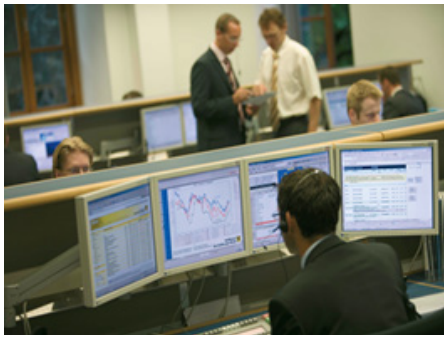
evidian

IAM
A strategic tool to meet the requirements of financial sector

Bull
atos technologies

Contents

"Extend your information systems beyond the traditional boundaries of your business premises in total security"



“Synopsis of a multinational bank”

The following case study concerns a bank with thousands of employees over a dozen countries worldwide. Its project is to provide its customers, subsidiaries and partners with secure fund management services. Opening the access to the information system is one of the cornerstones of the company’s development. However, it also creates various problems regarding the security and user lifecycle management.

To deploy such a project, the bank has listed specific requirements: it must be able to create, modify and delete a new client or partner, generate access rights to various applications that will be assigned to him throughout his contract, ensure the availability of the people validating the authorizations and the traceability from end to end for all actions performed.

In addition to the problem mentioned before, employees within the company must also be taken into account. Indeed, they often own high-level access rights that exceed their roles and are conveyors of security failures.

To meet regulatory requirements, the key players in financial markets and insurance companies must implement measures to manage their operational risks. These requirements particularly translate into implementing mechanisms to strengthen the access control to the information system in order to protect the integrity and confidentiality of data.

Concurrently with the increasing number of computer applications – and therefore the number of passwords to remember – these companies are looking for secure solutions to increase employee productivity and reduce the helpdesk workload. These solutions must also allow the implementation of strong authentication methods to ensure maximum security. Therefore, it is imperative to manage an integrated and scalable solution in order to avoid penalizing the end users or the services administering and operating these solutions.

Identity and Access Management has become a major concern for the governance of companies from the financial sector and is regularly displayed at the heart of the economic news.

The changing face of identity and access

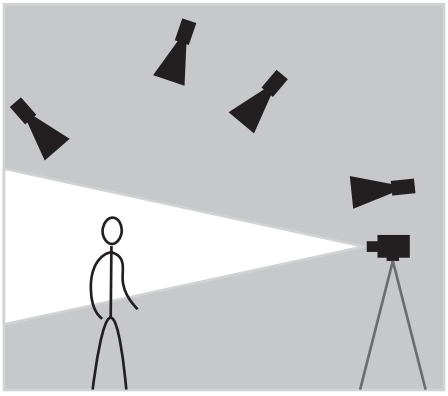
In the light of recent technological developments, companies are finding themselves with more and more opportunities to develop their activities. The emergence of the world of the Web, the Cloud and many different ways to access information is enabling companies to implement business processes and activities that go way beyond the traditional boundaries of technical environments.

The problems that a bank can encounter are the same that may be faced by an insurance company, a group of hospital or a professional industry body. But these organizations can now implement centralized, shared solutions, accessible by all their various branches, subsidiaries and partners.

However they still need to be reassured about security, user-friendliness and traceability when it comes to accessing services, without seeing a huge increase in their administrative overhead. It is imperative for them to be able to delegate the administration of local users to middle managers or even directly to end users, by allowing them to submit their own requests. And validation processes are essential to ensure the merits of these requests.

It is also important to be able to reuse current infrastructures, without having to modify existing elements such as the web site.

Consider a bank intending to extend its information system in order to offer its customers and subsidiaries a fine-grained and secured management of identities and accesses.



To meet its needs, the solution will have to:

- Offer an 'account creation' request system,
- Provide secure access to recently created accounts by means of a time-limited activation system, allowing the end user to set their password in line with a corporate password policy,
- Have a system of assigning user rights based on the job-related needs of each user, with control measures to ensure that each user only has the rights he or she needs for their job and no more. For example, the aim could be to isolate « front office, middle office and back office »,
- Allow the 'business' – in other words, users' immediate line managers – to apply for rights on their behalf, or to confirm/ deny requests made by their employees,
- Allow an easy delegation of administrative tasks related to users life cycle to specific cells,
- Offer a wide range of strong authentication methods adapted to the sensitivity of performed actions,
- Allow users not having to remember additional passwords in order to do their work, without jeopardizing corporate security,
- Allow to continue using the existing Web portal without it needing to be modified to provide the functionality described above.
- Have advanced reporting and traceability tools in order to allow governance and compliance with the regulations in case of an audit.

Obviously, this is not an exhaustive list of the features that a bank will require from the identity and access management solution that it needs to implement, but it does provide a reasonably representative overview of the heart of the problem.

In the following sections, this white paper shows what Evidian can offer to help you solve these problems.

The Evidian proposal

Evidian's proposal is based around its Identity and Access Management (IAM) Suite. The Evidian IAM Suite responds positively to the needs set out above, and goes beyond the points shown especially when it comes to the governance of identity and access management.

Evidian IAM Suite is a set of products developed entirely by Evidian, featuring native integration and covering all the functionality shown in the diagram below.

The ability to define a governance policy for identity and access management is at the very heart of Evidian IAM Suite. It lets you manage who can access which applications, with what rights, from where and in what way.

It also provides the functionality to:

- Determine, at any time, that this policy is being followed and respected,
- Simulate the impact of any change in the policy.

Evidian IAM Suite facilitates the creation of an identity repository including all people accessing to the information system, coming from different identity sources. In this repository, we will find employees, as well as externals and partners. Based on this identity repository, the identity and access governance policy will be applied.

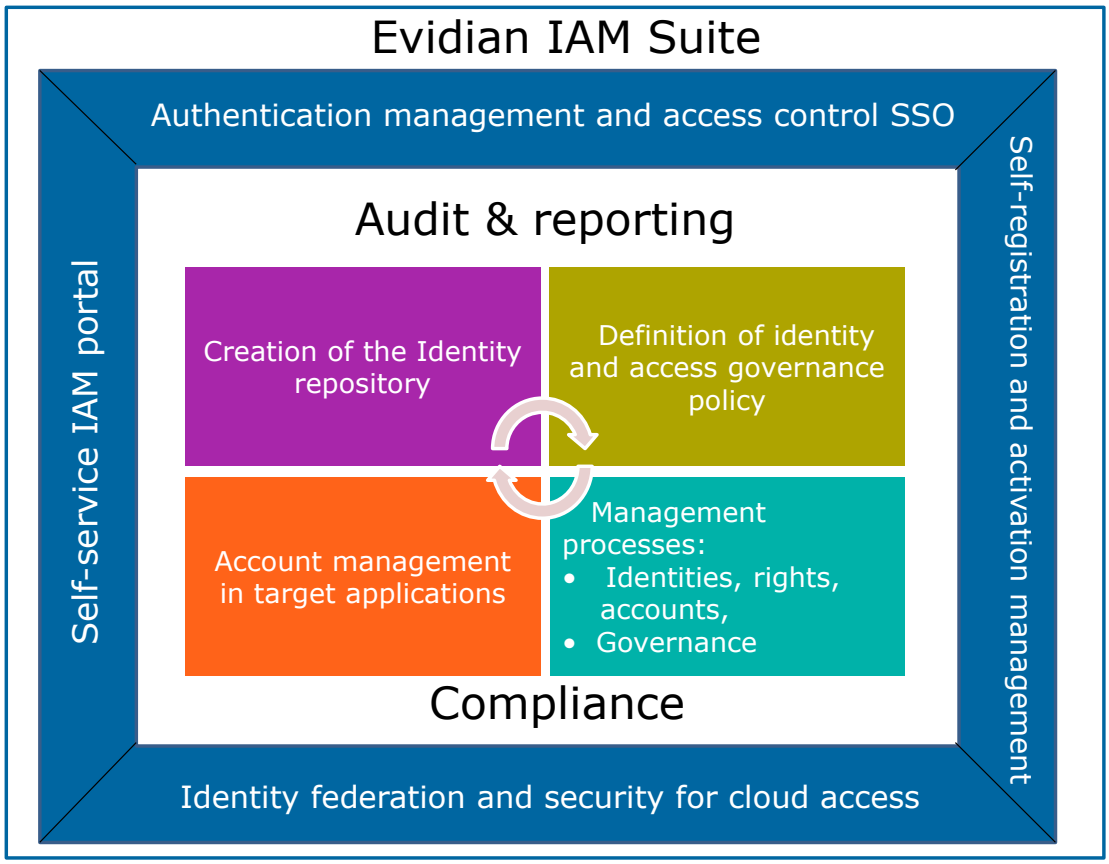
The various processes that Evidian IAM Suite offers as standard allow the company to give its users, among other things, the means to request rights to particular applications, to consult the identity repository, to maintain their own identity data, and to register the arrival or departure of an individual.

This takes place in a structured way, by involving the right people in the approval process and associated actions. These processes enable on-going actions to be properly monitored. The processes are available on the IAM portal for end users.

Once the rights assignment process is complete, account management in target applications is used to apply the identity and access governance policy.

Authentication, access control and SSO functions ensure secure and easy access to all types of applications. They are supplemented by identity federation and security for applications accessed via the Cloud, to provide a consistent working environment for the end user.

Of course, all actions are audited and it is possible to produce reports covering both administrative actions and user access to the information system.



Modeling the requirements for access rights

In order to assign access rights for users, IAM Suite uses an approach based on Role-Based Access Control (RBAC) and Organization-Based Access Control (OrBAC) models. These models allow you to link rights to a particular role: normally a job within the company. To avoid the proliferation of roles, Evidian also uses the concept of 'organization' to define the rights of people who fulfil a particular job in a given organization.

It is also possible to assign rights directly without going through role assignment in order to deal with exceptions.

The model also encompasses the concepts of organizational and hierarchical inclusion and exclusion to facilitate the task of assigning the rights associated with a role and how they are managed. The rules governing segregation of duties ensure consistency by avoiding assigning contradictory rights to the same person.

This modeling of rights will also be used internally to dynamically identify the players and their rights while the processes offered by IAM Suite are being executed.

For example, you give a departmental manager the role of 'validating access rights requests'. To further optimize the solution, it just remains to define the scope of those rights. This is achieved by using the concept of 'context'. So, for example, a context might be 'people in my team', 'people in store XX', 'external people' and so on. That's how various chains of clearance can be organized and operated, according to several different criteria.

This notion of 'context' can also be applied to other objects. For example, to determine the list of applications offered when an employee puts in a request for access rights, we can limit the information displayed in the white-pages directory, or limit information that can be modified via the workflow process interfaces provided as part of IAM Suite.

Using these concepts make for a very flexible and powerful solution, that can readily adapt to the changing needs of the business. Everything is configurable, which cuts operating costs.

Making it easier to assign rights and monitor changes

Once rights have been modeled, it's important to be able to assign these rights easily to employees, but also to have mechanisms to monitor functional changes that affect employees along with the associated changes in terms of rights.

Evidian IAM Suite makes use of user attributes values to assign roles to them that will involve rights. This granting of rights is made by applying so-called 'business rules'. These help define the roles that need to be associated with people, based on the values of certain attributes of these people. It is also possible to define exceptions. For example, everyone working in an banking agency must have the role of 'accessing the annual leave declaration application', apart from external people.

This feature makes it very easy to assign one or more roles to a newly hired employee, but also to dynamically adapt to any new roles that an employee may take on as a result of transferring within the company. So, for instance, a banking office employee that moves to the headquarters automatically obtains the rights that he needs for his new job.

Of course, it's possible to keep all the rights associated with both the banking office and the headquarter job for a while to facilitate the transition between the two positions.

Using business rules is not the only way to assign roles to individuals. It is also possible to do this using the role assignment process.

Delegating responsibility to the business

Evidian IAM Suite offers a standard set of processes for managing identities, roles and duties, accounts and services.

For example: setting up a new employee on the system; an employee leaving the organization; an employee transferring to another part of the organization; an employee requesting access rights for him/herself or for another person; modifying the attributes of an account; declaring a long period of absence; creating shared folders; etc. Currently, more than 40 processes are included as standard.

By using this process, the decisions involved in assigning rights and managing of the lifecycle of users are completely delegated to the business. You can move from centralized administration to an approach that is much closer to the 'field'.

Ensuring that rights are complied with at all times

Evidian IAM Suite provides the processes and functionality needed to control employee rights. The rights certification process enables managers to validate/correct the existing rights of one person or a group of employees.

Functions, such as reconciliation, allow you to detect discrepancies between what has been defined as the rights an employee must have and the rights they have in reality. Corrective actions are then proposed, to allow the company to respond and close the gap.

Reusing existing infrastructure

Evidian IAM Suite can be integrated into existing environments with no need for modifications.

For example, the picture in the next page shows the Evidian web site, secured using IAM Suite, whose structure has not been changed. This allows authenticated users to benefit from advanced services. The authorization form and links to secure services can be added without changing the existing site.

The option to request an account and secure its activation

The Evidian IAM Suite offers an auto-activation mechanism and allows users to request an access account.

In this current example, the person may indicate the banking agency where she works, her job and email address, for example. Using this data, the demands will be send to the right people and the right permissions will be assigned to her.

The IAM Suite then offers two modes of operation:

- Either IDs/passwords are sent out via SMS and/or email.
- Or the person receives an email with a configurable link – with a limited life span – asking her to activate the account that has just been created for her. At this point, the user can choose the password she will use in the future to connect to the information system.

Smartphone authentication

Evidian IAM Suite allows an employee to authenticate him/herself using a QR code via his/her smartphone.

IAM Suite can authenticate users using other methods such as:

- User ID and password,
- The virtual keyboard that allows a user to provide a username and password by clicking on a randomly positioned keyboard on the screen. This virtual keyboard provides extra protection against 'key loggers', without requiring additional software or an extra device,
- OTP (One Time Password),
- X .509 certified smart card,
- SAML (Service Provider/Identity Provider) token,
- Authentication method based on the Radius protocol,
- 'Grid Card password': each user has their own card for solving a one-time only challenge,
- SMS OTP or Mail OTP: each user can obtain an OTP via his mobile phone and/or email,
- Kerberos and other Windows domain authentication methods,
- External authentication mechanisms such as CAS, OpenID, OAuth, or linking to any external mechanism using SDK.

No password to remember

Evidian IAM Suite offers single sign-on (SSO) functionality. With this feature, the employee is authenticated only once and then any new request for authentication to access an application is taken into account by IAM Suite.

Goodbye to the problem of people forgetting their passwords after a long weekend or vacation!

Conclusion

By implementing Evidian IAM Suite, a bank will deliver an identity and access management solution to his customers, partners and subsidiaries that will enable them, among other thing, to:

- Manage the identities of people accessing the information system,
- Delegate rights management to those closest to these people, who really know their business needs,
- Ensure that the access governance policy currently in force is respected at all times,
- Immediately take into account any changes in people's rights, for example to reflect changes in their job role, a long absence, changes in their contract of employment...
- Evolve to reflect any organizational changes in the company,
- Give employees the autonomy to manage their own access without compromising company security,
- Have a set of reports to show the governance of the Information System,
- Provide simple and secure access (no password to remember),
- Adapt to the existing infrastructure.

Without being exhaustive in describing the capabilities of Evidian IAM Suite, this white paper shows how Evidian is the ideal partner to help financial market participants to meet their needs.

Evidian IAM Suite

Our IAM solution is recognized by customers and analysts for its completeness. The Evidian IAM Suite offers the following components that can be deployed independently or natively integrated.

- Evidian Identity Governance and Administration allows authorization governance and a full lifecycle management of identities and access to services, driven by a security policy combined with approval workflows.
- Evidian Web Access Manager manages access federation to Web applications, secures remote access for mobile users and replaces all user passwords with a single and strong authentication method.
- Evidian Enterprise SSO facilitates access to enterprise and personal applications from workstations and mobile devices, frees users from the password constraints.
- Evidian Authentication Manager provides strong authentication on workstations and mobile devices: smartcard or token, X509 certificate, contactless RFID cards, biometrics, one time password.
- Evidian SafeKit brings high availability and load balancing to applications.

www.evidian.com

Atos