**A case study of Identity and Access Management implementation on an Oil and Gas company**

Fadhillah Moulita Andiani, Faizal Abid, Hendri

Universitas Bina Nusantara, Jakarta

# Abstract

Identity and Access Management (IAM) implementation address the problem of managing the life-cycle of digital identities in an organisation and with the growing of cloud accesses, internet of things (iOT) devices robotic devices perhaps rubbing more salt into the wound. A number of organisation, has testified that with a proper IAM implementation in their organisation, they are more having a better control of IT services in a day to day operation. The objective of this article is to describe a case study related to an IAM project at an Indonesian Oil and gas company by focusing on the challenges and the adopted strategies and solutions.

**Keywords**: *Identity Management, Access, Digital Transformation, Cyber Security*

# Business Challenges and Case Study

This section presents a case study related to an oil and gas company due to the specific issues that a case study has raised. An oil and gas company's particularity is its hierarchical structure. While business firms have a well-structured hierarchy with all business units reporting to a common top, oil and gas firms are more like a collection of nearly independent organizations operating in a common project or based on a project. This adds to the identity architect's work more difficulties and challenges such as managing internal processes and organization chart design.

The project's requirements are different in nature (access or identity management), area (business logic, workflows, user interface, architectural, integration) and priority (strictly necessary for the project to be delivered, can be moved into further phases of the project or a simple "nice to have").

Within complex global and national frameworks, the oil and gas business operates. Expansion into new geographic regions and environments— such as ultra deepwater drilling — creates new revenue growth opportunities. But the complexity and risk of the business operations themselves is also increasing. In addition, ever-changing regulatory frameworks imposed by various national governments— such as those designed to cap carbon emissions and those imposed after the 2010 Macondo disaster — add to the increasing complexity and scrutiny within which oil and gas companies operate.

One of the challenges is to increase visibility in complex operations to control costs and optimize employee, facility and asset performance. In some of the world's most physically and politically challenging environments, oil and gas companies operate. Add factors such as volatile market prices, fluctuating demand, complex compliance and regulatory regimes, projects involving multiple third-party suppliers, and a workforce with varying levels of education and skills — to name a few — and it is clear that oil and gas companies have some of the most complex operations on Earth.

In order to manage risks, control costs and optimize the performance of employees, facilitate and assets, oil and gas companies need to gain increased visibility into their operations.

"One strategy to achieve this was to adopt a' digital oilfield' or' integrated operations' to improve reservoir recovery, optimize production, and reduce economic, environmental, health and safety risks," explains IDC analyst Roberta Bigliani. "Initially this strategy was only associated with upstream, but businesses are increasingly focused on accessing and managing key asset-related data to improve decision-making from field to refinery across the entire enterprise."

# Introduction to IAM

Identity and access management has become one of the hottest topics for public and private sectors in IT departments since the 1990s. One of the reasons that boosted the demand for such services was the introduction of new privacy standards and individual information security to enhance the safeguarding of sensitive user information managed or exchanged by organizations. Governments and international institutions have released a set of regulations in recent years that have become de-facto standards for many business lines sectors: banking, public administration, telecommunications. There are (in order of publication) among the regulations that led to the change:

* Health Insurance Portability and Accountability Act (HIPAA) - 1996;
* International Convergence of Capital Measurement and Capital Standards - A Revised Framework (Basel II) - 2001;
* Sarbanes – Oxley Act (SOX) - 2002;
* European General Data Protection Regulation 2016/679.

Organizations need to start regulatory compliance processes with the introduction of these standards, which often have significant impacts on internal IT infrastructures, business processes and security policies. Identity and Access Management's first guiding concept is data aggregation. Essentially, it consists of storing user data in repositories such as relational databases, directory servers, object-oriented databases, or even flat files. It is called provisioning the process of managing user identities in identity stores, initializing their credentials and allowing them to access IT resources. Deprovisioning is the opposite, leading to de-provisioning.

The process of provisioning is usually complex. It involves rules of business and security and spans more than one store of identity. Following a top-down approach, the full provisioning process is designed and the result is a set of workflows and tasks. In the design phase, tools and methodologies help the architect of identity. Another topic of identity management projects is security auditing, which is required to trace user activity and enable automated remediation actions (near) in real time. It reduces security risks associated with duties segregation, weak security policies, or illegal access. Security auditing is essential if an organization is to meet any standing requirements

Historically, the business driver of Access Management was the need for one-sign-on (SSO). SSO is something the average user understands very quickly: simply enter your username and password once and access any application you want without reauthenticating (if you are allowed to use the service). This has brought up systems such as SailPoint that take care not only of the two basic authentication and authorization processes, but also of the related security features that make such solutions an essential component of today's IT infrastructure.

## Related works

In an identity ecosystem that supports secure and convenient access to online services, trust frameworks play a vital role by laying the foundation upon which the various participants can trust each other as desribed in (David Temoshok, 2018), In an identity federation’s trust framework, the individual components define how federation members will interact with each other. By defining the expectations members have of each other, a federation is able to support the trusted transactions for which it was created. For the purposes of this document, we have identified four components that characterize an identity trust framework:

* System Rules, which govern the interactions between members;
* A Legal Structure, which identifies the rights, responsibilities, and liabilities associated with participation in the federation;
* A way of Establishing Conformance across its members; and
* A way of Recognizing that Conformance.

The fundamental goal of any federated identity management model is to ensure a reliable authentication of subscribed users according to the defined policies of different cloud servers and to protect information from un-authorized accesses. (Faraz Fatemi Moghaddam, 2017). OpenID (D. Recordon, 2006) is one of the most popular federated authentication models that allows cloud users to use a single identity for accessing various services from different cloud servers and for elimination of managing different identities by cloud users. However, OpenID relies on an ID provider to generate a unique identity for each user. And the most challenging concern of Shibboleth is to provide different levels of authentication based on the sensitivity of data in various cloud servers. In fact, mapping between federated identity information with different levels of security in cloud servers based on defined policies is still the main issue in these types of federated identity management models.

# The purpose of this paper is to present IAM application in an actual case study, to describe the solution designed and implemented, and to focus on the lessons learned.

# Method To Be Used

## IAM Strategy - Trust Framework

“Trust framework” is a generic term often used to describe a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements. (Esther Makaay -SIDN, Tom Smedinghoff -Locke Lord LLP, and Don Thibeau - Open Identity Exchange, 2017).

Trust frameworks is a method for IAM strategy and focused on identity systems. “Identity System” it self means an online environment for identity management transactions governed by a set of system rules (also referred to as a trust framework) where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their identities. An identity system involces:

1. A set of rules, methods, procedures and routines, technology, standars, policies, and processes
2. Applicable to a group of participating entities
3. Governing the collection, verification, storage, exchange, authentication, and reliance on identity attribute information about an individual person, a legal entity, device, or digital object
4. For the purpose of facilitating identity transactions

The content of trust framework are role and functions. A role does not refer to a specific individual, organisation or entity, it is a set of functions and obligations that are assigned to a particular defined position within the context of the trust framework, such as “identity provider” or “relying party”. And the function assigned to each roles. Generally, the functions defined by a trust framework may be grouped into two general categories:

1. **Operational Functions**: Functions relating to defining, governing, and operating the identity system itself, which are assigned to one or more roles within the trust framework
2. **Participating Functions:** Functions concerning the participating entities within the identity system and the transactions and services involved, which are assigned to one or more participant roles.

# Proposed Solution

## IAM: project scope and inception

The objectives of the identity management part of the project were to :

* Automate current identity data flows between databases, primarily based on (often unreliable) batch procedures for all categories of users (employees, managers) ;
* Improve basic identity provision with ' business logic ' (workflows) ;
* Provide a central console to manage and monitor identity flows ;
* Implement a state regulatory’s password management component ;

From the customer’s point of view once delivered, the system should be able to:

* Detect the creation of a new entry in the employee database as a result of the registration of a new employee;
* Generate a new identity for a new employee in the identity and access management system with attributes taken from the source databases (name, surname, email address, ID number);
* Automatically' replicate' the identity of the contractor in all web applications;
* Similarly, the above also applies to other user categories (managers and employees)

The goals of the access management sub-project were to:

* Providing a common infrastructure for authenticating users and controlling their access to Web applications;
* Global single-sign-on and single-log-out;
* Common framework for tracking user activity (login, logout, access events);
* Providing a central console for monitoring user sessions. To sum up, from the point of view of the customer, the access management system above all means us

## Solution Modeling

This project specification details how the system works in terms of workflows, user interactions, user profile management, integration, architecture and infrastructure delivery. An IAM system model has to deal with at least the following topics:

1. define (digital) identities ;
2. identify functional user categories ;
3. define identity profiles (set of managed attributes) ;
4. define life cycles of identity (creation, modification, deletion, activation / deactivation) ;
5. map the organization chart of the customer on the functional organization of the solution ;
6. identify user and administrative roles as well as role hierarchies;
7. define workflows;
8. define the password management model;
9. define the (delegated) administration model;
10. design Defined field of the identity stores.

Digital IDentities (DIDs) are the core of the identity management model. The simplest idea for identity management is to create a new central repository of user profiles from the source databases where users are first created. The supplying system feeds the target databases and the applications that use this data. However, the management of DIDs has a different approach: the central system only has a kind of super-account that connects all the accounts that a user owns in the organization (Cross, 2010).

For instance, a manager has:

* Record in the HR database system;
* Account in the Windows network of the company;
* Account in the Web portal directory of the company. In this case, a DID is defined by the Identity Management system, using a unique identifier such as the Social Security Number or employee identification number. The user accounts are then connected to the DID. Depending on the rules and workflows implemented,
* whenever a change occurs in one of the accounts, or passwords, the modification is reported to all the other linked accounts (synchronization). In this way the information is updated automatically, and data inconsistency is avoided.

The following figure reports the relationship among the user's DID, roles, resources, and accounts established in the Identity Management system.

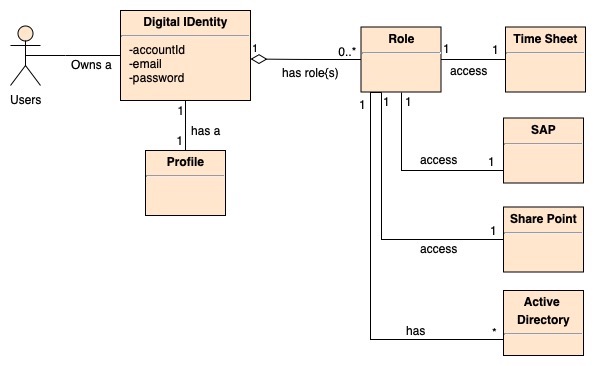


Figure 1. UML model of the relationship between the user, its role, resources and resource accounts

The first analysis showed three main user categories: government officials, contractors, and employees. Then, after a closer look, we identified the following exceptions:

* contractors are employed by the company and others are hired by temporary contracts;
* employees are employed in many departments (finance, marketing, IT, etc.);
* employees who have become managers;

# User Profiles

Once determined, the categories of identities need to be associated with user profiles. From an IAM point of view, a profile is a set of attributes related to one or more user accounts. Typically, a user profile can be roughly split into a “core” set, made of name, surname, full name, telephone number, email and a few other attributes. The rest of the attributes depend on the application context. An eCommerce site would probably add to the user's profile attributes like shipping and invoicing address, and/or paying information. As mentioned above, a DID is used to link together the user accounts. The DID is the super-account holding the links to the resource accounts.

Once determined, it is necessary to associate identity categories with user profiles. A profile is a set of attributes related to one or more user accounts from an IAM point of view. A user profile can typically be divided into a "core" set consisting of name, surname, full name, telephone number, email and some other attributes. The remaining attributes depend on the context of the application. Probably an eCommerce site would add attributes such as shipping and invoicing address and/or paying information to the user's profile. As mentioned above, the user accounts are linked together with a DID. The DID is the super-account that holds the resource accounts links. Consequently, the user entry on the IAM system itself has only the minimum set of attributes to manage.

The other attributes of the user profile are spread across the resources. The attribute stored in the IAM system built-in databases can be split into two categories. The first category is related to the application-specific attributes. In the Human Resource database, for example, there is a manager or employee's private address or telephone number, or their social security number. On the other hand, more specific information such as the ICQ or Skype ID number would be held on the employee's web portal. This latest information, which is well suited to portal applications, would be meaningless and cumbersome for the human resources system to manage.

Local attributes of this type of user are told to the resources. The second category of attributes is related to the attributes common to all the resources of the organization such as name, surname or email. The identity management system works on this set of common information, called global attributes. Impersonation was a special case that we had to handle in this project. Impersonation occurs when user A uses a service with user B credentials, so the service believes user B is effectively making transactions. This feature is primarily used by staff at the Help Desk when contractors report a critical issue and they need to reproduce the issue with the contractor's own account entering the application.

Although this practice is deprecated, it is often the last resort to understand and eventually fix the defect that causes a problem on the running system. Current Access Management products do not provide a temporary switch to another identity feature like this. Implementing it is rather complex and rarely used. More sophisticated SSO architecture should allow the primary account to be logged in and then a switch to the second identity that might choose to impersonate from a list of permitted identity. Our solution was to leave the behaviour of the Access Manager unchanged and provide another access (URL) reserved for operators of the Help Desk. The Access Management system ensures that only a few users access this particular URL and the application allows them to switch to the identity of the user. The Access Manager passes the true user account and the contractor account he acts on behalf of as the HTTP header for each HTTP request.

# Defined field

The next step in the analysis is to define Defined field after identifying local and global attributes. They are used by a remote resource-managed IAM system to link local attributes and correlate global attributes. For example, in the Human Resources Oracle database table employees, the u name column corresponds to the user first name attribute in the portal repository.

Defined field are used for:

* Customized transformation of attributes (introduction of some formatting in text, dates, etc.) ;
* generation of computed global attributes (e.g., fullname = concat(name, surname)) ;
* generation of local resources;
* Generate random, policy compliant passwords for newly created user accounts;
* Define authoritative account attributes for global attributes.

Defined field are designed to meet the customer's business rules and business analysts have a great responsibility in this area.

## Authoritative data source and flows

Another key concept in identity management is related to the authoritative data source for an attribute or set of attributes, which is worth introducing at this point. Although distinguishing between source database and target database is handy and common in each project, this distinction is made at attribute level by the identity management system, not at account level. For example, when hired, an employee gives his private email address, among other personal data. This type of information is subject to change, however, and he may enter a new email address in the personal profile form of the Web portal (where he uses it effectively).

In this case the web portal keeps the value of the e-mail updated, while the HR database has an ancient and invalid value. The IAM portal is the authoritative resource for the attribute, even if the HR database originates in addition to the other personal information. The worldwide SSO profile still needs to be considered in the presence of an Access Management scheme. The Identity Management System ensures that all customers who need to access a safe web server-an integral portion of the SSO authentication domain-in the Access Manager folder are integrated. To implement permission laws that can be built on user characteristics, the customer profile is subsequently enlarged in order to allow the Access Management System. For example, "only employees who have entered for page X can access the reserved area of application Y" Access Manager must have the information "accessible to page X" in the employee profile.

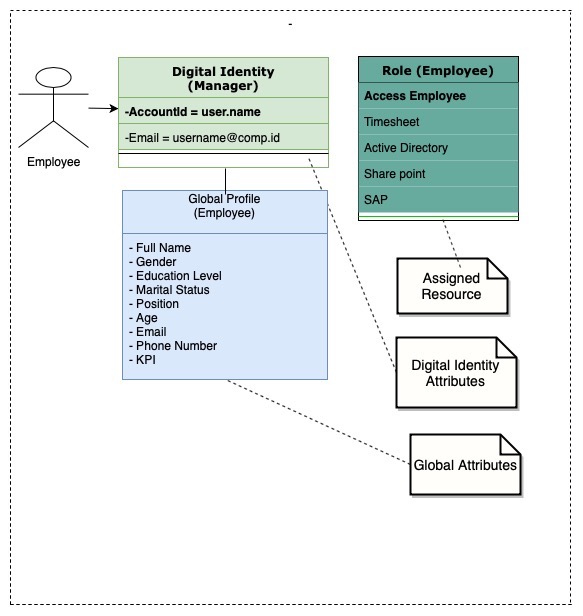


Figure 2. shows the UML model for the global profile for the manager

## Role Management

Role management is a key issue in the management of identity. User roles are the mechanism for associating a user's resources (Bartlett, 1995). One should allocate resources directly to the user without roles or alternative membership mechanisms. However, this is unpractical and complicated. Figure 2 clearly shows how role mediates resource allocation. Resources are the systems in terms of identity management where the identity of the user must be provided.

The problem with role modelling is to give the correct group of customers the correct function. Roles also have a strict obligation to access permits; to give a user a task means to give him access to a resource. By assigning a user a position for MANAGERS for instance, this user is effectively allowed access to the Windows database storage Active Directory

The capacity to identify hierarchies of positions is a lately presented feature of the role leadership subsystem. This enables to better design stuff like organisational graphs. We used this function and built the role tree shown in Figure 3:

# 

Figure 3. Role Hierarchy

## Business Process Modeling

The next stage in developing the IAM solution was to model company procedures. Processes are about how things have to occur. For instance, when a fresh worker is recruited, a sequence of activities must be conducted before he / she begins operating: attach his / her desk, PC and telephone, generate separate records in separate repositories, and so on (Scheer, 2012).

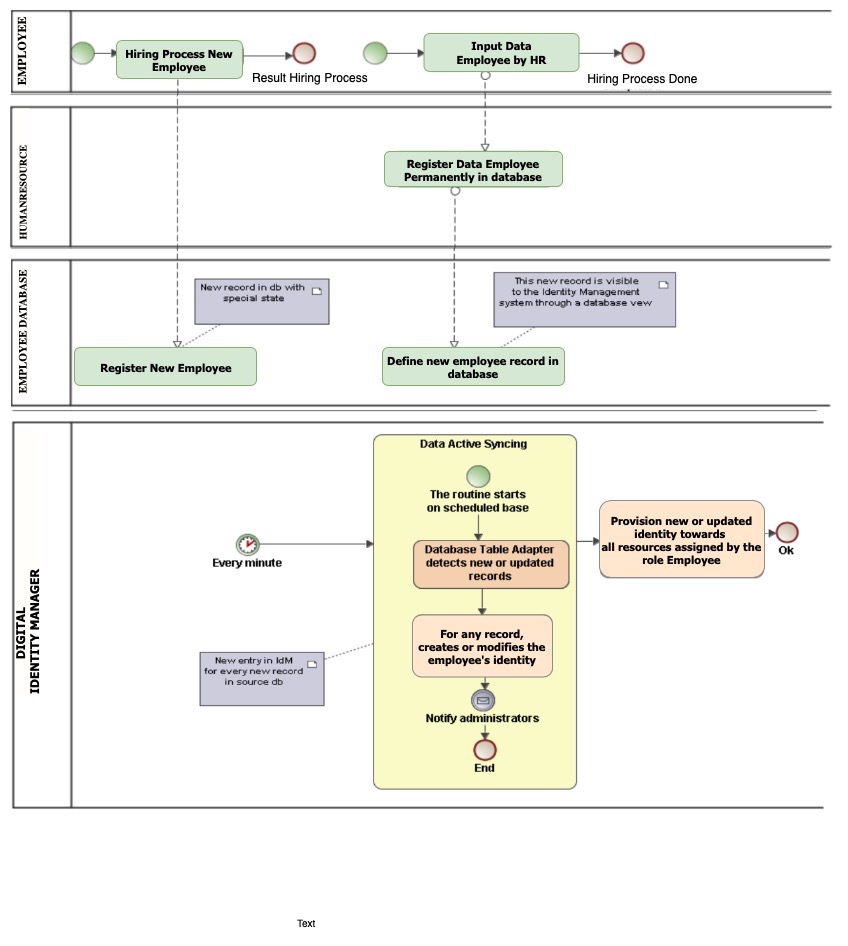


Figure 4 shows the registration process of a employee expressed in the Business Process Modelling Language (BPML).

In this situation, the method of establishing a fresh identity is quite straightforward. The Human Resources Division records a fresh worker through a web application, providing his or her private information and demonstrating the accountability of the worker. In his fundamental database, the request includes a fresh record. The Identity Manager detects the information incident and begins creating a new contractor workflow through the component Adapter and patented software called Adapter Active Sync. The idea used for company procedures by the Identity Manager is called workflow. For example, approvals, notifications and other specific actions taken on the resources are common extensions of product standard-providing workflows.

They essentially regulate how users are generated, altered, enabled / disabled and deleted if needed. There are, however, many other functions that are intended as workflows: reset password, modify password, lock / unlock account, and so on. Processes built from popular workflows Provided by the brand itself, represent the company guidelines already in place for user management as much as appropriate.

Workflows are developed and retained using a tool called Business Process Editor, like any other type of artefacts in Identity Manager. This graphic instrument makes it simple for the administrator to alter the laws. For example, it may arise the need to notify a new department of the creation of new employees. In this case, the workflow administrator will simply add a new activity with the email alias of the department as recipient called "Notify." It is not unusual to have firms that almost every year undergo a restructuring. Organizations especially appreciate having a tool to visually adjust the workflow after the constant modifications.

# Conclusion

In a real case research in this paper, we investigated the implementation of IAM. We have outlined the most prevalent mechanism for an IAM alternative, the primary problems and how they can be tackled.

Following are findings and conclusion that we have gathered: The IAM solution plays a key role in enabling interactions and transactions in today’s digital world; Some IAM capabilities are required for providing end-to-end security, thus aiding in determination and improvement of the security posture of the organization; Unfortunately, IAM implementations often suffer roadblocks or are ultimately stalled, mostly due to poor management of the program; However, by following the best practices detailed in this article, mishaps can be minimized or avoided completely, and the IAM solution implementation can be smooth, realizing maximum business value; and Compliance with industry regulations, reduction in IT administration costs and improvement in user productivity are some of the benefits of successful IAM solution implementation.

# References

Bartlett, C. A. (1995). Changing the role of top management: beyond systems to people. *Harvard Business Review*, 132–142.

Cross, D. B. (2010). Digital identity management. *Google Patents*.

D. Recordon, a. R. (2006). OpenID 2.0: A Platform for UserCentric Identity Management. *Proc. of the second ACM workshop on*.

David Temoshok, C. A. (2018). Developing Trust Frameworks to Support Identity Federations. *NISTIR 8149*.

Esther Makaay -SIDN, Tom Smedinghoff -Locke Lord LLP, and Don Thibeau - Open Identity Exchange. (2017). Trust Frameworks for Identity Systems. *OIX White Paper The Trust Framework Series*.

Faraz Fatemi Moghaddam, P. W. (2017). A Policy-Based Identity Management Schema for Managing Accesses in Clouds. *2017 8th International Conference on the Network of the Future (NOF)*.

Scheer, A.-W. (2012). ARIS business process modeling. *Springer Science & Business Media*.