are always some rules that can be parameterized, namely, which is the validation flow for the profile to be assigned.

Figure 12 - Example of a Workflow concerning Permissions Request

Source: (Teixeira, 2020)

3.1.4 An IAM Provider

An IAM provider must ensure that identities and accesses work as a whole.

A user should be able to request access when he needs it, but that request can only be made while the user is working at the company.

For an IAM System to be effective, it must be linked to the business programs used by the company, namely the Human Resources program, in order to know when the user's contract will end or if the user will change teams.

The importance of these details is what will make security more rigid and the user's account will be suspended / inactive on the date of his departure, or that some of the accesses will be removed if he changes team or department.

From a more technical perspective, namely access, the IAM provider must be able to serve as a bridge between the identities and the different directories used in the company, whether they use different technologies or not, for example to access AD groups, access servers Linux, ERP's, etc.

The System must be able to automatically provision for each of the company's directories, making requests follow a specific Workflow and policies defined by the System Administrators.

This, in turn, greatly facilitates the work of auditors and compliance, as any request for access must be justified and validated in order to be in a more suitable format for potential audits or analyses.

Figure 13 - How IAM connect with the Corporate Programs

Source: (Meta-Byte)

3.2 Identity Access Management Providers

To improve access management for identities, systems have emerged on the market that ensure the management of identity and access in a more efficient way, the most popular IAM System providers are SailPoint, IBM, RSA and Core Security.

3.2.1.1 Sailpoint

SailPoint's identity management solution includes password management, compliance control, data access governance, access request, automated provisioning and Single Sign-On* (SailPoint).

*Single Sign-On (SSO) is an authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems (AuthenticationWorld.com).

3.2.1.2 IBM

The IBM Identity and access management includes authentication, privileged access management, identity governance and access management solutions. Grant access rights, provide single sign-on from any device, enhance security with multi-factor authentication, enable user lifecycle management, and protect privileged accounts (IBM).

3.2.1.3 RSA SecurID Suite

RSA SecurID Suite includes authentication, access management, identity governance, risk analytics and lifecycle management (RSA).

3.2.1.4 Core Security

Core Security provides a comprehensive suite of identity management and access governance solutions including authentication, access management, identity governance, password management, risk analytics and lifecycle management (Identity Governance & Administration (IGA) Solutions).

3.2.2 Identity Access Management Providers (comparation)

After checking Table 2, we can have a clearer idea of what each provider offers.

We can see that they are all very similar in terms of functionalities and allow the total management of the user's life cycle with the automatic attribution of accesses through profiles present in the governance layer.

We can see that they are technically very similar.

Table 2 - Matrix Identity Management Providers

	Authentication	Manage Password	Data Access Governance	Lifecycle management	Automated Provisioning	SSO	Multi-factor Authentication	Compliance Control
SailPoint identity management	X	X	X	X	X	X	unknown	x
IBM Identity and access management	X	X	X	X	X	X	X	x
RSA SecurID Suite	X	unknown	X	X	unknown	X	x	unknown
Core Security	X	X	X	X	x	unknown	unknown	x

4 - Proposed Solution

This chapter describes the proposed solution and simulation of the implementation presented in this dissertation.

The proposed solution is to reformulate the architecture of the accesses used at Natixis.

This solution aims to simplify all the processes of the various actors in the company related to access, namely users, security teams, control teams and annual recertifications.

For the solution meet what was intended, some clear objectives and premises were defined so that the simulation of the implementation would meet the intended objectively.

Section 4.1 gives a detailed explanation of how accesses are automatically provisioned by the access platform directly in the users' account.

Section 4.2 presents the existing access architecture, as well as the identification of potential problems identified in the current architecture.

In section 4.3, the main objectives for the new access architecture are defined, followed by a presentation of the same, as well as the main aspects that differentiate this model from the current model.

Section 4.4 identifies the actors and their relationship to this process.

4.1 Provisioning of Accesses

Natixis accesses are available on an internal company platform, where they can be requested by users.

However, technically there are some important aspects to highlight.

Each user can only have one identity, and each identity can have several types of accounts, for example an AD account and a Linux account, in the case of different directories, the accounts will be different but the login between them will be the same, this including the password that will be synchronized from one directory to another.

All Natixis identities are declared on a platform for this purpose, which is directly linked to the Natixis IAM, ensuring the life cycle of a user, because when a user leaves the company, this movement is declared on the identity platform that will communicate with the IAM.

For applications it works the same way, each application must contain a unique code, that code is defined by 3 characters (numbers and / or letters). All Natixis applications and their codes are hosted on an internal platform dedicated to the effect and which is connected to Natixis's IAM.

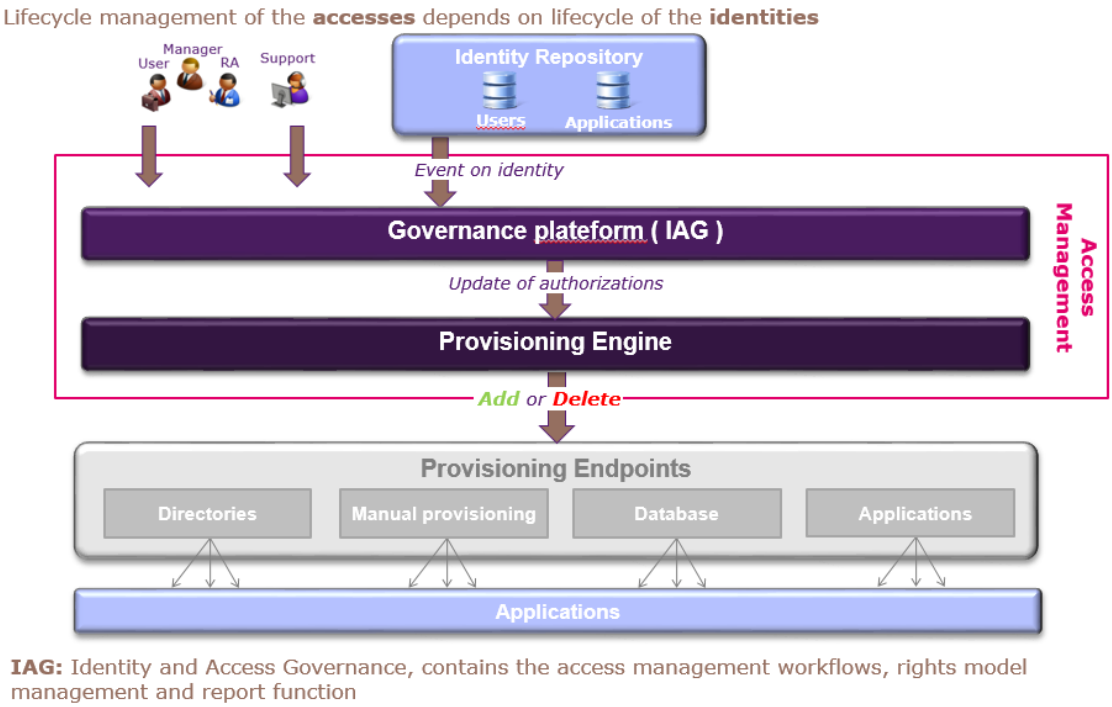


Figure 14 Lifecycle management of the user's accesses used in Natixis

The life cycle of users in a company varies from employee to employee, and it is important for a company that access is properly removed when an employee leaves the company.

After checking Figure 15 it is possible to check Natixis's IAM is guided by user and application identity platforms.

In the case of the users, the IAM will ensure that each user can request profiles on the access platform, and that these authorizations linked to theses profiles will be provisioned in the users' accounts.

In the case of applications, the IAM will incorporate information related to the application in the access platform and will allow the creation of profiles with the application code that may contain certain authorizations in the application.

Then comes the governance layer, which will contain all profiles and authorizations defined in the access platform.

Within the governance layer we will have a list of all application profiles that can be requested by users, and the authorizations associated with those profiles that should be linked to a specific Natixis directory, such as AD and Linux.

This layer is what will ensure the theoretical accesses defined for each user, that is, the accesses and authorizations that each user should have.

Figure 15 Workflow concerning Permissions Request (Theorical Permissions)

The provisioning layer is the layer that will ensure that the theoretical authorizations that the user has are converted into real authorizations, ensuring that the provisioning of these authorizations is done automatically, that is, that the authorizations are added or not according to the profiles that the user have on the platform.

The provisioning layer will communicate directly with directories and assign or remove authorizations in user accounts.

Moreover, Natixis directories, in turn, will communicate with Natixis applications, and will manage the accesses defined in the application.

Figure 16 Workflow concerning Permissions Assignement (Real Permissions)

4.2 Current architecture

Currently, Natixis contains a series of profiles that were modeled on the access platform, and which depend heavily on manual actions by the several security teams, namely the creation of groups in Natixis directories.

After the groups are created in the Natixis directories, it is necessary to model a profile on the access platform that will contain the created group, which in turn must give specific access to an application.

To proceed with the creation of a profile, it is necessary to fill in the following information:

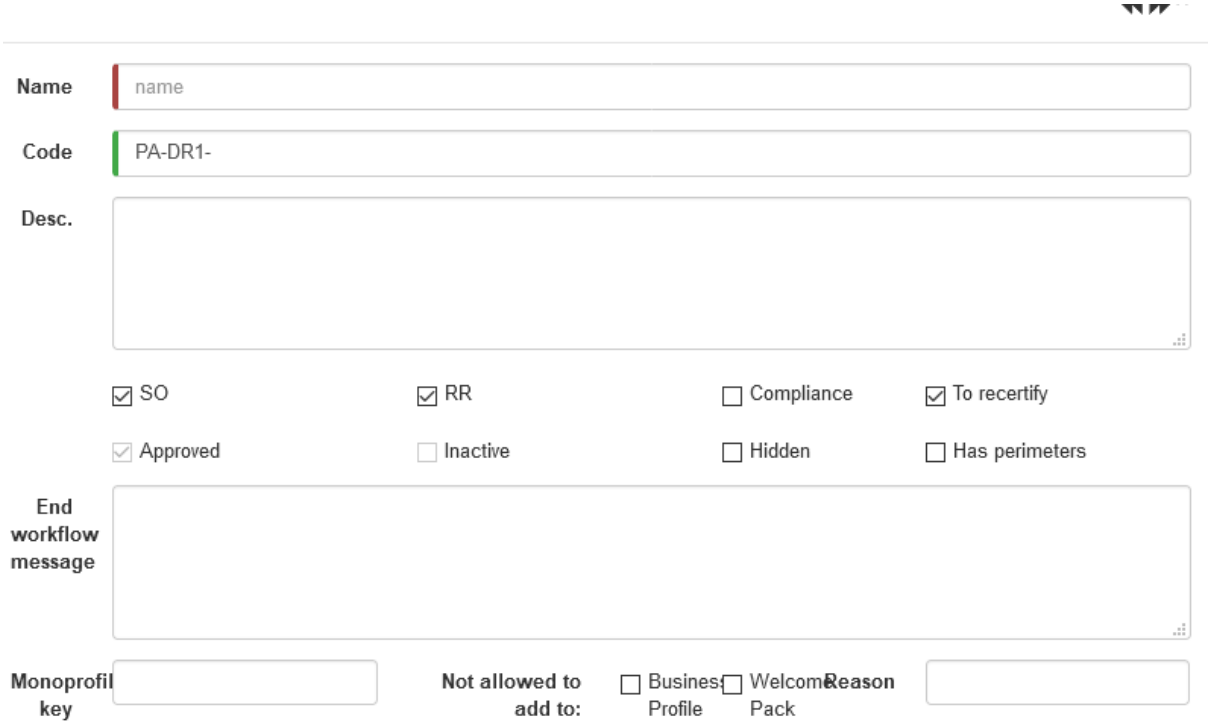


Figure 17 Creation of a Profile

In other words, we are talking about a truly manual procedure that depends on some teams so that it can be created.

In addition to being necessary to fill each of the fields, it is necessary to wait for the system to synchronize the created group so that it is possible to associate the authorizations to that profile and open the visibility to users.

After the profile has been created and visible, users will be able to request the profile on the access platform, the main problem is that in the current architecture each application can contain hundreds of profiles, with Natixis having thousands of applications, which makes it difficult for the average user to know which profile is best suited to their needs.

From the perspective of annual recertifications, it becomes complicated for a person responsible for an application to know for sure what each profile related to their application does for certain, and the annual recertification is based on an annual review to know whether or not users should have access to a certain profile / authorization.

Currently for the JIRA application, the common user has the following list of profiles that can be requested through the access platform:

Figure 18 Requesting a profile in the Access Platform

Despite the explained manual process, there are also templates that create certain profiles automatically, but that must be executed manually, but the end result will be the same, plus a profile linked to an application.

4.3 Primary objectives

In this section, the actors that most benefit from the implementation of the proposed architecture will be listed.

The main objective that led to the idea of creating a new access architecture, aims to increase efficiency and facilitate processes related to access by users, security teams, control teams, application managers and users' managers.

Then a small analysis is made of how it would be advantageous for each of these actors to implement the proposed architecture.

4.3.1 From the user's perspective

Facilitate the process for users to be able to request the access they really want.

Currently, the process for users to request access is long and complex, as users often ask for the wrong accesses that do not correspond to what would be intended.

The problem is essentially the high number of profiles available on the access platform that are linked to Natixis applications.

4.3.2 From security team's perspective

Security teams spend a lot of time maintaining profiles and analyzing which profiles the user really needs.

In short, improving efficiency and quality in the daily work of security teams, which can reduce the time wasted in resolving requests by users regarding what was mentioned in the previous paragraph.

4.3.3 From control team's perspective

The control teams work mainly on the quality of the accesses and the integrity of the accesses, that is, they are the main responsible for carrying out different monthly / quarterly / annual controls so that there is a strict control of the accesses that are attributed to the users.

An example of these controls are the annual recertifications that will be sent to users 'managers in a first phase and to those responsible for applications in a second phase, to validate the list of users' accesses.

With the proposed architecture, the extraction of data for recertifications will be in a more suitable format and with much less data to be processed, this is due to the number of profiles going down significantly.

The implementation of the new architecture will allow the control teams to make more types of controls, a lot of time is currently dedicated to launching extractions for recertifications due to the high level of data to be processed, which time can be usefully reused in the implementation new controls, always aiming to raise the bar in access controls.

4.3.4 From the perspective of user's managers

Facilitate the analysis of the access list to be validated in the recertifications by the users' Managers.

In the view of user managers, it would be beneficial if the listing of profiles to be validated were in a more appropriate format in which it was easier and more intuitive to confirm or not whether users should have their profiles assigned or not.

4.3.5 From the perspective of the responsible for applications

Facilitate the analysis of the list of accesses to be validated in recertifications by those responsible for Natixis applications.

From the perspective of those responsible for the applications, the implementation of this new architecture turns out to be even more sensitive and more advantageous.

Currently an application manager, can have more than 4 or 5 applications associated with it, now multiplying it by dozens or hundreds of existing profiles, and multiplying by the number of users who have profiles associated with those applications.

It turns out to be an exhausting and even thankless job for those responsible for the applications. With the implementation of the new architecture, the profiles to be validated by application would be only 3 and would be profiles with names much more appealing than the existing profiles, facilitating the task of those responsible for the applications.

4.4 Proposed Architecture

To automate and centralize Natixis accesses it is necessary that these accesses be created automatically, the only way to achieve this is through the creation of a template, in which this template will be executed in a tool used by security teams.

The templates must contain a name, a description, a template (the lines of code that will be executed), the ParamNumber that will define the number of parameters to be taken into account and the ParamDescription that will describe the parameters to be taken into account, below we can see the fields to fill in to create a new template.

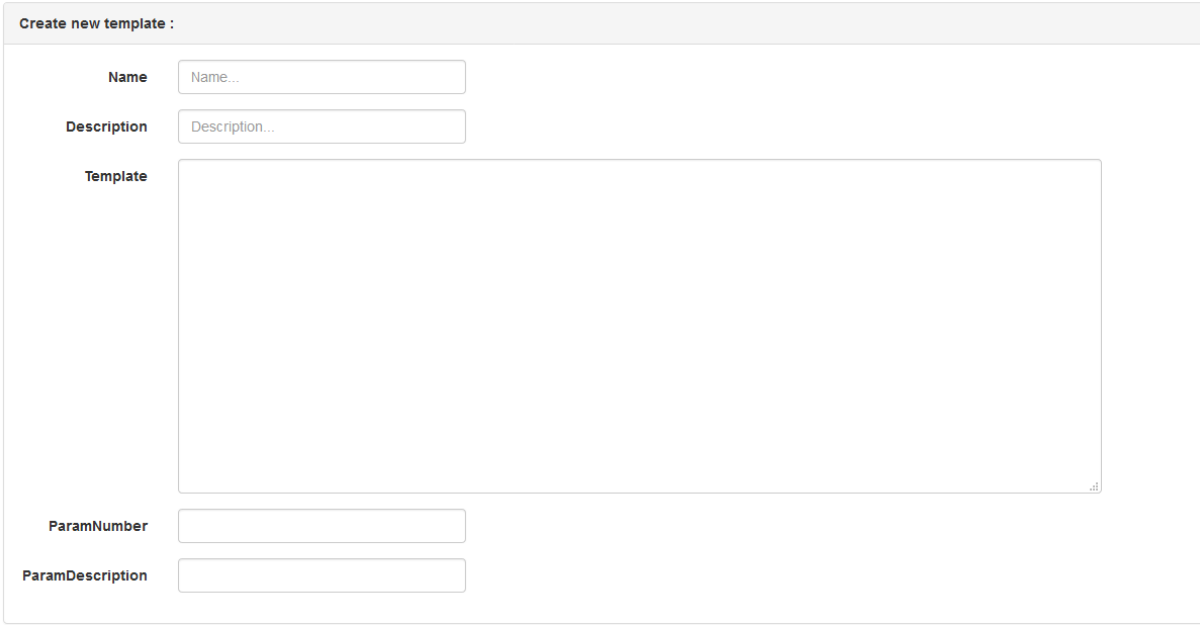


Figure 19 A Template

4.4.1 Creation of the profiles via template

The template created was made as follows:

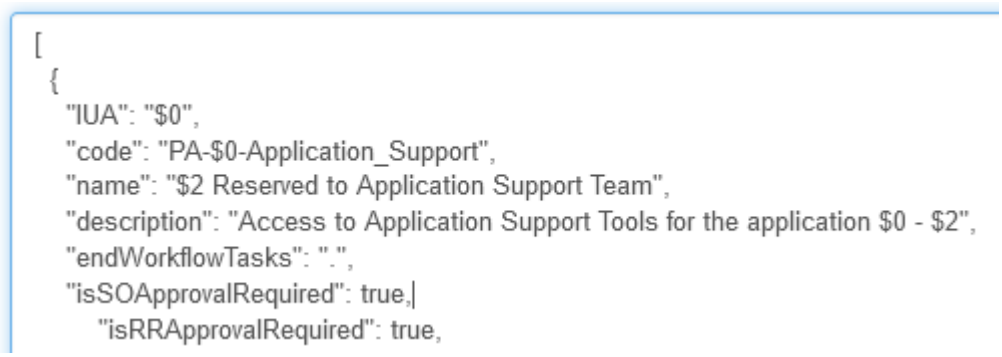
Name

TeamsByApplication (Tony)

Description

TeamsByApplication

Template:

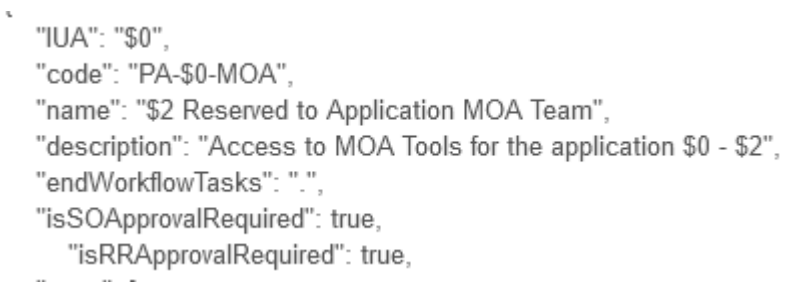


```
[
  {
    "IUA": "$0",
    "code": "PA-$0-Application_Support",
    "name": "$2 Reserved to Application Support Team",
    "description": "Access to Application Support Tools for the application $0 - $2",
    "endWorkflowTasks": ".",
    "isSOApprovalRequired": true,
       "isRRApprovalRequired": true,
```

Figure 20 Code summary for creating the Application Support Team profile

```
{
"IUA": "$0",
"code": "PA-$0-Developers",
"name": "$2 Reserved to Application Developers Team",
"description": "Access to Developers Tools for the application $0 - $2",
"endWorkflowTasks": ".",
"isSOApprovalRequired": true,
   "isRRApprovalRequired": true,
```

Figure 21 Code summary for creating the Application Developers Team profile



```
"IUA": "$0",
"code": "PA-$0-MOA",
"name": "$2 Reserved to Application MOA Team",
"description": "Access to MOA Tools for the application $0 - $2",
"endWorkflowTasks": ".",
"isSOApprovalRequired": true,
   "isRRApprovalRequired": true,
```

Figure 22 Code summary for creating the Application MOA Team profile

4.4.1.1 Explanation of the fields required for the creation of the profiles

IUA

Unique application code, each application has one and only one code. It is not possible to have more than one application with the same code.

$0

Variable defined when we want to execute the template to a specific IUA, that IUA will be $0 That is, this variable will only have 3 characters that will contain numbers or letters.

Code

Profile code that will be made available to users on the platform where access is requested, the format will be the same regardless of the application, and the only field that will be differentiated from application to application is $0.

The Code must be unique.

To simplify and make it more intuitive to know what each of the profiles created corresponds, it was decided to create profiles of the type:

➔ PA-$0-Application_Support

Aimed at Application Support teams, these teams are usually responsible for configuring authorizations in applications, so they have higher access than the Developers and MOA teams, especially in the production environment.

It is the teams that must respond and assist the access teams, when an access is not giving access to a certain authorization in the application, or if there is a specific problem in the application.

➔ PA-$0-Developers

Aimed at the teams of Developers, usually composed of application programmers, they have access to the lowest environments and do many tests before any resource goes into production.

➔ PA-$0-MOA

Designed for MOA teams, these teams are usually more functional, and are responsible for analyzing functional failures of the application, as well as working together with the application support teams and Developers in case it is necessary to improve some more functional or performance aspect of the application.

Name

Field where the name of the application is described and a brief introduction to whom the profile is intended.

Description

Brief description of the profile and what the profile gives access to and to whom it is intended.

EndWorkflowTasks

Once the profile is assigned, a notification is sent to the user, it is usually used when it is necessary to access a profile that gives access to a specific link, and the EndWorkflowTasks will contain the URL to connect to the application.

isSOApprovalRequired

When this field is required, it means that the user responsible will have to validate the profile assignment, that validation step is only the first step in the process to request a profile.

isRRApprovalRequired

Validation of the person in charge of the application, this is the second stage of validation and in these profiles, it will be the last stage before the profile is assigned to a user.

To Recertify

This field, although transparent when creating and executing the template, is active automatically.

Recertification is nothing less than the annual access control, which is divided into two phases.

The first phase is dedicated to the managers of the employees, who will have access to the list of profiles of their employees and will have to validate the list of accesses that they have assigned, being able to delete some profiles from the user's account and these will be automatically removed by the system.

The second phase is aimed to the responsible of the applications, where they will have the responsibility to validate the list of users who have access to their application profiles, the application recertifications also serve to help those responsible to identify profiles that may be obsolete.

Paps

Paps are the authorizations associated with each application profile.

They can be linked with any Natixis directory, for example AD, Linux, etc.

As a rule, it has 3 or 4 fields, the main fields being as follows:

- ➔ **Name**

Randomly generated code following the principle (it has changed in recent years): (**IUA**) - (**Environment**) - (**profile / group name**) _ (**PAP**).

The last field (“PAP”) is the only field that remains the same, the others are variable, Natixis having thousands of IUA / applications, 4 environments (Production, PREX, DEV, UAT), the name of the profile / group is also variable and does not follow a prefix.

➔ **itimProfileName**

It serves as a connector between the theoretical permissions and the real permissions, that is, the attribute that will link the Natixis directory with the IAM.


```
"paps": [
    {
    "name": "$0-PROD-EJ1-ngip$1_PAP",
    "content": "ngip$1",
    "itimProfileName": "PA_PRD_UNIX#NG-ngip$1"
  },
    {
    "name": "BQ4-PRD-DXC_MYCLOUD_$0_OPS_PAP",
    "description": "ATHENA mycloud access for $2",
    "itimProfileName": "PA_PRD_ATHENA-DXC-DXC_MYCLOUD_$0_OPS"
  },
    {
    "name": "DXC-HPROD-R08-DXC_MyCloud_Access_PAP",
    "description": "Accès à MyCloud (DevOps)",
    "content": "RCIB-DSI-GSA-DXC_MyCloud_Access",
    "itimProfileName": "PA_PRD_AD-RCIB-DSI-GSA-DXC_MyCloud_Access"
  },
{
    "name": "$0-HPROD-R08-$0_AdminSrv_HProd_PAP",
    "content": "RCIB-DSI-GSD-$0_AdminSRV_HProd",
    "itimProfileName": "PA_PRD_AD-RCIB-DSI-GSD-$0_AdminSRV_HProd"
  },
{
    "name": "$0-HPROD-EJ1-ngiu$1_PAP",
    "content": "ngiu$1",
    "itimProfileName": "PA_PRD_UNIX#NG-ngiu$1"
  },
    {
    "name": "BQ4-PRD-DXC_MYCLOUD_$0_DEV_PAP",
    "description": "ATHENA mycloud access for $2",
    "itimProfileName": "PA_PRD_ATHENA-DXC-DXC_MYCLOUD_$0_DEV"
  },
    {
    "name": "BQ4-PRD-DRP_ACCES_PAP",
    "description": "CONFLUENCE (shared platform)-Accès à l'outil (DRP)",
    "itimProfileName": "PA_PRD_ATHENA-DRP-DRP_ACCES"
  },
```


Figure 23 Code summary for create and associate the authorisations into the profiles created

UO’s

Organizational Units, codes are designated to identify the users' department and the Natixis hierarchy.

In this particular context, the definition of OUs will allow to select which OU's will have visibility of the profiles created, in this practical case the opening is restricted to DSI users, which is a more IT department and not so much aimed at Business.

However, as Natixis IT is in more than one Continent, more than 1 OU must be defined to open visibility, so as not to prevent IT users from actually asking for these profiles on the company's internal platform.

```
  "uos": [
    "SN00000018", "SN17332963", "SN29610441", "SN34244124"
  ]
},
```

Figure 24 Code summary for declaring the UO's that will have visibility open

After the template has been created, it is necessary to execute the template to a specific IUA so that the 3 pre-defined profiles created via the template are automatically created with the set of authorizations defined in the template.

We can see that the profiles do not exist when a "+" appears before the profile code and it is in green.

Example:

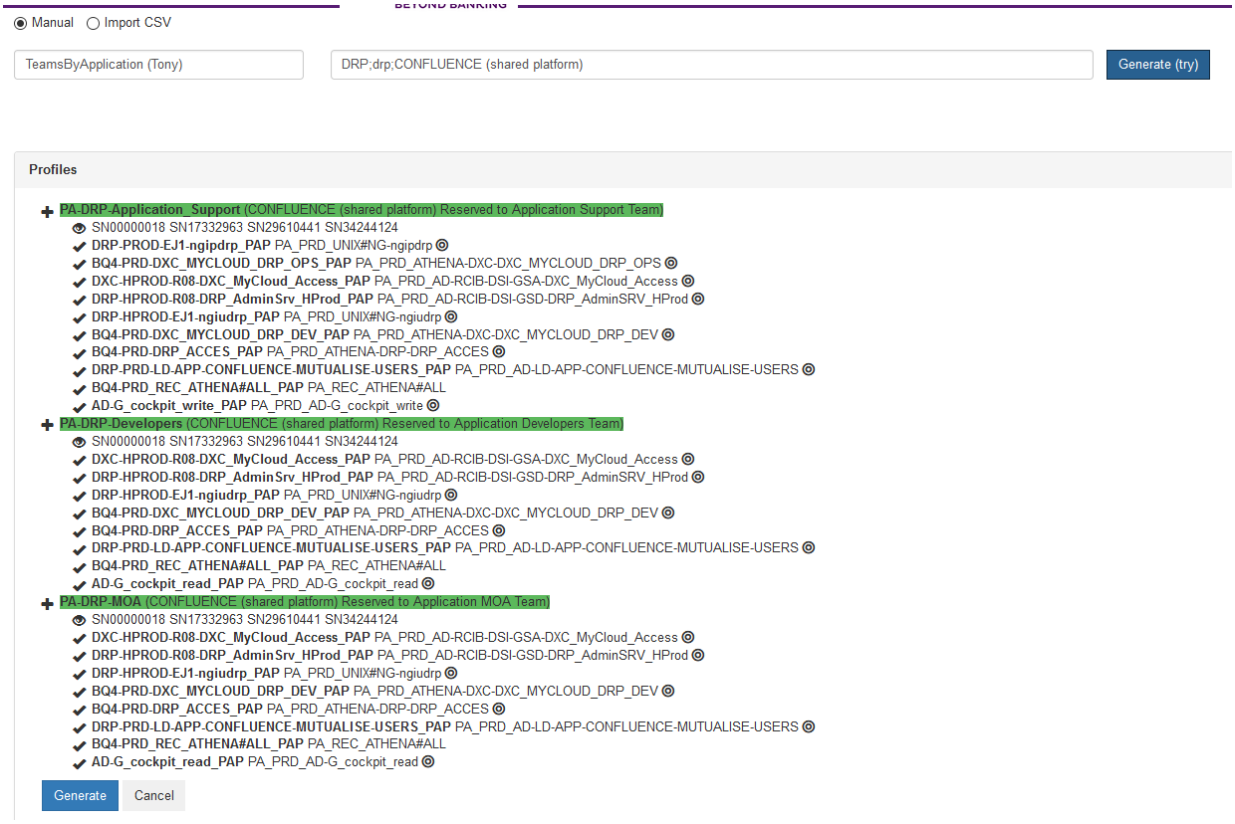


Figure 25 Generate the Template

After clicking on "Generate", it is necessary to choose the "Provisioning" option so that the profiles are created.
However, in the future work foreseen by the author, it is included that many of the existing templates can be synchronized to the profiles created in this project, making these profiles group the set of authorizations defined in the other templates.

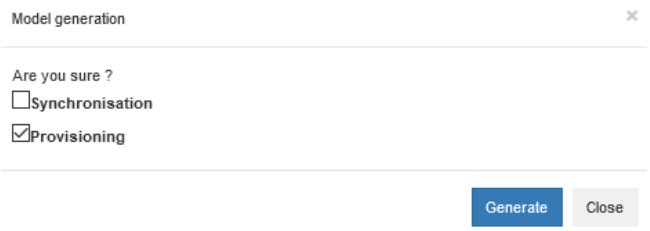


Figure 26 Generate the Template - Provisioning

After the template is executed, we will be able to verify that the profiles have been properly created and are already available on the access platform.

Only the users properly inserted in the defined OU's can request access to those profiles, always subject to double validation (Manager + Responsible for the application).

We can check the creation of profiles in the system:

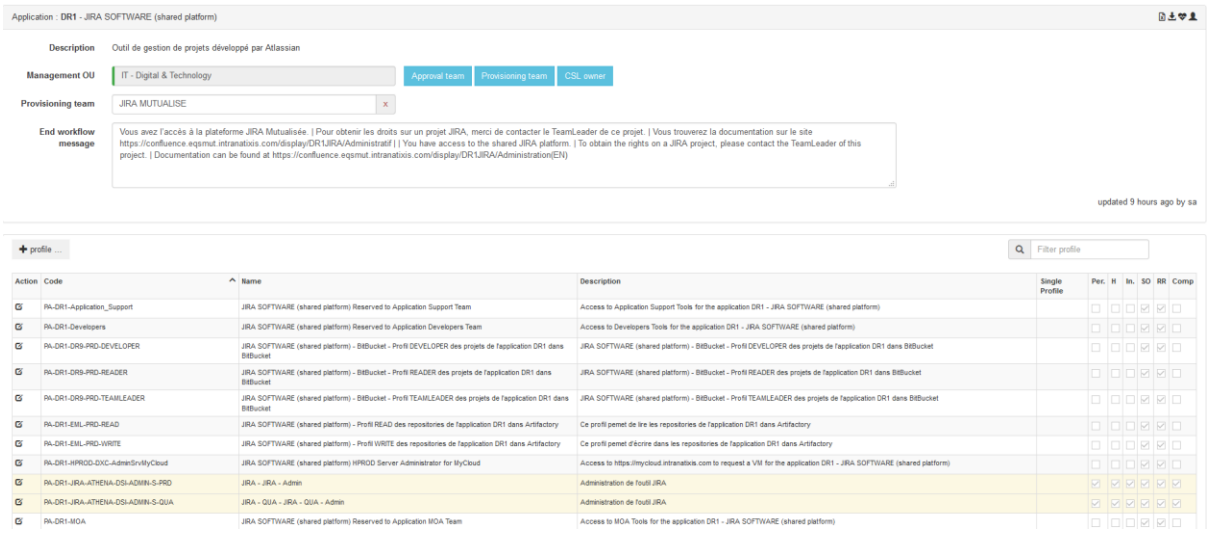


Figure 27 Profiles Created

After a more detailed analysis of one of the profiles created, we can verify that all fields selected via template, and the fact that these profiles are with open visibility.

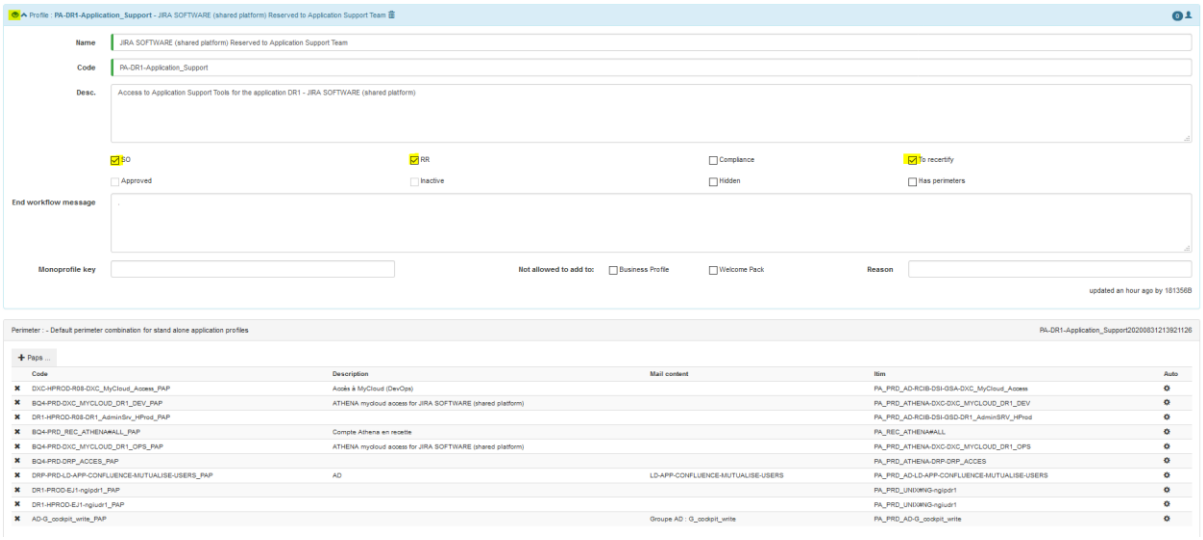


Figure 28 Checking the profile created in detail

After the accesses are modeled, they will be made available to users on the platform used to request accesses.

Figure 29 Access Platform (Before Implementation)

After the implementation of these profiles, the idea is to group the authorizations of the old profiles in the recently created ones, in order to make only the 3 most technical profiles available to users, as can be seen in the image below:

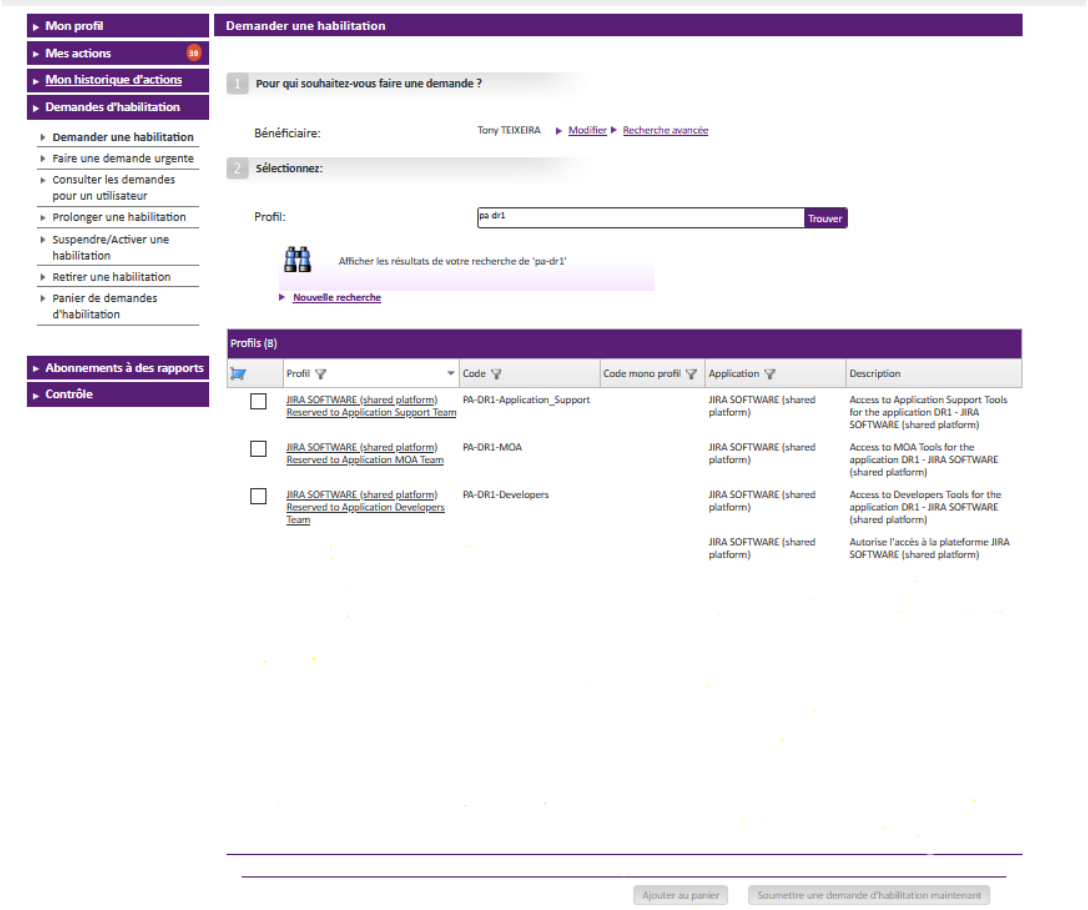


Figure 30 Access platform (as it is supposed to look after implementation)

The fact that three profiles are made available to the user turns out to be more intuitive for the user to know what to order on the platform.

The requests for access by users always pose some complications, namely it could happen that the requested profiles do not correspond to what was intended.

By reducing the range of options, the user will be able to easily identify the profile to be used, as he will have to ask for the profile corresponding to the team he belongs to. From the perspective of security teams, it is much easier to manage 3 profiles per application, than dozens or in some cases hundreds of profiles, not only for the maintenance of the profiles, but for the purpose of controls and audits and annual recertifications. Security teams maintain the profiles.

4.4.2 Edit some of the existing templates

There are some templates that are automatically executed and will create new profiles, keeping this in mind, a change was made to the templates in order to synchronize the authorizations for the profiles created in the template presented in this document.

The codes currently present in the 2 templates:

Template 1 - BITBUCKET Accesses (with corrections made and duly marked in bold and underlined in yellow)

```
[
 {
  "IUA": "$0",
  "code": "~~PA-$0-DR9-PRD-DEVELOPER~~",  -->  PA-$0-Developers
  "name": "$1 - BitBucket - Developer Profile",
  "description": "Dans le gestionnaire de sources BitBucket, accès en création et modification des codes sources destiné aux développeurs IT",
  "isRRApprovalRequired": true,
  "isSOApprovalRequired": true,
  "paps": [
   {
    "name": "BQ4-PRD-DR9_$0_DEVELOPER_PAP",
    "content": "DR9_$0_DEVELOPER",
    "itimProfileName": "PA_PRD_ATHENA-DR9-DR9_$0_DEVELOPER"
   }
  ],
  "uos": [
   "SN00000018",
   "SN17332963",
   "SN29610441",
```

```
            "SN34244124",
            "SN62068336"
  ]
 },
 {
  "IUA": "$0",
  "code": "~~PA-$0-DR9-PRD-READER~~",  --> PA-$0-MOA
  "name": "$1 - BitBucket - Reader Profile",
  "description": "Dans le gestionnaire de sources BitBucket, accès en lecture des codes sources. Profil destiné à l'IT (MOA…)",
  "isRRApprovalRequired": true,
  "isSOApprovalRequired": true,
  "paps": [
   {
    "name": "BQ4-PRD-DR9_$0_READER_PAP",
    "content": "DR9_$0_READER",
    "itimProfileName": "PA_PRD_ATHENA-DR9-DR9_$0_READER"
   }
  ],
  "uos": [
   "SN00000018",
   "SN17332963",
   "SN29610441",
            "SN34244124",
            "SN62068336"
  ]
 },
```

```
 {
  "IUA": "$0",
  "code": "~~PA-$0-DR9-PRD-TEAMLEADER~~", --> PA-$0-Application_Support
  "name": "$1 - BitBucket - TeamLeader Profile",
  "description": "Dans le gestionnaire de sources BitBucket, profil destiné aux Chefs de projets IT permettant l'administration du projet",
  "isRRApprovalRequired": true,
  "isSOApprovalRequired": true,
  "paps": [
   {
    "name": "BQ4-PRD-DR9_$0_TEAMLEADER_PAP",
    "content": "DR9_$0_TEAMLEADER",
    "itimProfileName": "PA_PRD_ATHENA-DR9-DR9_$0_TEAMLEADER"
   }
  ],
  "uos": [
   "SN00000018",
   "SN17332963",
   "SN29610441",
        "SN34244124",
        "SN62068336"
  ]
 }
]
```

Template 2 – EML is an application that allows the consultation of logs (with corrections made and duly marked in bold and underlined in yellow)

```
[
 {
  "IUA": "$0",
  "code": "~~PA-$0-EML-PRD-READ~~", --> PA-$0-MOA
  "name": "$1 - Profil READ des repositories de l'application $0 dans Artifactory",
  "description": "Ce profil pemet de lire les repositories de l'application $0 dans Artifactory",
  "isRRApprovalRequired": true,
  "isSOApprovalRequired": true,
  "paps": [
   {
    "name": "BQ4-PRD-EML_$0_READ_PAP",
    "content": "EML_$0_READ",
    "itimProfileName": "PA_PRD_ATHENA-EML-EML_$0_READ"
   }
  ],
  "uos": [
   "SN00000018",
   "SN17332963",
   "SN29610441",
        "SN34244124"
  ]
 },
 {
  "IUA": "$0",
  "code": "~~PA-$0-EML-PRD-DEVELOPPER~~", --> PA-$0-Developers
  "name": "$1 - Profil DEVELOPPER des repositories de l'application $0 dans Artifactory",
```

```
  "description": "Ce profil pemet d'écrire dans les repositories de l'application $0 dans
Artifactory",
  "isRRApprovalRequired": true,
  "isSOApprovalRequired": true,
  "paps": [
   {
    "name": "BQ4-PRD-EML_$0_WRITE_PAP",
    "content": "EML_$0_WRITE",
    "itimProfileName": "PA_PRD_ATHENA-EML-EML_$0_WRITE"
   }
  ],
  "uos": [
   "SN00000018",
   "SN17332963",
   "SN29610441",
          "SN34244124"
  ]
 },
{
  "IUA": "$0",
  "code": "~~PA-$0-EML-PRD-OPS~~", --> PA-$0-Application_Support
  "name": "$1 - Profil dédié aux équipes de prod appli de l'application $0 dans Artifactory",
  "description": "Profil dédié aux équipes de prod appli de l'application $0 dans Artifactory",
  "isRRApprovalRequired": true,
  "isSOApprovalRequired": true,
  "paps": [
   {
```

```
      "name": "BQ4-PRD-EML_$0_OPS_PAP",
      "content": "EML_$0_OPS",
      "itimProfileName": "PA_PRD_ATHENA-EML-EML_$0_OPS"
    }
  ],
  "uos": [
    "SN00000018",
    "SN17332963",
    "SN29610441",
    "SN34244124"
  ]
 }
]
```


In order for these templates to be executed and to modify the profiles created through the main template presented in this document, it is necessary to change the option defined in the template's execution, and configure the template to synchronize the existing profiles or create them if they do not exist:

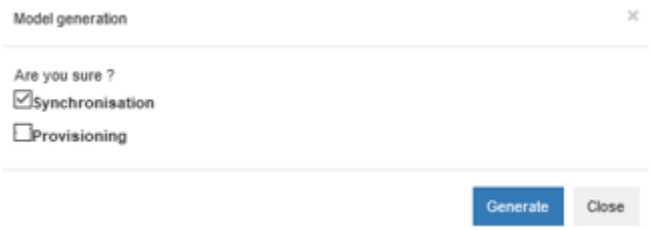


Figure 31 Generate the Template - Synchronisation

This option will ensure that the set of authorizations will be grouped into the 3 profiles created by the main template, that is, by editing these 2 templates, it has already been possible to delete at least 6 profiles that could be created via template for each of the Natixis applications.

5 - Experimentation and Evaluation

In view of the situation of COVID 19 currently present in our daily lives, it was not possible to carry out the implementation in the production environments, limiting the obtaining of feedback from people who have access to the testing environment.

This environment does not allow the assessment to be objective, as it is an environment where tests are carried out to analyze the behavior of the access platform in a lower environment, and only after verifying that everything is ok do a certain feature or functionality pass to the environment of production.

5.1 Evaluation Methodologies

In an initial phase, only security teams will have a perception of the impact of the new architecture on the access platform since they have access to the access platform in the testing environment.

For the security teams and some people in charge of the applications, the solutions were presented and the impact on their daily lives, the first impression was very positive and quite satisfactory.

But for the remaining actors involved it is impossible to obtain feedback, so for future work and for the assessment to be more conclusive.

It would be necessary to make a satisfaction questionnaire to the main actors involved in the process of requesting and maintaining access so that it can be possible to have a more demanding assessment of the benefits of the new architecture compared to the current one.

This questionnaire would have to be sent to a sample corresponding to at least 25% of the members of each of the teams involved to be able to analyze, equally, which teams have benefited most from the implementation.

5.1.1 Questionnaire for teams

As mentioned in the previous point, the sample should consist of at least 25% of the members of each of the teams involved. Since most teams do not have access to the test environment, the solution was presented to members who had access to that environment, below the questions asked from them.

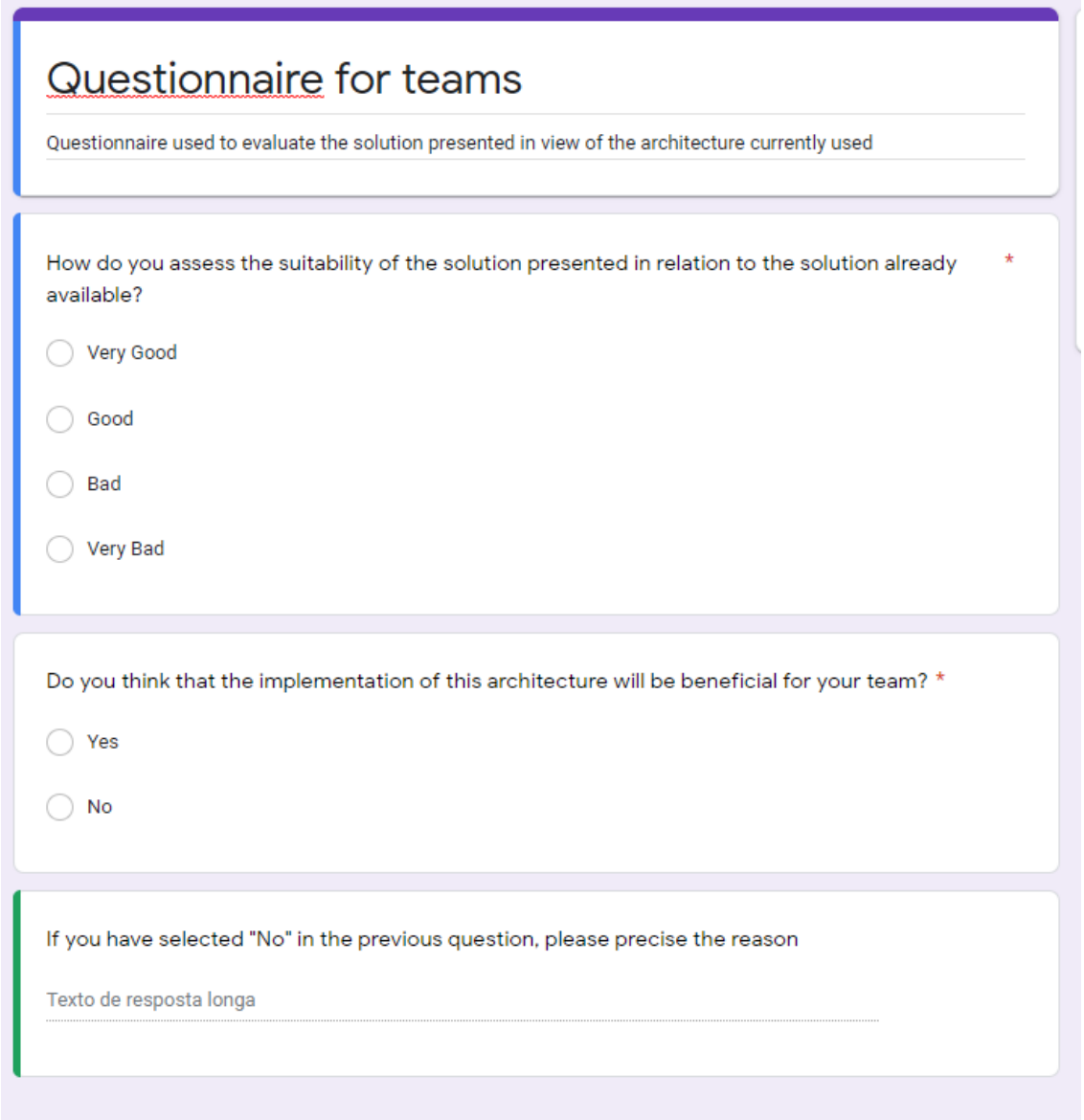


Figure 32 - Questionnaire for teams

This was the solution found in view of the situation in which we are currently living (COVID-19).

The questionnaires were sent so that the feedback is given by the sample.

6 - Future Work

As it was possible to verify, the execution of the main template must be done manually, but there are already templates that are executed automatically. Therefore, one of the main topics to be carried out is automatic execution since an application is declared on the Natixis application platform.

Another of the themes that should be carried out in the future, is the creation of a profile for the auditors or for the teams that need reading access to the application's resources, for example for code sharing between teams, etc.

The creation of these profiles was not possible due to the lack of elements, and this implementation would require a more in-depth and even more demanding analysis together with Business Lines, in order to identify which types of access would make sense to make available to auditors and other teams that only want read access.

Another aspect that will have to stay for future work is the implementation of the architecture in the production environment, as this is the environment where the accesses that are available on the portal are located, where users can request accesses.

References

Access Security Blog. (s.d.). Obtido em 22 de 02 de 2020, de http://www.accesssecurityblog.com/author/tvanstiphout.aspx

Active Directory 360. (22 de 02 de 2020). Obtido de https://www.windows-active-directory.com/the-structures-and-benefits-of-organizational-units.html

AuthenticationWorld.com. (s.d.). SSO and LDAP Authentication. Obtido em 18 de 09 de 2020

Benantar, M. (2006). Security, Identity, Management and Trust Models.

Byrd, T., & Turner, D. (2000). *Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct.* Journal of Management Information Systems.

Carbonel, M. (2001). *Dérives organisationnelles dans les projets ERP : les cas de Guerbet et Gaumont. Systèmes d'Information et Management* (Vol. 6).

Chuck Ballard, John Baldwin, Alex Baryudin, Gary Brunell, Christopher Giardina, Marc Haber, . . . Sandeep Shah. (2014). *IBM Information Governance Solutions.* IBM Redbooks.

D. B., R. J., A. R., & L.-N. A. (2009). *Active Directory, Fourth Edition.* O'Reilly Media.

Davenport, T. (1998). *Putting the enterprise into the enterprise system.* Harvard Business.

D'Souza, D.E., & Williams, F. (2000). *Toward a taxonomy of manufacturing flexibility dimension.*

etuturials. (s.d.). Obtido de http://etutorials.org/Server+Administration/Active+directory/Part+I+Active+Directory+Basics/Chapter+2.+Active+Directory+Fundamentals/2.1+How+Objects+Are+Stored+and+Identified/

Evolveum. (s.d.). Obtido em 22 de 02 de 2020, de https://evolveum.com/glossary/identity-lifecycle/

IBM. (s.d.). Obtido em 22 de 02 de 2020, de https://www.ibm.com/security/identity-access-management

Identity Governance & Administration (IGA) Solutions. (s.d.). Obtido em 22 de 02 de 2020, de Core Security: https://www.coresecurity.com/iam-products

Klaus, Helmut, Rosemann, Michael, & Gable, Guy G. (2000). *What is ERP? Information Systems Frontiers.* Kluwer Academic Publishers.

Meta-Byte. (s.d.). Obtido em 23 de 02 de 2020, de http://www.meta-byte.com/?p=390

Microsoft. (2017). Obtido de https://docs.microsoft.com/en-us/windows/security/identity-

protection/access-control/active-directory-security-groups
Must be geek. (s.d.). Obtido em 18 de 02 de 2020, de https://www.mustbegeek.com/understanding-logical-structure-of-active-directory/#.XlFQs0pUnIU
PAESSLER. (s.d.). Obtido em 16 de 02 de 2020, de https://www.paessler.com/it-explained/active-directory?utm_source=google&utm_medium=cpc&utm_campaign=PRT_EN_DSA_Pages&utm_adgroup=PRT_EN_DSA_Website_Pages&utm_adnum=dsa_en_03&utm_campaignid=790614948&utm_adgroupid=41599420059&utm_targetid=dsa-19959388920&
Rowe, F. (1999). *Cohérence, intégration informationnelle et changement : esquisse d'un programme de recherche à partir des Progiciels Intégrés de Gestion.*
RSA. (s.d.). *Identity and Access Management.* Obtido em 22 de 02 de 2020, de https://www.rsa.com/en-us/products/rsa-securid-suite
SailPoint. (s.d.). *SailPoint.* Obtido em 22 de 02 de 2020, de https://www.sailpoint.com/identity-management-solutions/
SearchSecurity. (s.d.). Obtido em 19 de 02 de 2020, de https://searchsecurity.techtarget.com/definition/identity-management-ID-management
Sylvestre Uwizeyemungu, & Louis Raymond. (2004). *ESSENTIAL CHARACTERISTICS OF AN ERP SYSTEM : CONCEPTUALIZATION AND OPERATIONALIZATION.*
Teixeira, T. (2020).
Ty Mey Eap, Marek Hatala, & Dragan Gasevic. (2007). Enabling User Control with Personal Identity Management. IEEE.
Ufamfsi2014. (s.d.). Obtido de https://ufamfsi2014.wordpress.com/2014/08/21/sistema-integrado-de-gestao-empresarial-erp/
Ward, C. J. (2006). *ERP: Integrationg and Extending the Enterprise.*